Computational Algebraic Geometry

Algebraische Geometrie auf dem Computer

Joachim Wehler

Wintersemester 2003/04

Version 1.0

Ludwigs-Maximilians-Universität München

1 EINLEITUNG 3

1.1 ZIELSETZUNG 3
1.2 BEISPIELE: KURVEN, FLÄCHEN, HYPEREBENENSCHNITTE 4

2 AFFINE VARIETÄTEN UND AFFINE ALGEBREN 7

2.1 AFFINE VARIETÄTEN UND REGULÄRE ABBILDUNGEN 8
2.2 AFFINE ALGEBREN UND ALGEBRA MORPHISMEN 18

3 ERGEBNISSE DER KOMMUTATIVEN ALGEBRA 26

3.1 RESULTANTENSYSTEME 26
3.2 ENDLICHE ABBILDUNGEN 31
3.3 IRREDUZIBLE VARIETÄTEN UND PRIMIDEALE 41

4 GRÖBNER BASICS 49

4.1 DIVISIONS ALGORITHMUS 49
4.2 GRÖBNER BASEN 58
4.3 DAS RECHNEN MIT IDEALEN 71

5 PROJEKTIVE VARIETÄTEN UND GRADUIERTE ALGEBREN 81

5.1 PROJEKTIVE VARIETÄTEN UND REGULÄRE ABBILDUNGEN 81
5.2 DAS HILBERT POLYNOM 97

6 BASISWECHSEL 102

6.1 ZAHLENTHEORIE 102
6.2 RIEMANNSCHE FLÄCHEN 108

7 SKRIPTE AUSGEWÄHLTER TOOL-BEISPIELE 112

7.1 SINGULAR-SKRIPTE 112
7.2 MACAULAY2-SKRIPTE 122
7.3 PARI-SKRIPTE 131

8 LITERATUR 137

8.1 KOMMUTATIVE ALGEBRA 137
8.2 ALGEBRAISCHE GEOMETRIE 137
8.3 ZAHLENTHEORIE 137
8.4 RIEMANNSCHE FLÄCHEN 138
8.5 TOOLS 138

1 Einleitung

1.1 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 in Kapitel 6.

1.2 Beispiele: 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

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

1.2.1 Tool-Beispiel *(Ebenes Achsenkreuz)*

- Curves/PlaneCoordinates

Ebenes Koordinatenkreuz =

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

1.2.2 Tool-Beispiel *(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 $a \in [-2, +2]$.

1.2.3 Tool-Beispiel *(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 $a \in [-1.2, +1.2]$.

1.2.4 Tool-Beispiel *(Räumliches Achsenkreuz)*

- Curves/SpaceCoordinates

Räumliches Koordinatenkreuz =

$$\begin{aligned}&\{(x,y,z)\in \boldsymbol{R}^3 : z=0 \ \ und \ y=0\}\\ \cup&\{(x,y,z)\in \boldsymbol{R}^3 : z=0 \ \ und \ x=0\}\\ \cup&\{(x,y,z)\in \boldsymbol{R}^3 : x=0 \ \ und \ y=0\}\end{aligned}$$

1.2.5 Tool-Beispiel (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

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

1.2.6 Tool-Beispiel (Flächen 3. Grades im 3-dimensionalen Raum)

- Surfaces/SmoothFermatSurface

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

- Surfaces/WhitneyUmbrella

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

Alle Punkte auf der y-Achse sind singulär.

1.2.7 Tool-Beispiel (Hyperebenenschnitte von Flächen im 3-dimensionalen Raum)

- Surfaces/HyperbolicSurfaces

Hyperebenenschnitt einer kubischen Fläche:

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

mit

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

- Surfaces/FamilyOfQuadricSurfaces

Hyperebenenschnitt einer kubischen Fläche:

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

mit

$$H_c=\{(x,y,z)\in \boldsymbol{R}^3 : z-c=0\},\ c\in\{-1,0,1,4\}$$

- Surfaces/FamilyOfCubicSurfaces

Hyperebenenschnitt einer kubischen Fläche:

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

mit

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

- Surfaces/BlowUp

  Hyperebenenschnitt einer quadratischen Fläche:

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

  mit

  $$H_c = \{(x, y, z) \in \boldsymbol{R}^3 : z - c = 0\}, \; c \in [-4, 4]$$

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:

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

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* über 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.

2.1 Affine Varietäten und reguläre Abbildungen

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

2.1.1 Definition *(Affine Varietät)*

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 $\boldsymbol{A}_K^n$. Man schreibt

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

Affine Varietäten, die Nullstellengebilde eines einzigen, von Null verschiedenen Polynoms sind, heißen *Hyperflächen* bzw. im Falle eines linearen Polynoms *Hyperebenen.*

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

$$g : X \longrightarrow Y,$$

die durch Polynome gegeben werden kann, d.h. es existieren Polynome

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

mit

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

Hinweis. [Har1977] verwendet statt des Begriffes „affine Varietät“ den Begriff „algebraische Teilmenge des $\boldsymbol{A}_K^n$“. Eine affin-algebraische Varietät im Sinne von [Har1977] ist zusätzlich *irreduzibel*; siehe Definition 3.3.4.

2.1.2 Bemerkung *(Affine Varietät)*

i) Eine affine *k-Varietät* ist einerseits eine Teilmenge des $\boldsymbol{A}_K^n$. Die Punkte dieser Teilmenge haben ihre Koordinaten in dem algebraisch-abgeschlossenen Körper K. 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

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

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). 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

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

bezeichnet. Dabei kann es verschiedene Ideale geben

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

welche dieselbe Varietät

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

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

$$\boldsymbol{A}_K^n \longrightarrow \boldsymbol{A}_K^m$$

zwischen den einbettenden affinen Räumen induziert.

Das Verschwindungsideal einer affinen Varietät hat die Eigenschaft:

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

2.1.3 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

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

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

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

2.1.4 Beispiel (Reguläre Abbildungen zwischen affinen Varietäten)

i) Die Abbildung

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

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; siehe Beispiel 1.2.3. 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

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

kein Isomorphismus affiner Varietäten. Wir werden in Beispiel 3.2.10, Teil i) sehen, daß die affine Gerade und die Neil Parabel auch bzgl. keiner anderen regulären Abbildung isomorph sind.

ii) 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

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

siehe Beispiel 1.2.2. 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.

iii) 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

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

eine reguläre Abbildung

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

Ihr Bild läßt die punktierte y-Achse aus:

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

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 - unter der Abbildung, welche dem Parameter $(0,0,z) \in E$ die Gerade mit der Steigung z zuordnet:

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

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; siehe Beispiel 1.2.7, Teil iv).

Eine zweite reguläre Abbildung

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

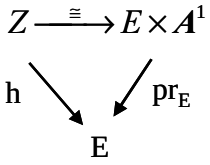
ist die Einschränkung der Projektion

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

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

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

mit regulärer Umkehrung

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

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

iv) Die Deformation von Varietäten läßt sich als reguläre Abbildung auffassen.

Das Beispiel 1.2.7, Teil i) der Hyperebenenschnitte, welche Kurven 2. Ordnung darstellen, läßt sich als reguläre Abbildung folgendermaßen beschreiben: Man definiert für ein festes $b \in k$, z.B. $b = 1$, die Fläche

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

Schränkt man die Projektion

$$pr_2 : \boldsymbol{A}^2 \times \boldsymbol{A}^1 \longrightarrow \boldsymbol{A}^1$$

auf diese Fläche ein

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

so *fasert* diese Einschränkung die Fläche als eine Familie ebener Kurven 2. Ordnung: Die Faser über dem Punkt $z \in \boldsymbol{A}^1$ ist die Kurve

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

Bei Variation des Basispunktes $z \in \boldsymbol{A}^1$ durchlaufen die Fasern eine Deformation quadratischer Kurven.

Analog läßt sich das Beispiel 1.2.7, Teil ii) von Hyperebenenschnitten beschreiben, die kubische Kurven darstellen: Es sei

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

und

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

die Einschränkung der Projektion

$$pr_2 : \boldsymbol{A}^2 \times \boldsymbol{A}^1 \longrightarrow \boldsymbol{A}^1.$$

Jede Faser

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

ist eine kubische Kurve.

2.1.5 Bemerkung (Differentialgeometrie des rellen Blow-up)

Vom Standpunkt der Algebraischen Geometrie sind das Blow-up $Z \subset \boldsymbol{A}^3$ aus Beispiel 2.1.4, Teil iii) und die affine Ebene $\boldsymbol{A}^2$ nicht unterscheidbar. Wir haben einen regulären Isomorphismus angegeben.

Im Falle des reellen Grundkörpers $k = \boldsymbol{R}$ bilden die rellen Punkte des Blow-up aus Beispiel Beispiel 2.1.4, Teil iii)

$$Z(\boldsymbol{R}) := \{(x_1, x_2, x_3) \in Z : x_i \in \boldsymbol{R}\}$$

eine Fläche $Y \subset \boldsymbol{R}^3$, die auch in der Differentialgeometrie studiert wird. Vom Standpunkt der Differentialgeometrie tragen Y und die Euklidische Ebene $\boldsymbol{R}^2$ auf natürliche Weise eine Riemannsche Metrik. Die hieraus resultierenden Riemannschen Mannigfaltigkeiten sind jedoch nicht isomorph.

Denn die Euklidische Ebene $\boldsymbol{R}^2$ hat die Gauss Krümmung $G = 0$. Das relle Blow-up Y, versehen mit der induzierten Riemannschen Metrik des umgebenden Euklidischen Raumes $\boldsymbol{R}^3$, hat dagegen eine nicht-verschwindende Gauss Krümmung: Bzgl. der Parametrisierung

$$\varphi : \boldsymbol{R}^2 \longrightarrow Y, (u,v) \mapsto (u, u \cdot v, v)$$

berechnet sich die 1. Fundamentalform von Y als

$$E = \langle \varphi_u, \varphi_u \rangle = 1 + v^2,\ F = \langle \varphi_u, \varphi_u \rangle = v \cdot u,\ G = \langle \varphi_v, \varphi_v \rangle = 1 + u^2$$

und die 2. Fundamentalform als

$$e = \frac{\det |\varphi_{uu} \quad \varphi_u \quad \varphi_v|}{\sqrt{E \cdot G - F^2}} = 0,\ f = \frac{\det |\varphi_{uv} \quad \varphi_u \quad \varphi_v|}{\sqrt{E \cdot G - F^2}} = \frac{-1}{(E \cdot G - F^2)^{\frac{3}{2}}},$$

$$g = \frac{\det |\varphi_{vv} \quad \varphi_u \quad \varphi_v|}{\sqrt{E \cdot G - F^2}} = 0.$$

Der Weingarten Operator

$$L_p : T_p Y \longrightarrow T_p Y$$

hat an der Stelle $p = \varphi(u,v)$ bzgl. der Basis (φ_u, φ_u) des Tangentialraumes $T_p Y$ die Matrix

$$L_p = \frac{1}{E \cdot G - F^2} \begin{pmatrix} G & -F \\ -F & E \end{pmatrix} \cdot \begin{pmatrix} g & -f \\ -f & e \end{pmatrix} = \frac{1}{(1 + u^2 + v^2)^{\frac{3}{2}}} \begin{pmatrix} u \cdot v & -(1+u^2) \\ -(1+v^2) & u \cdot v \end{pmatrix}.$$

Seine Eigenwerte sind die beiden Hauptkrümmungen

$$\kappa_1 = \frac{u \cdot v + \sqrt{\left(1+u^2\right)\cdot\left(1+v^2\right)}}{\left(1+u^2+v^2\right)^{\frac{3}{2}}} \text{ und } \kappa_2 = \frac{u \cdot v - \sqrt{\left(1+u^2\right)\cdot\left(1+v^2\right)}}{\left(1+u^2+v^2\right)^{\frac{3}{2}}}.$$

Die Gauss Krümmung ist

$$G = \kappa_1 \cdot \kappa_2 = \frac{-1}{\left(1+u^2+v^2\right)^2} \neq 0$$

Bezogen auf den Normalenvektor

$$N_p = \frac{\varphi_u \times \varphi_v}{\left|\varphi_u \times \varphi_v\right|} = \frac{1}{\sqrt{1+u^2+v^2}} \begin{pmatrix} v \\ -1 \\ u \end{pmatrix}$$

beträgt die Hauptkrümmung

$$H = \frac{1}{2}\left(\kappa_1 + \kappa_2\right) = \frac{u \cdot v}{\left(1+u^2+v^2\right)^{\frac{3}{2}}}$$

Speziell im Punkt $p = (0,0,0) \in Y$ hat die Fläche bezogen auf den Normalenvektor

$$N_p = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$$

die beiden Hauptkrümmungsrichtungen

- $\varphi_u + \varphi_v = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ mit Krümmung $\kappa = -1$
- und $\varphi_u - \varphi_v = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ mit Krümmung $\kappa = +1$.

2.1.6 Bemerkung (Affine Varietäten und Ideale)

i) Die folgende Tabelle 1 zeigt eine erste Übersetzung zwischen geometrischen und algebraischen Objekten der Algebraischen Geometrie, nämlich zwischen einer affinen Varietät als Punktmenge eines affinen Raumes und zwischen ihrem Ideal im Polynomring.

Geometrie	Übersetzung	Algebra
Affine k-Varietät $X \subset \boldsymbol{A}_K^n$	$X \mapsto Id(X)$ $Var(I) \leftarrow\mid I$	Reduziertes Ideal $I \subset k[X_1,...,X_n]$
Durchschnitt von Varietäten	$X_1 \cap X_2 \mapsto \sqrt{Id(X_1)+Id(X_2)}$ $Var(I_1) \cap Var(I_2) \leftarrow\mid I_1 + I_2$	Summe von Idealen
Vereinigung von Varietäten	$X_1 \cup X_2 \mapsto Id(X_1) \cap Id(X_2)$ $Var(I_1) \cup Var(I_2) \leftarrow\mid I_1 \cap I_2$	Durchschnitt von Idealen

Tabelle 1: Korrespondenz von Geometrie und Algebra

Hinweis. 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

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

ii) Für eine Varietät X gilt stets

$$Var(Id(X)) = X .$$

Für ein Ideal $I \subset k[X_1,...,X_n]$ gilt stets

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

Ist das Ideal I reduziert, so gilt also

$$Id(Var(I)) = I .$$

Das ist die Aussage des Hilbertschen Nullstellensatzes ([CLO1997] Chap. 4, §1). Dabei ist es entscheidend, daß die Varietät eines Ideals als Teilmenge mit Koordinaten in einem algebraisch-abgeschlossenen Körper K aufgefaßt wird.

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

- Beliebiger Durchschnitt

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

- Endliche Vereinigung

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

- Leere Varietät, gesamter affiner Raum

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

Damit erfüllen affine k-Varietäten in einem festen affinen Raum 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:

2.1.7 Definition (Topologie)

Eine *Topologie* auf einer Menge X ist eine Familie T von Teilmengen von X mit folgenden Eigenschaften:

- T enthält die leere Menge $\varnothing$ und die gesamte Menge X
- T enthält mit je zwei Mengen U_1 und U_2 auch deren Durchschnitt $U_1 \cap U_2$
- 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, T) heißt *topologischer Raum*, die Mengen aus T heißen *offene* Mengen, ihre Komplemente

$$A := X - U, U \in T$$

heißen *abgeschlossene* Mengen.

2.1.8 Definition (Zariski Topologie)

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

$$Z = Y \cap X\ .$$

2.1.9 Bemerkung (Zariski Topologie)

i) Reguläre Abbildungen zwischen affinen Varietäten sind stetig bzgl. der Zariski Topologie. Dabei heißt eine Abbildung

$$g : (X, T_X) \longrightarrow (Y, T_Y)$$

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 regulären Abbildung folgt daraus, daß das Urbild einer affinen Varietät wieder eine affine Varietät ist.

Die Umkehrung gilt nicht: Die Abbildung der Neil Parabel

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

aus Beispiel 2.1.4 ist stetig: Alle affine Varietäten von $\boldsymbol{A}^1$, welche von $\boldsymbol{A}^1$ verschieden sind, sind endliche Punktmengen. Ihre Urbilder sind wiederum endliche Punktmengen. Die Abbildung ist jedoch nicht regulär.

ii) Im Falle $k = \boldsymbol{R}$ oder $k = \boldsymbol{C}$ sind Polynome stetige Funktionen bzgl. der Euklidischen Topologie des Zahlenraumes $\boldsymbol{A}_C^n$. 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 $\boldsymbol{A}_C^1$.
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.

2.2 Affine Algebren und Algebra Morphismen

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:

2.2.1 Definition *(Koordinatenring einer affinen Varietät)*

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

$$k[X] := k[X_1,...,X_n] / \ Id(X).$$

2.2.2 Bemerkung *(Koordinatenring)*

i) Der Koordinatenring einer affinen k-Varietät X ist eine endlich erzeugte, reduzierte k-Algebra (*affine k-Algebra*). Der Koordinatenring ist zugleich der Ring der k-regulären Funktionen

$$g : X \longrightarrow \boldsymbol{A}^1_{\boldsymbol{K}}$$

von der Varietät in den algebraischen Abschluß des Grundkörpers.

ii) Umgekehrt ist jede affine k-Algebra Quotient

$$A = k[X_1,...,X_n] / I$$

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

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

Das Ideal I ist genau dann reduziert, wenn A reduziert ist. Mit

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

erhält man eine affine k-Varietät mit der affinen Algebra A als Koordinatenring.

2.2.3 Bemerkung *(Induzierter Morphismus zwischen Koordinatenringen)*

Es seien $X \subset \boldsymbol{A}^n$, $Y \subset \boldsymbol{A}^m$ zwei affine Varietäten.

i) Mit Hilfe einer regulären Abbildung

$$g : X \longrightarrow Y$$

lassen sich reguläre Funktionen auf Y zurückziehen zu regulären Funktionen auf X, d.h. es wird (kontravariant) ein Morphismus

$$\varphi := \varphi_g : k[Y] \longrightarrow k[X],\ h \mapsto h \circ g\ .$$

der Koordinatenringe induziert.

Zum Nachweis, daß der Rückzug wieder eine reguläre Funktion ist, geht man aus von einer Darstellung der regulären Abbildung durch Polynome:

$$g(X_1,...,X_n) = (\ g_1(X_1,...,X_n),...,g_m(X_1,...,X_n)\ )\ \text{ mit }\ g_i \in k[X_1,...,X_n],\ i = 1,...,m\ .$$

Diese definiert eine Abbildung von Polynomringen

$$\Phi : k[Y_1,...,Y_m] \longrightarrow k[X_1,...,X_n],\ \Phi(Y_i) := g_i \in k[X_1,...,X_n],\ i = 1,...,m\ ,$$

durch das Pull-back der Koordinatenfunktionen von Y mit Hilfe der definierenden Polynome der regulären Abbildung g. Es gilt

$$\Phi(Id(Y)) \subset Id(X).$$

Der Rückzug auf dem Niveau der Koordinatenringe

$$\varphi_g : k[Y_1,...,Y_m]/Id(Y) \longrightarrow k[X_1,...,X_n]/Id(X)$$

ist dann die kommutative Ergänzung des folgenden Diagramms:

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

ii) Umgekehrt induziert ein Morphismus affiner k-Algebren

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

kontravariant eine reguläre Abbildung

$$g := g_\varphi = (\ g_1,...,g_m) : X \longrightarrow Y$$

zwischen den affinen Varietäten: Man liftet zunächst

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

auf die Ebene der Polynomringe zu einer Abbildung

$$\Phi : k[Y_1,...,Y_m] \longrightarrow k[X_1,...,X_n] \text{ mit } \Phi(Id(Y)) \subset Id(X)$$

und definiert dann

$$g_i := \Phi(Y_i) \in k[X_1,...,X_n],\ i = 1,...,m\ .$$

Aus dieser Bemerkung ergibt sich als Konsequenz:

2.2.4 Satz (Affine Varietät und affine Algebra)

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

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

- Entweder geometrisch als Nullstellengebilde von Polynomen und als polynomiale Abbildungen
- oder algebraisch als affine Algebren und als 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.

2.2.5 Lemma (Punkte und Auswertungsmorphismen)

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

$$\varepsilon : X \xrightarrow{\cong} Hom_k(k[X], K),\ x \mapsto [\varphi \mapsto \varphi(x)].$$

Beweis. Die Abbildung ist injektiv, da sich zwei verschiedene Punkte $x \neq y \in X$ durch mindestens eine Koordinatenfunktion unterscheiden lassen.

Für die Surjektivität betrachtet man zu einem gegebenen Morphismus

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

die Bilder der Restklassen der Koordinatenfunktionen

$$x_\nu := \varphi(\overline{X_\nu}) \in K,\ \nu = 1,..., n.$$

Dann liegt der Punkt

$$x := (x_1,..., x_n) \in K^n$$

bereits in X : Denn für jedes $g \in Id(X)$ gilt

$$g(x) = g(\varphi(\overline{X_1}),..., \varphi(\overline{X_n})) = \varphi(\overline{g}) = \varphi(0) = 0.$$

Schließlich rechnet man nach

$$\varepsilon(x) = \varphi \text{ , q.e.d.}$$

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 2.1.4, 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

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

2.2.6 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.

i) Dann gilt

$$\overline{g(X)} = Var\left(\pi^{-1}\left(\ker \varphi_g\right)\right)$$

mit der kanonischen Restklassenabbildung

$$\pi : k[Y_1,...,Y_m] \longrightarrow k[Y].$$

ii) Desweiteren gilt

- Es 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 ist.

Beweis. i) Durch Komposition mit der Inklusion

$$Y \xrightarrow{\subset} \boldsymbol{A}^m$$

können wir uns auf den Spezialfall

$$Y = \boldsymbol{A}^m$$

beschränken, also eine reguläre Abbildung

$$g : X \longrightarrow \boldsymbol{A}^m$$

voraussetzen. Wir zeigen zunächst die Inklusion

$$g(X) \subset Var\left(\ker \varphi_g\right).$$

Für jede Funktion $f \in \ker \varphi_g$ gilt

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

d.h.

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

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

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

Zum Beweis der Umkehrung: Zunächst gilt

$$\ker \varphi_g \supset Id(g(X)),$$

denn für jede Funktion

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

gilt

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

Es folgt

$$Var(Id(g(X))) = Var\left(Id\left(\overline{g(X)}\right)\right) = \overline{g(X)} \supset Var(\ker \varphi_g)$$

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

$$Z = Var\left(\pi^{-1}(\ker \varphi_g)\right)$$

folgen im Falle eines algebraisch-abgeschlossenen Grundkörpers mit dem Hilbertschen Nullstellensatz das Verschwindungideal

$$Id(Z) = Id\left(Var\left(\pi^{-1}(\ker \varphi)\right)\right) = \sqrt{\pi^{-1}(\ker \varphi)} = \pi^{-1}(\ker \varphi)$$

und der Koordinatenring

$$k[Z] = k[Y_1,...,Y_m]/Id(Z) = k[Y_1,...,Y_m]/\pi^{-1}(\ker \varphi_g) = k[Y]/\ker \varphi_g .$$

Die Injektivität der Abbildung

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

ist äquivalent mit

$$\ker \varphi_g = 0$$

also mit

$$Id(Z) = Id(Y).$$

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 2.2.4 äquivalent mit der Isomorphie

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

2.2.7 Tool-Beispiel (Induzierte Morphismen)

i) Die Neil Parabel Z , siehe Beispiel 2.1.4, Teil i), hat den Koordinatenring

$$k[Z] = k[X,Y] / \langle Y^2 - X^3 \rangle.$$

Der Koordinatenring ist isomorph zur affinen Algebra

$$k[T^2, T^3]$$

unter der Isomorphie

$$k[X,Y] / \langle Y^2 - X^3 \rangle \xrightarrow{\sim} k[T^2, T^3],\ X \mapsto T^2 \text{ und } Y \mapsto T^3.$$

Die reguläre Abbildung aus Beispiel 2.1.4, Teil i),

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

induziert den Morphismus affiner Algebren

$$\varphi : k[X,Y] \longrightarrow k[T],\ X \mapsto T^2 \text{ und } Y \mapsto T^3.$$

Ihre Einschränkung

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

induziert die Abbildung der Koordinatenringe

$$\varphi : k[Z] \cong k[T^2, T^3] \xrightarrow{\subset} k[T].$$

- Die Injektivität der Abbildung φ entspricht der Tatsache, daß die reguläre Abbildung g ein dichtes Bild hat, es gilt sogar

$$g(\boldsymbol{A}^1) = Z.$$

- Die Abbildung φ ist nicht surjektiv. Das entspricht der Tatsache, daß die reguläre Abbildung g kein Isomorphismus ist.

ii) Die Hyperbel Z, siehe Beispiel 2.1.4, Teil ii), hat den Koordinatenring

$$k[Z] = k[X,Y] / \langle X \cdot Y - 1 \rangle .$$

Der Koordinatenring ist isomorph zur affinen Algebra

$$k\left[T, \frac{1}{T}\right]$$

unter der Isomorphie

$$k[X,Y] / \langle X \cdot Y - 1 \rangle \xrightarrow{\sim} k\left[T, \frac{1}{T}\right],\ X \mapsto T \text{ und } Y \mapsto \frac{1}{T}.$$

Die erste Projektion

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

induziert als Morphismus affiner Algebren die Inklusion

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

Die Einschränkung

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

induziert die Inklusion affiner Algebren

$$\varphi : k[X] \longrightarrow k\left[T, \frac{1}{T}\right],\ X \mapsto T .$$

- Die Injektivität der Abbildung φ entspricht der Tatsache, daß die reguläre Abbildung g ein dichtes Bild hat:

$$\overline{g(Z)} = \boldsymbol{A}^1 .$$

- Die Abbildung φ ist nicht surjektiv. Das entspricht der Tatsache, daß die reguläre Abbildung g kein abgeschlossenes Bild hat.

iii) 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 folgenden Beispiele sind mit dem Computertool Singular berechnet.

- MyExamples/FiniteMap/Examples

Definition regulärer Abbildungen der Neil Parabel, Hyperbel und Blow-up.

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.

3.1 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.

3.1.1 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.

3.1.2 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.

3.1.3 Bemerkung (Resultante und Diskriminante)

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

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

3.1.4 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

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

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

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

3.1.5 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.

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

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 3.1.2, 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 3.1.2, 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.

3.2 Endliche Abbildungen

3.2.1 Bemerkung *(Ringmorphismus und Algebra- bzw. Modulstruktur)*

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.

3.2.2 Definition *(Endliche Abbildungen)*

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.

Obige Definitionen gelten insbesondere für Morphismen zwischen affinen Algebren. Man überträgt sie auf reguläre Abbildungen, indem man für die induzierten Morphismen der Koordinatenringe die entsprechende Eigenschaft fordert: Eine reguläre Abbildung zwischen affinen Varietäten heißt *endlich* (bzw. *von endlichem Typ* bzw. *ganz*), wenn der induzierte Morphismus der Koordinatenringe endlich (bzw. von endlichem Typ bzw. ganz) ist.

3.2.3 Bemerkung *(Endlichkeit)*

i) 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.

ii) 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.

iii) Im Falle einer Körpererweiterung

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

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

3.2.4 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

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

Wir bezeichnen mit

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

die Matrix der algebraischen Komplemente von C. Aus der Gleichung

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

folgt

$$\det C = 0,$$

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

3.2.5 Lemma *(Transitivität von Endlichkeit und Ganzheit)*

Die Komposition endlicher (bzw. ganzer) Abbildungen

$$R \xrightarrow{\varphi} S \text{ und } S \xrightarrow{\psi} T$$

ist wieder endlich (bzw. ganz).

Beweis. 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

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

mit Elementen

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

Also ist insbesondere die Abbildung

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

ganz.

Außerdem ist die Abbildung

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

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

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

Dann ist nach Satz 3.2.4 die Inklusion

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

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 3.2.4 ganz über R, q.e.d.

3.2.6 Lemma (Endlichkeit und Ganzheit)

Für einen Morphismus von Ringen

$$\varphi : R \longrightarrow S$$

gilt:

i) Aus der Endlichkeit von φ folgt seine Ganzheit.

ii) Ist φ von endlichem Typ, so folgt aus der Ganzheit von φ auch seine Endlichkeit.

iii) Die ganzen Elemente bzgl. φ bilden einen Unterrring von S.

Beweis. ad i) Die Aussage ist Inhalt von Satz 3.2.4.

ad ii) 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 3.2.4 und der Transitivität der Endlichkeit nach Lemma 3.2.5.

ad iii) Sind zwei Elemente $x, y \in S$ ganz über R, so ist $R[x, y]$ endlich über R, und nach Teil ii) auch ganz über R, q.e.d.

3.2.7 Definition (Normalisierung)

Es sei R ein Integritätsbereich. Die *Normalisierung* von 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.

Die Bedeutung der Ganzheit von Ringerweiterungen liegt in folgendem Fortsetzungssatz. Seine geometrische Formulierung ist der Projektionssatz für endliche reguläre Abbildungen.

3.2.8 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

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

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 3.1.5 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 Abbildungen ist der Projektionssatz. Er heißt in der Sprache der Zariski Topologie:

3.2.9 Korollar (Projektionssatz für endliche Abbildungen)

Jede endliche reguläre Abbildung zwischen affinen Varietäten

$$g: X \longrightarrow Y$$

ist abgeschlossen, d.h. sie bildet eine abgeschlossene Teilmenge von X auf eine abgeschlossene Teilmenge 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 2.2.6 ist dann die induzierte Abbildung der Koordinatenringe

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

injektiv. Nach Voraussetzgung ist sie endlich, nach Lemma 3.2.4 also ganz. Damit liegt die Situation von Satz 3.2.8 vor. Es sei $y \in Y$ ein vorgegebener Punkt und

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

der zugehörige Auswertungshomomorphismus. Nach Satz Satz 3.2.8 gibt es eine Fortsetzung

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

Nach Lemma 2.2.5 ist dieser k – Algebra-Morphismus die Auswertung an einer Stelle $x \in X$. Man rechnet nach:

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

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, siehe Beispiele 3.2.10.

*3.2.10 **Tool-Beispiel** (Normalität, endliche Abbildungen)*

i) Jeder faktorielle Ring ist normal, insbesondere jeder Polynomring $k[X_1,...,X_n]$.

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.

ii) Die Neil Parabel Z, siehe Beispiel 2.1.4, 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 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.

iii) Die Projektion der Hyperbel Z, siehe Beispiel 2.1.4, Teil ii) auf die x-Achse ist keine endliche Abbildung. Denn die induzierte Abbildung der Koordinatenringe

$$\varphi : k[X] \longrightarrow k\left[T, \frac{1}{T}\right],\ X \mapsto T$$

ist nicht endlich.

iv) Mit dem Computertool Singular lassen sich die Normalisierungen von Koordinatenringen berechnen.

- MyExamples/Normalization/Examples

Die Normalisierung der *Neil-Parabel* ist die Abbildung

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

bzw. auf dem Niveau der Koordinatenringe die Inklusion

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

Die Normalisierung des *Whitney-Umbrella*

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

ist auf dem Niveau der Koordinatenringe die Inklusion

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

Der Whitney-Umbrella hat also den Koordinatenring

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

Auf dem Niveau der Varietäten ist die Normalisierung die reguläre Abbildung

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

Sie hat dichtes Bild, siehe Bemerkung 2.2.3, Teil i).

Die Normalisierung der *5-nodalen Kurve*

$$Z = \left\{(x, y) \in \boldsymbol{A}^2 : 32x^2 - 2097152y^{11} + 14441792y^9 - 360448y^7 + 39424y^5 - 1760y^3 + 22y - 1 = 0 \right\}$$

ist die reguläre Abbildung

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

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

3.2.11 ***Satz*** *(Noethersche Normalisierung)*

Es sei

$$A = k[X_1, ..., X_n] / I$$

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

$$\varphi : k[X_1, ..., X_n] \xrightarrow{\cong} k[X_1, ..., X_n]$$

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

$$k[X_1, ..., X_d] \longrightarrow k[X_1, ..., X_n] / \varphi(I) \cong A$$

injektiv und endlich ist (*Noether Normalisierung*).

Beweis. siehe [GP2002], Theor. 3.4.1.

Satz 3.2.11 besagt in geometrischer Formulierung, daß sich jede affine Varietät als verzweigte Überlagerung über einem wohlbestimmten affinen Raum darstellen läßt: Zu jeder affinen Varietät $X \subset \boldsymbol{A}_K^n$ gibt es eine Zahl $d \leq n$, so daß sich X - eventuell nach einer Koordinatentransformation des affinen Raumes $\boldsymbol{A}_K^n$ - unter der regulären Abbildung

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

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

*3.2.12 **Tool-Beispiel** (Noethersche Normalisierung)*

Singular Beispiele

- MyExamples/NoetherNormalization/Example

Hyperbol, Blow-up, Affine Ebene mit transversaler affiner Geraden.

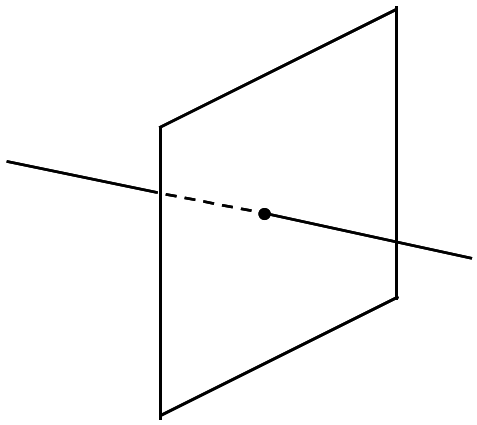


Abbildung 1: Y/Z-Ebene vereinigt mit X-Achse

3.3 Irreduzible Varietäten und Primideale

Ein weiterer Bezug zwischen dem Koordinatenring einer affinen Varietät und ihren geometrischen Eigenschaften wird bei der Zerlegung einer affinen Varietät deutlich. Hier entpricht der Zerlegung des Ideals der Varietät in Primideale der Zerlegung der Varietät in irreduzible Teilmengen bzgl. der Zariski Topologie. Aufgrund dieser Entsprechung kann man die Dimension einer Varietät sowohl algebraisch als auch geometrisch definieren - mit gleichem Resultat.

3.3.1 Definition *(Primideal)*

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:

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

Das Radikal eines Primärideals ist immer ein Primideal:

$$\sqrt{Primärideal} = Primideal .$$

Ein maximales Ideal ist immer auch ein Primideal.

3.3.2 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.

3.3.3 Tool-Beispiel (Primärzerlegung)

i) Mit Hilfe von Singular berechnet man die Primärzerlegung von Idealen:

- MyExamples/PrimaryDecomposition/Examples

ii) 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. 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.

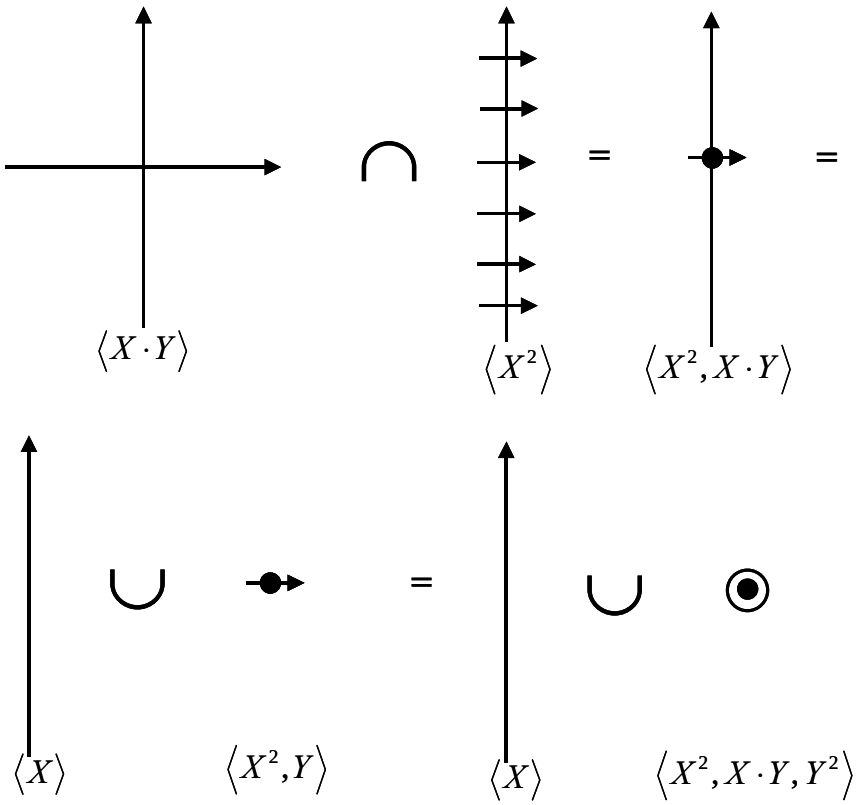


Abbildung 2: Eingebetteter Doppelpunkt

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

3.3.4 Definition (Irreduzible Varietät)

Eine nicht-leere affine Varietät

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

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

$$X = X_1 \cup X_2$$

mit zwei nichtleeren, voneinander verschiedenen, in der Zariski Topologie abgeschlossenen Teilmengen. Andernfalls heißt sie *reduzibel*.

Die leere Menge heißt reduzibel.

3.3.5 Satz (Irreduzible Varietät und Primideal)

Für eine algebraische k-Varietät $X \subset \boldsymbol{A}_K^n$ sind äquivalent:

- Es ist $X \subset \boldsymbol{A}_K^n$ irreduzibel
- Das Verschwindungsideal $Id(X) \subset k[X_1,...,X_n]$ ist ein Primideal.
- Der Koordinatenring $k[X]$ ist ein Integritätsbereich.

Unter Benutzung der beiden Funktoren aus Bemerkung 2.1.2

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

kann man die algebraische Aussage der Darstellung eines reduzierten Ideals als Durchschnitt von Primidealen in die geometrische Aussage der Darstellung einer affinen Varietät als Vereinigung irreduzibler Teilmengen übersetzen.

3.3.6 Satz (Zerlegung in irreduzible Komponenten)

Jede nicht-leere affine Varietät $X \subset \boldsymbol{A}^n$ besitzt eine endliche Zerlegung

$$X = \bigcup_{j \in J} X_j, \#J < \infty$$

in irreduzible affineVarietäten X_j. Im Falle einer unverkürzbaren Darstellung, d.h.

$$X_i \not\subset X_j, i \neq j,$$

sind die irreduziblen Mengen X_j eindeutig bestimmt *(irreduzible Komponenten)*. Sie entsprechen bijektiv den Primidealen

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

in einer unverkürzbaren Primzerlegung

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

unter der Zuordnung

$$Id(X_j) = p_j.$$

3.3.7 Definition (Dimension)

i) Die *kombinatorische Dimension* $d \in \boldsymbol{N}$ einer affinen Varietät X ist die maximale Länge einer Kette irreduzibler abgeschlossener Teilmengen von X

$$X_0 \underset{\neq}{\subset} X_1 \underset{\neq}{\subset} ... \underset{\neq}{\subset} X_d.$$

Man nennt 1-dimensionale Varietäten *Kurven* und 2-dimensionale Varietäten *Flächen*.

ii) Die *Krull-Dimension* $d \in \boldsymbol{N}$ eines Noetherschen Ringes R ist die maximale Länge einer Kette von Primidealen

$$p_0 \subsetneq p_1 \subsetneq ... \subsetneq p_d \, .$$

Der Dimensionsbegriff wurde hier als eine globale Größe eingeführt.

Die Dimension einer affinen Varietät hängt zudem nur von der irreduziblen Komponente maximaler Dimension ab.

3.3.8 Lemma (Erweiterung eines Primideals)

Bei einer ganzen Abbildung von Ringen

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

existiert zu jedem Primideal $p \subset R$ ein Primideal $P \subset S$ mit

$$P \cap R = p \, .$$

Beweis. Der Quotient R/p ist ein Integritätsbereich, es sei $k := Q(R/p)$ sein Quotientenkörper und $K := \overline{k}$ der algebraische Abschluß. Die Komposition der kanonischen Abbildungen

$$\varphi := \left[R \longrightarrow R/p \xrightarrow{\subset} k \xrightarrow{\subset} K \right]$$

hat nach Satz 3.2.8 eine Fortsetzung zu einem Ringmorphismus

$$\Phi : S \longrightarrow K, \Phi \mid R = \varphi \, .$$

Dann ist

$$P := \ker \Phi \subset S$$

ein Primideal mit $P \cap R = p$, q.e.d.

3.3.9 Satz (Dimensionstreue ganzer Ringerweiterungen)

Für eine ganze Abbildung von Ringen

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

gilt die Dimensionsformel

$$\dim R = \dim S \, .$$

Beweis. i) Wir zeigen zunächst $\dim R \geq \dim S$: Dazu sei

$$P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_d$$

eine Kette von Primidealen in S von maximaler Länge. Mit

$$p_i := P_i \cap R, i = 0,...,d$$

erhält man eine aufsteigende Folge von Primidealen in R

$$p_0 \subset p_1 \subset ... \subset p_d .$$

Zu zeigen ist

$$p_i \subsetneq p_{i+1}, i = 0,...,d-1.$$

Für einen indirekten Beweis nehmen wir an

$$p_{i+1} = p_i \text{ für ein } i \in \{0,...,d-1\}$$

und wählen ein Element

$$f \in (P_{i+1} - P_i) \subset S .$$

Wegen der Ganzheit der Ringerweiterung erfüllt f eine ganze Gleichung über R, insbesondere gibt es Elemente $a_i \in R, i = 1...,r$ mit

$$f^r + a_1 \cdot f^{r-1} + ... + a_{r-1} \cdot f + a_r \in P_i .$$

Die Zahl $r \in \boldsymbol{N}$ sei minimal gewählt mit dieser Eigenschaft. Aus der letzten Gleichung folgt

$$a_r \in R \cap P_{i+1} = p_{i+1} = p_i \subset P_i ,$$

also auch

$$f \cdot \left(f^{r-1} + a_1 \cdot f^{r-2} + ... + a_{r-2} \cdot f + a_{r-1} \right) \in P_i .$$

Wegen der Minimalität der Zahl r gehört der zweite, geklammerte Faktor dieses Produkt nicht zu P_i. Da P_i ein Primideal ist, muß dann gelten

$$f \in P_i ,$$

ein Widerspruch zur Wahl von $f \in P_{i+1} - P_i$.

ii) Wir zeigen nun $\dim S \geq \dim R$: Dazu gehen wir aus von einer Kette von Primidealen in R maximaler Länge

$$p_0 \subsetneq p_1 \subsetneq ... \subsetneq p_d .$$

Zu zeigen ist, daß sie sich zu einer Kette von Primidealen in S

$$P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_d, P_i \cap R = p_i, i = 0,...,d-1$$

erweitern läßt. Diese Aussage wird durch Induktion über d bewiesen.

Der Induktionsbeginn $d = 0$ ist die Aussage von Lemma 3.3.8. Für den Induktionsschritt sei eine Kette von Primidealen

$$P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_j, P_i \cap R = p_i, i = 0,..., j$$

schon gefunden. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\subset} & S \\ \downarrow \pi_R & & \downarrow \pi_S \\ R/p_j & \xrightarrow{\varphi} & S/P_j \end{array}$$

in welchem die induzierte Abbildung

$$\varphi : A \longrightarrow B,\ A := R/p_j,\ B := S/P_j,$$

nach Induktionsvoraussetzung injektiv ist. Diese Abildung ist ebenfalls ganz. Das Ideal

$$p := \pi_R(p_{j+1}) \subset A$$

unter der surjektiven Abbildung π_R ist ein Primideal. Damit können wir auf die Abbildung

$$\varphi : A \longrightarrow B$$

und das Primideal $p \subset A$ wieder die Aussage von Lemma 3.3.8 anwenden. Wir erhalten ein Primideal $P \subset B$ mit

$$P \cap A = p.$$

Das Urbild

$$P_{j+1} := \pi_S^{-1}(P) \subset S$$

ist ein Primideal und erfüllt

$$P_{j+1} \cap R = p_{j+1},\ \text{q.e.d.}$$

3.3.10 Satz (Dimension)

i) Der Polynomring $k[X_1,...,X_n]$ hat die Krull-Dimension n.

ii) Die kombinatorische Dimension einer affinen Varietät ist identisch mit der Krull-Dimension ihres Koordinatenringes.

iii) Endliche Abbildungen sind dimensionstreu, d.h. bei einer endlichen regulären Abbildung zwischen zwei Varietäten

$$g : X \longrightarrow Y$$

gilt

$$\dim g(X) = \dim X.$$

Insbesondere gilt für eine Noethersche Normalisierung

$$X \longrightarrow \boldsymbol{A}_{\boldsymbol{K}}^{\boldsymbol{d}}$$

einer affinen Varietät X die Dimensionsgleichung

$$d = \dim(X).$$

Beweis. ad i) [GP2002], Theor. 3.5.1.

ad ii) Siehe Satz 3.3.6.

ad iii) Die Aussage folgt aus Satz 3.3.9.

*3.3.11 **Definition** (Nicht-singulärer Punkt)*

Eine irreduzible affine Varietät

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

heißt *nicht-singulär in einem Punkt* $p \in X$, wenn an dieser Stelle der Rang der Jacobi Matrix gleich der Codimension ist, d.h. für

$$I = \langle f_1,...,f_m \rangle \subset k[X_1,...,X_n]$$

gilt

$$rang\begin{pmatrix} \frac{df_1}{dX_1}(p) & ... & \frac{df_m}{dX_1}(p) \\ \vdots & & \vdots \\ \frac{df_1}{dX_n}(p) & ... & \frac{df_m}{dX_n}(p) \end{pmatrix} = n - \dim X .$$

Eine irreduzible Varietät heißt *nicht-singulär*, wenn sie in jedem Punkt nicht-singulär ist.

Die Definition der Nicht-Singularität ist unabhängig von dem gewählten Erzeugendensystem und sogar unabhängig von der gewählten Einbettung: Nicht-Singularität ist eine intrinsische Eigenschaft der Varietät.

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 der Algorithmen zum Rechnen mit Polynomen 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 im Rahmen der Gröbner Theorie ausgezeichneten Erzeugendensysteme heißen Gröbner Basen.

4.1 Divisions Algorithmus

Der Divisionsalgorithmus verallgemeinert den Euklidischen Divisionsalgorithmus auf den Fall von Polynomen mehrerer Veränderlicher. Mit Hilfe des Euklidische Divisionsalgorithmus läßt sich für den Polynomring in einer einzigen Veränderlichen entscheiden, ob ein Polynom zu einem gegebenen Ideal gehört oder nicht: Man dividiert durch ein erzeugendes Polynom des Hauptideals und betrachtet den Rest. Im Falle mehrerer Veränderlichen führt die analoge Fragestellung auf ein endliches Erzeugendensystem des Ideals. Man braucht daher einen Algorithmus, welcher den Rest einer simultanen Division durch mehrere Polynome berechnet. Dabei stellt sich allerdings heraus, daß der Rest der Division nicht eindeutig bestimmt ist.

Der Divisionsalgorithmus hat wie im Falle einer Veränderlichen zwei Schritte:

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

Die Auszeichung des Leitmonoms 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.

4.1.1 Definition (Monome und Terme)

Die *Monome* eines Polynomringes

$$R = k[X_1,...,X_n]$$

sind die Produkte der Form

$$X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot ... \cdot X_n^{\alpha_n}, \alpha_1,\alpha_2,...,\alpha_n \in \mathbf{N}.$$

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

$$\deg\left(X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot ... \cdot X_n^{\alpha_n}\right) := \sum_{j=1}^{n} \alpha_j .$$

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

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.

4.1.2 Definition (Monomiales Ideal)

Ein Ideal $I \subset k[X_1,...,X_n]$ heißt *monomiales* Ideal, wenn es ein Erzeugendensystem aus Monomen besitzt.

4.1.3 Bemerkung (Monome und Polynome)

i) Die Monome des Polynomringes $k[X_1,...,X_n]$ entsprechen bijektiv den Elementen

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

Dabei 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 $(\mathbf{N}^n, +)$ mit n Erzeugenden.

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

iii) 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.

4.1.4 Satz (Varietät eines monomiales Ideals)

Die Varietät eines monomialen Ideals ist eine endliche Vereinigung von Vektorräumen, d.h. für ein monomiales Ideal

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

hat die affine Varietät

$$X = Var(I)$$

eine Zerlegung in irreduzible Komponenten

$$X = \bigcup_{i=1}^{m} X_i$$

mit Untervektorräumen $X_i \subset K^n = \mathbf{A}_K^n, i = 1,...,m$.

Beweis. Sei

$$I = \langle f_1,..., f_k \rangle \text{ mit Monomen } f_j \in k[X_1,...,X_n],\ j = 1,...,k .$$

Dann gilt

$$X = Var(I) = \bigcap_{j=1}^{k} Var\left(\left\langle f_j \right\rangle\right).$$

Für das von einem Monom

$$f = X_{i_1}^{\alpha_1} \cdot X_{i_2}^{\alpha_2} \cdot \ldots \cdot X_{i_r}^{\alpha_r},\ \alpha_s \neq 0$$

erzeugte Ideal gilt

$$\left\langle f \right\rangle = \bigcap_{s=1}^{r} \left\langle X_{i_s}^{\alpha_s} \right\rangle,$$

also

$$Var\left(\left\langle f \right\rangle\right) = \bigcup_{s=1}^{r} Var\left(\left\langle X_{i_s}^{\alpha_s} \right\rangle\right) = \bigcup_{s=1}^{r} Var\left(\left\langle X_{i_s} \right\rangle\right),$$

und jede Varietät

$$Var\left(\left\langle X_{i_s} \right\rangle\right)$$

ist eine Hyperebene. Insgesamt ist

$$X = Var(I) = \bigcap_{j=1}^{k} Var\left(\left\langle f_j \right\rangle\right) = \bigcap_{j} \left(\bigcup_{s} H_{j,s}\right) = \bigcup_{s} \left(\bigcap_{j} H_{j,s}\right)$$

endliche Vereinigung eines endlichen Durchschnitts von Hyperebenen $H_{j,s}$, also Vereinigung endlich vieler Vektorräume, q.e.d.

4.1.5 Definition (Monomordnung)

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 $\left(\boldsymbol{N}^n, +\right)$)

Eine Monomordnung heißt *graduiert*, wenn gilt:

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

4.1.6 Beispiel (Monomordnung)

Die wichtigsten Monomordnungen des Polynomringes $R = k[X_1, \ldots, X_n]$ 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
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 $\gamma = (\gamma_1, \gamma_2, ..., \gamma\ ) := \alpha - \beta$ ist negativ	rp	RevLex
Graduiert rückwärts lexikographisch	• Entweder $\deg(\alpha) > \deg(\beta)$ • oder $\deg(\alpha) = \deg(\beta)$ und $\alpha >_{\mathrm{RevLex}} \beta$	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 $\alpha >_{G\,\mathrm{RevLex}} \beta$	(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.

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

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

$$X_1, ..., X_r$$

größer ist als jedes Momon, das nur die Variablen

$$X_{r+1}, ..., X_n$$

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

4.1.7 Definition (Leitmonom, Leitterm, Leitkoeffizient)

In einem Polynomring mit einer festen Monomordnung $(R = k[X_1,...,X_n],<)$ lassen sich die Terme eines Polynoms $f \in R$ über ihre Monome eindeutig nach absteigender Größe anordnen.

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

- das größte Monom das *Leitmonom* $LM(f)$,
- der zugehörige Term der *Leitterm* $LT(f)$
- und sein Koeffizient der *Leitkoeffizient* $LC(f)$:

$$LT(f) = LC(f) \cdot LM(f).$$

ii) Für ein Ideal $0 \neq I \subset k[X_1,...,X_n]$ bezeichnet man mit

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

das von den Leittermen der nicht-verschwindenden Elemente aus I erzeugte monomiale Ideal.

Durch eine gegebene Monomordnung wird auf der Menge $k[X_1,...,X_n]$ aller Polynome eine partielle Ordnung eingeführt.

4.1.8 Definition (Induzierte Ordnung im Polynomring)

Es sei $(M,>)$ die Menge aller Monome im Polynomring $k[X_1,...,X_n]$ 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 $f, g \in k[X_1,...,X_n]$ definieren wir die *partielle Ordnung* $f \leq g$ durch die Vorschrift:

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

Die Ordnung $(k[X_1,...,X_n],\leq)$ ist Noethersch, ebenso wie die vorgegebene Monomordnung, d.h. jede absteigende Folge von Elementen wird nach endlich vielen Schritten stationär.

4.1.9 **Bemerkung** *(Euklidischer Divisionsalgorithmus)*

Im Polynomring einer Veränderlichen ist jedes Ideal ein Hauptideal. Die Frage der Zugehörigkeit eines Polynoms zu einem gegebenen Ideal reduziert sich damit auf die Frage nach der Teilbarkeit zweier Polynome:

$$I = \langle g \rangle \subset k[X],$$

und für $f \in k[X]$ gilt

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

Um die Teilbarkeit zu prüfen, reduziert man f modulo g vermöge sukzessiver Probedivision durch den Leitterm von g nach dem Euklidischer Divisionsalgorithmus. Man erhält:

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

Dann entscheidet 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 $k[X_1,...,X_n]$ sind zwar weiterhin endlich erzeugt, aber benötigen i.a. ein Erzeugendensystem aus mehr als einem Element

$$I = \langle g_1,..., g_k \rangle \subset k[X_1,...,X_n].$$

Um die Zugehörigkeit eines Polynoms $f \in k[X_1,...,X_n]$ zu I zu klären, wird eine Reduktion von f nach der Menge $\{g_1,..., g_k\}$ gesucht, d.h. eine Darstellung

$$f = \sum_{i=1}^{k} a_i \cdot g_i + r \text{ mit } a_i, r \in k[X_1,...,X_n],$$

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

Man kann zunächst den Euklidischen Divisionsalgorithmus

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

erweitern zu einem Divisionsalgorithmus

$$f : \{g_1,..., g_k\} \text{ mit Polynomen } f, g_i \in k[X_1,...,X_n] \text{ mehrerer Veränderlicher.}$$

4.1.10 **Algorithmus** *(Division von Polynomen)*

Vorgegeben ein Polynomring und eine Monomordnung.

Input: Polynom f, Liste von Null verschiedener Polynomen $(g_1,..., g_k)$

Output: Polynom r, Liste von Polynomen $(a_1,...,a_k)$ mit folgenden Eigenschaften:

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

$r = 0,\ a_1 = ... = a_k = 0$		
$p = f$		
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:

$$p > p - \frac{LT(p)}{LT(g_i)}$$

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

4.1.11 Tool-Beispiel (Divisionsalgorithmus)

i) Für die Implementierung des Divisionsalgorithmus 4.1.10 mit Hilfe des Tools Macaulay2 siehe

- MyExamples/DivisionAlgorithm/Examples

ii) Trivialerweise ist die Bedingung $r = 0$ hinreichend für die Zugehörigkeit von f zum Ideal

$$\langle g_1,...,g_k \rangle .$$

Jedoch ist diese Bedingung nicht notwendig, und i.a. ist der Rest auch nicht eindeutig bestimmt. Im Polynomring $(k[X,Y], >_{Lex})$ soll festgestellt werden, ob das Polynom

$$f = X \cdot Y^2 - X$$

im Ideal

$$I := \langle g_1 = X \cdot Y + 1,\ g_2 = Y^2 - 1 \rangle$$

liegt. Es 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

$$f = Y \cdot g_1 - X - Y = Y \cdot g_1 + r .$$

Keiner der beiden Terme X bzw. Y ist durch $LT(g_1)$ oder $LT(g_2)$ teilbar. Daher terminiert der Divisionsalgortihmus mit dem von Null verschiedenen Rest

$$r = -Y - X .$$

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.

In der Tat gehört auch der Rest r zum Ideal I. Da sich in der Darstellung

$$r = -Y - X = -Y \cdot g_1 + X \cdot g_2 \in I$$

die Leitterme von g_1 und g_2 jedoch gegeneinander herausheben, läßt sich der Leitterm

$$LT(r) = -X$$

durch keinen der beiden Leitterme mehr dividieren. Der Leitterm $LT(r)$ liegt nicht in dem Ideal, das durch die Leitterme von g_1 und g_2 erzeugt wird:

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

4.2 Gröbner Basen

Der Algorithmus aus 4.1.10 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.

4.2.1 Definition *(Gröbner Basis)*

Eine endliche Menge

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

von Null verschiedener Elemente eines Ideals

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

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 4.1.10 folgt, daß jede Gröbner Basis eines Ideals auch das Ideal erzeugt:

4.2.2 Lemma *(Gröbner Basis)*

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

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

von Elementen eines Ideals

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

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 4.1.10 zur Berechnung von

$$f : G$$

mit einem Rest

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

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

$$LT(r) \in \langle\, LT(g_1), ..., LT(g_k) \,\rangle .$$

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 4.1.10 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.

4.2.3 Definition (Reduktion)

Eine endliche Menge $G \subset k[X_1, ..., X_n]$ nicht-verschwindender Polynome definiert auf der Menge $k[X_1, ..., X_n]$ 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 4.1.10 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.

4.2.4 Lemma (Translationslemma)

Es sei G eine endliche Menge nicht-verschwindender Polynome aus $k[X_1,...,X_n]$. Für zwei Polynome $f_1, f_2 \in k[X_1,...,X_n]$ gebe es eine Reduktion ihrer Differenz:

$$f_1 - f_2 \xrightarrow[G]{*} r \text{ für ein Polynom } r \in k[X_1,...,X_n].$$

Dann gibt es zwei Polynome

$$r_i \in k[X_1,...,X_n], i = 1, 2, \text{ mit } r_1 - r_2 = r$$

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

Term $t = c \cdot m$, Koeffizient $c = LC(t)$, Monom $u := \frac{m}{LM(g)}$ 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.

4.2.5 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 $f_1 \xleftrightarrow[G]{*} f_2$ 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

$$f_1 \xleftrightarrow[G]{*} f_2 + a_{k+1} \cdot g_{k+1} .$$

Es bleibt zu zeigen

$$f_2 + a_{k+1} \cdot g_{k+1} \xleftrightarrow[G]{*} f_2 .$$

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 4.2.4 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 4.2.5 läßt sich für den Fall einer Gröbner Basis wesentlich verschärfen zur Church-Rosser Eigenschaft der Reduktion. Zugleich zeigt der folgende Satz, daß der Divisionsalgorithmus 4.1.10 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.

4.2.6 Satz (Reduktion modulo einer Gröbner Basis)

Für eine endliche Menge G nicht-verschwindender Polynome aus $k[X_1,..., X_n]$ 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 4.2.5 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 4.2.5. 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 Gröbnerbasis: In welcher Reihenfolge man auch die einzelnen Divisionen ausführt, stets erhält man im Falle einer Gröbner Basis denselben Rest

$$r = r_1 = r_2 .$$

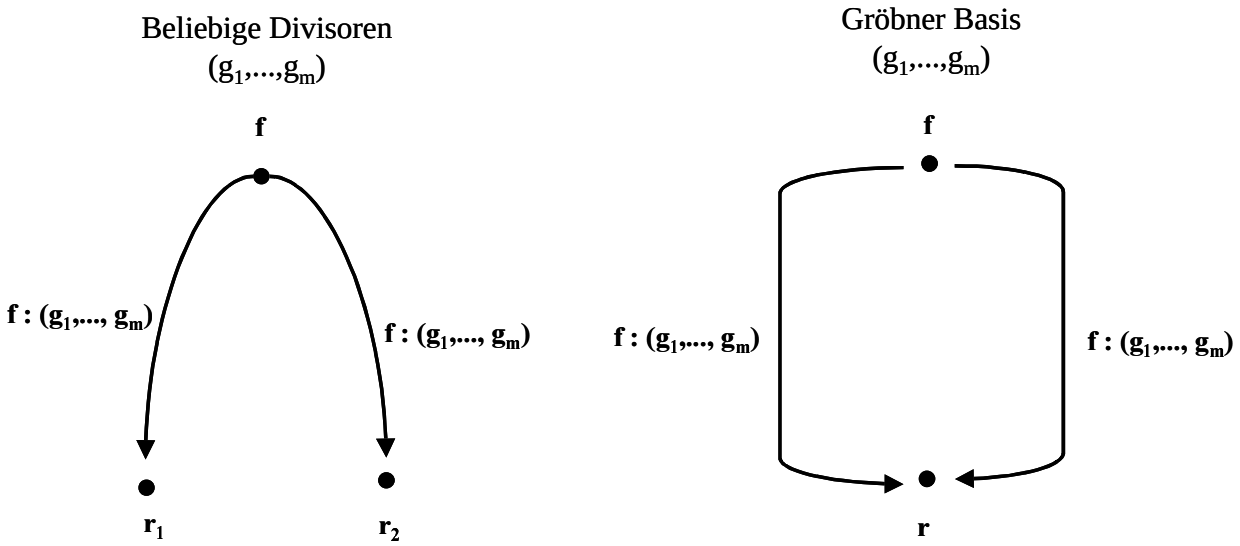


Abbildung 3: Unabhängigkeit des Restes bei Division durch Elemente einer Gröbner Basis

Beispiel 4.1.11 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.

4.2.7 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 dieses Buchberger Kriteriums in Satz 4.2.9 beweisen einen Hilfssatz.

4.2.8 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 4.2.6 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 4.2.4 folgt die Existenz zweier Reduktionen

$$f_i \xrightarrow[G]{*} r_i, i = 1, 2$$

mit einem eindeutig bestimmten Polynom

$$r_1 = r_2 \in k[X_1,..., X_n], \text{ q.e.d.}$$

4.2.9 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 4.2.6.

ii) Zum Beweis der Umkehrung wenden wir Lemma 4.2.8 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 4.2.8 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 $k[X_1,...,X_n]$.

4.2.10 *Algorithmus* (Buchberger)

Vorgegeben ein Polynomring mit Monomordnung.

Input: Endliche Menge $\{g_1,...,g_k\}$ von Elementen $0 \neq g_i \in k[X_1,...,X_n]$

Output: Gröbner Basis $G = \{g_1,..., g_k, g_{k+1},...,g_m\}$ des Ideals $\langle g_1,...,g_k \rangle \subset k[X_1,..., X_n]$

$G = \{g_1,...,g_k\}$		
	$G' = G$	
	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.

4.2.11 Tool-Beispiel (Gröbner Basis)

i) Algorithmus 4.2.10 berechnet für das Ideal

$$I := \langle g_1 = X \cdot Y + 1,\ g_2 = Y^2 - 1 \rangle \subset k[X, Y]$$

aus Beispiel 4.1.11 bzgl. der Lex-Ordnung die Gröbner Basis

$$G = \{g_1,\ g_2,\ X + Y\}.$$

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

$$G' = \{g_2,\ X + Y\}.$$

- „MyExamples/GroebnerBase/Examples“

4.3 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 4.2.10.
- Entscheidung der Zugehörigkeit eines Elementes zu dem erhaltenen Ideal durch eine Reduktion modulo G mit Hilfe des Divisionsalgorithmus 4.1.10.

In diesem Abschnitt bezeichne K den algebraischen Abschluß des Körpers k.

Die Zugehörigkeit zu einem Radikal läßt sich nach einem Trick von Rabinovitsch auf die Zugehörigkeit der Eins zu einem geeigneten erweiterten Ideal zurückführen.

4.3.1 Lemma *(Zugehörigkeit zu einem Radikal)*

Sei $I \subset k[X_1,...,X_n]$ ein Ideal. Dann gilt für ein Polynom $f \in k[X_1,...,X_n]$:

$$f \in \sqrt{I} \;\Leftrightarrow\; 1 \in I^e + \langle\, 1 - T \cdot f \,\rangle \subset k[X_1,...,X_n,T].$$

Dabei bedeutet

$$I^e := k[X_1,...,X_n,T] \cdot I \subset k[X_1,...,X_n,T]$$

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

$$1 \in I^e + \langle\, 1 - T \cdot f \,\rangle \subset k[X_1,...,X_n,T].$$

ii) Ohne Einschränkung sei $f \neq 0$. Dann existiert das Inverse

$$\frac{1}{f} \in k(X_1,...,X_n)\,.$$

Sei

$$I = \langle g_1,...,g_k \rangle \subset k[X_1,...,X_n].$$

Nach Voraussetzung existiert eine Darstellung

$$1 = \sum_{i=1}^{k} a_i(T)\cdot g_i + a_0(T)\cdot(1 - T\cdot f) \in k[X_1,...,X_n,T]$$

mit Elementen

$$a_i(T) \in k[X_1,...,X_n][T],\ i = 0,1,...,k\ .$$

Unter der kanonischen Abbildung

$$k[X_1,...,X_n][T] \longrightarrow k(X_1,...,X_n),\ T \mapsto \frac{1}{f}$$

geht obige Darstellung über in die Gleichung

$$1 = \sum_{i=1}^{k} a_i\left(\frac{1}{f}\right)\cdot g_i + a_0\left(\frac{1}{f}\right)\cdot\left(1 - \frac{1}{f}\cdot f\right) \in k(X_1,...,X_n),$$

d.h.

$$1 = \sum_{i=1}^{k} a_i\left(\frac{1}{f}\right)\cdot g_i \in k(X_1,...,X_n).$$

Nach Multiplikation mit einer genügend hohen Potenz f^m lassen sich alle Nenner eliminieren, so daß die Gleichung im Quotientenkörper

$$f^m = \sum_{i=1}^{k}\left(f^m \cdot a_i\left(\frac{1}{f}\right)\right)\cdot g_i \in k(X_1,...,X_n)$$

sogar schon eine Gleichung im Polynomring $k[X_1,...,X_n]$ ist, q.e.d.

4.3.2 Definition (Eliminationsideal)

Es sei $I \subset k[X_1,...,X_n]$ ein Ideal. Für eine Zahl $1 \le r < n$ heißt das Ideal

$$I_r := I \cap k[X_{r+1},...,X_n] \subset k[X_{r+1},...,X_n]$$

das *r-te Eliminationsideal* von I .

Das r -te Eliminationsideal enthält alle Elemente des Ideals, die nicht von den ersten r Variablen abhängen. Auf der Ebene der Varietäten entspricht der Elimination von Variablen die Projektion auf einen affinen Teilraum.

4.3.3 Lemma (Projektion und Elimination)

Es sei

$$X = Var(I) \subset \mathbb{A}_K^n$$

die affine Varietät eines Ideals $I \subset k[X_1,...,X_n]$. Mit $1 \le r < n$ gilt für die Projektion

$$pr : \boldsymbol{A}_K^n \longrightarrow \boldsymbol{A}_K^{n-r}, (x_1,...,x_n) \mapsto (x_{r+1},...,x_n)$$

längs der ersten r Koordinaten die Gleichung

$$\overline{pr(X)} = Var(I_r) \subset \boldsymbol{A}_K^{n-r}.$$

Beweis. Die Einschränkung der Projektion ist eine reguläre Abbildung

$$g : X \longrightarrow \boldsymbol{A}_K^{n-r}.$$

Für sie gilt nach Satz 2.2.6

$$\overline{g(X)} = Var(\ker \varphi_g) \subset \boldsymbol{A}_K^{n-r}$$

mit der induzierten Abbildung der Koordinatenringe

$$\varphi_g : k[X] = k[X_{r+1},...,X_n] \longrightarrow k[X_1,...,X_n]/I$$

die von der Inklusion

$$k[X_{r+1},...,X_n] \xrightarrow{\subset} k[X_1,...,X_n]$$

stammt. Offensichtlich gilt

$$\ker \varphi_g = k[X_{r+1},...,X_n] \cap I = I_r, \text{ q.e.d.}$$

Auch die Kerne allgemeinerer Morphismen in affine Algebren sind Eliminationsideale.

4.3.4 Satz (Kern von Morphismen in affine Algebren)

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

$$\ker \varphi = J_n \subset k[Y_1,...,Y_m]$$

für das n-te 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

$$J := I^e + \left\langle\ Y_j - \Phi_j\ :\ j = 1,...,m\ \right\rangle \subset k[X_1,...,X_n,Y_1,...,Y_m].$$

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

$$I_\Gamma := \left\langle\ Y_j - \Phi_j\ :\ j = 1,...,m\ \right\rangle \subset k[X_1,...,X_n,Y_1,...,Y_m].$$

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

$$\Gamma \subset \boldsymbol{A}_K^{n+m}$$

der zu Φ gehörigen regulären Abbildung

$$\boldsymbol{A}_K^n \longrightarrow \boldsymbol{A}_K^m,$$

dem Morphismus Φ^e entspricht die Einbettung

$$\boldsymbol{A}_K^n \xrightarrow{\cong} \Gamma \subset \boldsymbol{A}_K^{n+m}$$

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:

4.3.5 Satz (Gröbner Basis des Eliminationsideals)

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

$$G_r := G \cap k[X_{r+1},...,X_n]$$

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:

$$LT(I_r) = \langle\, LT(g) : g \in G_r \,\rangle.$$

i) Wegen $G_r \subset I_r$ gilt

$$LT(I_r) \supset \langle\, LT(g) : g \in G_r \,\rangle.$$

ii) Zum Beweis der Umkehrung

$$LT(I_r) \subset \langle\, LT(g) : g \in G_r \,\rangle$$

sei ein Polynom $f \in I_r$ vorgegeben. Da G eine Gröbner Basis von $I \supset I_r$ ist, gilt

$$LT(f) \in \langle\, LT(g) : g \in G \,\rangle.$$

Bei einem monomialen Ideal gilt dann

$$LT(f) \in \langle\, LT(g) \,\rangle \text{ für ein geeignetes } g \in G.$$

Da $f \in I_r$ keine der Variablen $X_1,...,X_r$ 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 $X_1,...,X_r$ enthält: Wenn ein Monom von g eine der Variablen $X_1,...,X_r$ enhielte, wäre dieses Monom bzgl. der Lex-Ordnung oder der r-ten Eliminationsordnung größer als jedes Monom aus $k[X_{r+1},...,X_n]$, insbesondere größer als das Leitmonom $LT(g)$, ein Widerspruch. Daher gilt $g \in k[X_{r+1},...,X_n]$, d.h.

$$g \in G_r, \text{ q.e.d.}$$

4.3.6 Tool-Beispiel (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 2.2.6 ist daher das Bild

$$Z := f\left(\boldsymbol{A}_K^1\right) \subset \boldsymbol{A}_K^3$$

abgeschlossen und die Einschränkung

$$f : \boldsymbol{A}_K^1 \longrightarrow Z \subset \boldsymbol{A}_K^3$$

ein regulärer Isomorphismus. Das Bild $Z \subset \boldsymbol{A}_K^3$ ist die affine Varietät zum Ideal

$$\ker \varphi = \left\langle X^2 - Y,\ X \cdot Y - Z,\ Y^2 - X \cdot Z \right\rangle \subset k[X,Y,Z].$$

Dieses Ideal wird überdies auch schon von 2 Elementen erzeugt:

$$\ker \varphi = \left\langle X^3 - Z,\ X^2 - Y \right\rangle \subset k[X,Y,Z]$$

Der Durchschnitt zweier Ideale ist ein geeignetes Eliminationsideal:

4.3.7 Lemma (Durchschnitt zweier Ideale)

Der Durchschnitt zweier Ideale $I_1, I_2 \subset k[X_1,...,X_n]$ ist das 1-Eliminationsideal

$$I_1 \cap I_2 = J_1 \subset k[X_1,...,X_n]$$

des Ideals

$$J := \langle T \cdot I_1 \rangle + \langle (1-T) \cdot I_2 \rangle \subset k[T, X_1,...,X_n].$$

Beweis. i) Die Inklusion

$$I_1 \cap I_2 \subset J_1$$

folgt aus der für beliebiges $f \in k[X_1,...,X_n]$ gültigen Darstellung

$$f = T \cdot f + (1-T) \cdot f \in k[T, X_1,...,X_n]$$

ii) Die Umkehrung

$$I_1 \cap I_2 \supset J_1$$

folgt, indem man in einer Darstellung

$$f(X_1,...,X_n) = a_1(T, X_1,...,X_n) \cdot T \cdot g_1(X_1,...,X_n) + a_2(T, X_1,...,X_n) \cdot (1-T) \cdot g_2(X_1,...,X_n),$$

$$g_i \in I_i \subset k[X_1,...,X_n],\ i = 1, 2,$$

sukzessive $T = 0$ bzw. $T = 1$ setzt, q.e.d.

Dem Durchschnitt zweier Ideale entspricht geometrisch die Vereinigung der zugehörigen Varietäten (siehe Bemerkung 2.1.6):

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

4.3.8 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 4.3.9 gilt insbesondere für den Fall eines Polynomringes R.

4.3.9 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.

4.3.10 Lemma (Komplement einer affinen Varietät)

Für die Varietäten zweier Ideale

$$I, J \subset k[X_1,...,X_n],\ I = \sqrt{I}\ \text{reduziert},$$

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

$$(f \cdot g_0)(x) = 0\text{, aber } g_0(x) \neq 0\text{,}$$

folgt $f(x) = 0$. Also gilt

$$f \in Id(\ Var(I) - Var(J)\ ).$$

ii) Beweis der umgekehrten Inklusion

$$Id(\ Var(I) - Var(J)\ ) \subset I : J\ .$$

Sei

$$f \in Id(\ Var(I) - Var(J)\ ).$$

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

$$f \cdot g \in Id(Var(I)).$$

Nach dem Hilbertschen Nullstellensatz (siehe Bemerkung 2.1.6) und der Voraussetzung über I gilt

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

und daher

$$f \cdot g \in I .$$

Es folgt

$f \cdot J \subset I$, d.h. $f \in I : J$, q.e.d.

4.3.11 Tool-Beispiel (Komplement einer affinen Varietät)

Macaulay2:

- MyExamples/IdealOperations/Examples

Aus der Varietät von Beispiel 3.2.12 entsteht durch Herausnahme der x-Achse die y/z-Ebene:

$$\overline{Var(\langle X \cdot Y, X \cdot Z \rangle)} - Var(\langle X, Y \rangle) = Var(\langle X \rangle).$$

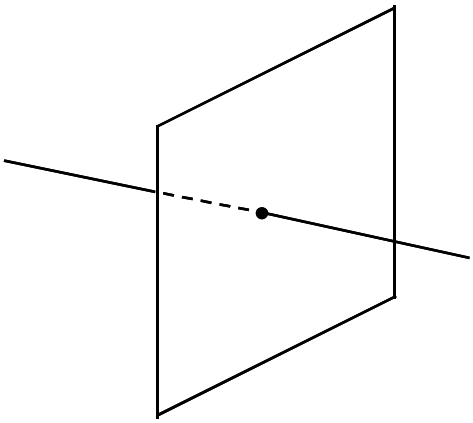


Abbildung 4: Y/Z-Ebene vereinigt mit X-Achse

5 Projektive Varietäten und graduierte Algebren

Affine Varietäten sind die ersten anschaulich gegebenen Objekte der Algebraischen Geometrie. Allerdings gelten global für affine Varietäten und ihre Morphismen nicht die einfachsten Aussagen. Es sind an verschiedenen Stellen Zusatzvoraussetzungen oder Fallunterscheidungen nötig.

Beispiele:

- Das Bild einer regulären Abbildung zwischen zwei affinen Varietäten ist wieder eine affine Varietät unter der Zusatzvoraussetzung der Endlichkeit der Abbildung.
- Zwei verschiedene Geraden der affinen Ebene sind entweder parallel, oder sie schneiden sich in genau einem Punkt.

Durch Abschließung des affinen Raumes zum projektiven Raum werden viele globale Sätze allgemeiner, Fallunterscheidungen werden überflüssig:

- Das Bild einer regulären Abbildung zwischen projektiven Varietäten ist wieder eine projektive Varietät.
- Zwei verschiedene Geraden in der projektiven Ebene schneiden sich in genau einem Punkt – im Falle paralleler Geraden der affinen Ebene ist der Schnittpunkt ein unendlich ferner Punkt.

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

5.1 Projektive Varietäten und reguläre Abbildungen

Der projektive Raum und projektive Varietäten lassen sich als Vervollständigung des affinen Raums bzw. von affinen Varietäten durch „fehlende“ unendlich ferne Punkte auffassen. Sie ähneln damit den kompakten Räumen in der Topologie. Da die Zariski Topologie jedoch keine Hausdorff Topologie ist, handelt es sich nur um eine Analogie.

5.1.1 Definition *(Projektiver Raum)*

Der *projektive Raum* $\boldsymbol{P}^n = \boldsymbol{P}_K^n$ ist der Quotient des punktierten affinen Raums $\boldsymbol{A}_K^{n+1} - 0$ nach der Äquivalenzrelation „liegt auf derselben Geraden durch den Nullpunkt“:

$$\boldsymbol{P}_K^n := \left(\boldsymbol{A}_K^{n+1} - 0 \right) / \sim$$

mit

$$x \sim y \text{ für } x, y \in \left(\boldsymbol{A}_K^{n+1} - 0 \right) :<=> \exists \lambda \in K^* \text{ mit } x = \lambda \cdot y .$$

5.1.2 Bemerkung *(Projektiver Raum)*

i) Die Äquivalenzklasse eines Punktes $x \in \boldsymbol{A}^{n+1} - 0$ ist die Menge aller von Null verschiedener Punkte auf der Geraden in $\boldsymbol{A}^{n+1}$, die durch x und durch den Nullpunkt geht.

Die Punkte des projektiven Raumes $\boldsymbol{P}^n$ entsprechen also bijektiv den Geraden durch den Nullpunkt des affinen Raumes $\boldsymbol{A}^{n+1}$.

Die Äquivalenzklasse

$$p = [\ x\ ] = [\ (x_0, x_1, ..., x_n)\ ] \in \boldsymbol{P}^n$$

bezeichnet man mit

$$p = (x_0 : x_1 : ... : x_n)$$

und nennt ein zugehöriges Tupel $(x_0, x_1, ..., x_n)$ *homogene Koordinaten* des Punktes p. Die homogenen Koordinaten eines Punktes sind nur bis auf einen gemeinsamen Faktor $\lambda \in K^*$ eindeutig bestimmt.

ii) Als Menge ist der projektive Raum $\boldsymbol{P}^n$ in natürlicher Weise die disjunkte Vereinigung des affinen Raumes

$$\boldsymbol{A}^n \xrightarrow{\cong} \{(x_0 : x_1 : x_2 : ... : x_n) \in \boldsymbol{P}^n : x_0 \neq 0\}, (x_1, x_2, ..., x_n) \mapsto (1 : x_1 : x_2 : ... : x_n)$$

und eines niederdimensionalen projektiven Raumes

$$\boldsymbol{P}^{n-1} \xrightarrow{\cong} \{(x_0 : x_1 : x_2 : ... : x_n) \in \boldsymbol{P}^n : x_0 = 0\}, (x_0 : x_1 : ... : x_{n-1}) \mapsto (0 : x_0 : x_1 : ... : x_{n-1})$$

d.h.

$$\boldsymbol{P}^n = \boldsymbol{A}^n \dot{\cup} \boldsymbol{P}^{n-1}.$$

Insbesondere entsteht die projektive Gerade $\boldsymbol{P}^1$ aus der affinen Geraden $\boldsymbol{A}^1$ durch Hinzunahme eines einzigen Punktes

$$\boldsymbol{P}^0 = \{(0:1)\}.$$

Aus Sicht der affinen Geraden ist dieser Punkt der unendlich ferne Punkt

$$\infty = (0:1) \in \boldsymbol{P}^1.$$

Analog ist die projektive Ebene $\boldsymbol{P}^2$ die Vervollständigung der affinen Ebene $\boldsymbol{A}^2$ durch die unendlich ferne projektive Gerade

$$\boldsymbol{P}^1 \cong \{(z_0 : z_1 : z_2) \in \boldsymbol{P}^2 : z_0 = 0\}.$$

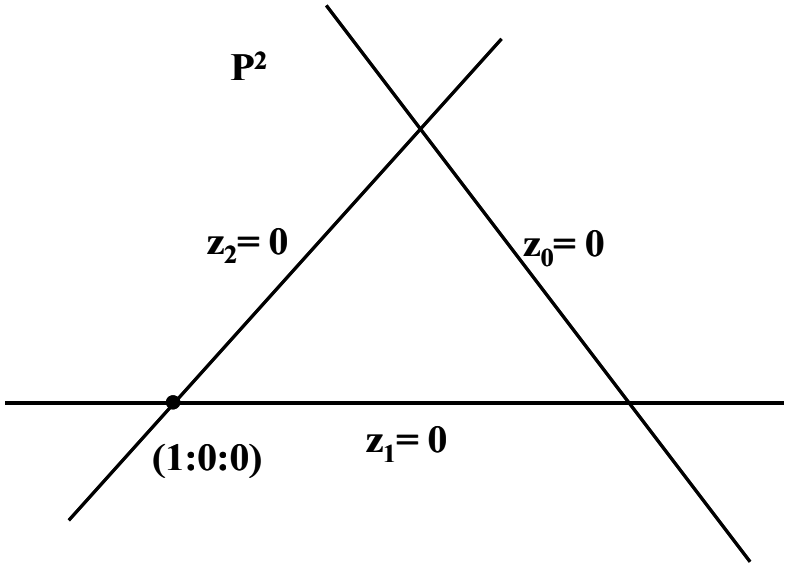


Abbildung 5: Projektive Ebene mit unendlich ferner Geraden

Polynome lassen sich i.a. nicht als Funktionen auf dem projektiven Raum auffassen, da ihr Funktionswert in einem gegebenem Punkt des projektiven Raumes von dem gewählten Repräsentanten des Punktes abhinge. Bei einer wichtigen Teilklasse, der Klasse der *homogenen* Polynome, läßt sich aber noch die Alternative entscheiden, ob das Polynom in einem Punkt des projektiven Raumes verschwindet oder nicht. Homogene Polynome haben daher ein wohldefiniertes Nullstellengebilde im projektiven Raum. Sie definieren projektive Varietäten.

5.1.3 Definition (Homogenes Polynom, homogenes Ideal)

i) Ein Polynom $f \subset k[X_0, X_1, ..., X_n]$ heißt *homogen vom Grad* $d \in \boldsymbol{N}$, wenn alle seine Terme vom Grad d sind.

ii) Ein Ideal $I \subset k[X_0, X_1, ..., X_n]$ heißt *homogen*, wenn es ein Erzeugendensystem aus homogenen Polynomen besitzt.

Die Erzeuger eines homogenen Ideals dürfen unterschiedliche Grade haben.

5.1.4 Bemerkung (Homogenes Polynom, homogenes Ideal)

i) Im Falle eines unendlichen Körpers k gilt die Äquivalenz: Ein Polynom ist genau dann homogen vom Grad d, wenn für alle $x \in k^{n+1}$ und für alle $\lambda \in k^*$ gilt:

$$f(\lambda \cdot x) = \lambda^d \cdot f(x).$$

ii) Jedes Polynom

$$f \in k[X_0, X_1, ..., X_n]$$

hat eine eindeutige Summendarstellung

$$f = \sum_{i=0}^{d} f_i$$

mit homogenen Polynomen $0 \neq f_i \in k[X_0, X_1, ..., X_n]$ des Grades i, seinen *homogenen Komponenten* vom Grad i. Das Polynom f gehört genau dann zu einem homogenen Ideal

$$I \subset k[X_0, X_1, ..., X_n],$$

wenn jede seiner homogenen Komponenten zu I gehört.

iii) Die reduzierte Gröbner Basis eines homogenen Ideals besteht aus homogenen Polynomen.

iv) Das Radikal eines homogenen Ideals ist wieder ein homogenes Ideal.

Beweis. ad iii) siehe [CLO1997], Chap.7, §3, Theor. 2.

5.1.5 Definition (Projektive Varietät)

Eine *projektive k-Varietät* X ist das gemeinsame Nullstellengebilde einer Familie homogener Polynome

$$f_j \in k[X_0, X_1, ..., X_n],\ j \in J,$$

im projektiven Raum $\boldsymbol{P}_K^n$. Die definierenden Polynome dürfen unterschiedliche Grade haben. Für die Varietät als Teilmenge von $\boldsymbol{P}_K^n$ schreibt man

$$X = \{(x_0 : ... : x_n) \in \boldsymbol{P}_K^n : f_j(x_0, ..., x_n) = 0 \text{ für alle } j \in J\}.$$

Da alle Polynome f_j homogen sind, gilt die Eigenschaft

$$f_j(x_0, x_1, ..., x_n) = 0,\ j \in J,$$

unabhängig vom gewählten Repräsentanten des Punktes $p = [(x_0, x_1, ..., x_n)]$.

5.1.6 Bemerkung (Projektive Varietät und homogenes Ideal)

i) Einem homogenen Ideal

$$I \subset k[X_0, X_1, ..., X_n]$$

wird die projektive Varietät zugeordnet

$$Var(I) := \{(x_0 : ... : x_n) \in \boldsymbol{P}^n : f(x_0, ..., x_n) = 0 \text{ für alle homogenen } f \in I\}.$$

Dabei definiert neben dem Einheitsideal

$$\langle 1 \rangle \subset k[X_0, X_1, ..., X_n]$$

auch schon das *irrelevante* homogene Ideal

$$m := \langle X_0, X_1, ..., X_n \rangle \subset k[X_0, X_1, ..., X_n]$$

die leere projektive Varietät

$$\varnothing = Var(m) \subset \boldsymbol{P}^n .$$

ii) Einer projektiven Varietät $X \subset \boldsymbol{P}^n$ wird als homogenes Ideal ihr *Verschwindungsideal* zugeordnet

$$Id(X) := \langle f \in k[X_0, ..., X_n] : f \text{ homogen und } f(x_0, ..., x_n) = 0 \text{ für alle } (x_0 : ... : x_n) \in X \rangle .$$

Wegen der Noether-Eigenschaft des Polynomringes läßt sich die Varietät eines homogenen Ideals bereits durch endlich viele homogene Polynome definieren.

5.1.7 Definition (Homogener Koordinatenring)

Für eine projektive Varietät $X \subset \boldsymbol{P}^n$ heißt der Quotientenring

$$S(X) := k[X_0, X_1, ..., X_n] / Id(X)$$

der *homogene Koordinatenring* der Einbettung

$$X \xrightarrow{\subset} \boldsymbol{P}^n .$$

Über einem algebraisch-abgeschlossenen Grundkörper folgt aus dem Hilbertschen Nullstellensatz und der Tatsache, daß das Radikal eines homogenen Ideals wieder homogen ist, ähnlich wie im affinen Fall die Charakterisierung projektiver Varietäten durch ihr Verschwindungsideal:

5.1.8 Satz (Projektive Varietäten und homogene Ideale)

Die beiden folgenden Zuordnungen sind zueinander invers:

$$\left\{ I \subset k[X_0, ..., X_n] : \text{homogen}, I \neq m, \sqrt{I} = I \right\} \underset{Id}{\overset{Var}{\rightleftarrows}} \left\{ X \subset \boldsymbol{P}^n : \text{projektive } k-\text{Varietät} \right\}$$

Es gilt

$$Var\left(\sum_j I_j \right) = \bigcap_j Var(I_j), \ j \in J \text{ beliebig},$$

$$\text{und } Var\left(\bigcap_j I_j \right) = \bigcup_j Var(I_j), \ j \in J \text{ endlich}$$

Beweis. siehe [CLO1997], Chap. 8, §3, Theor. 10 und Ex. 7.

5.1.9 Definition (Zariski Topologie)

Die *Zariski-Topologie* des projektiven Raumes $\boldsymbol{P}_K^n$, aufgefaßt als projektive k-Varietät, ist die eindeutig bestimmte Topologie mit den projektiven k-Varietäten des $\boldsymbol{P}^n$ als abgeschlossenen Mengen.

Die Zariski-Topologie einer projektiven k-Varietät $X \subset \boldsymbol{P}_K^n$ ist die induzierte Unterraumtopologie: Genau die Mengen der Form

$$X \cap A \text{ mit einer Zariski-abgeschlossenen Teilmenge } A \subset \boldsymbol{P}_K^n$$

sind nach Definition die abgeschlossenen Mengen von X.

Offene Teilmengen einer projektiven Varietät heißen *quasi-projektiv*.

Eine reguläre Abbildung zwischen zwei projektiven k-Varietäten ist eine Abbildung, die *lokal* durch homogene Polynome ohne gemeinsame Nullstelle gegeben werden kann. Anders als im affinen Falle fordert man im projektiven Falle nicht die globale Gültigkeit der Polynomdarstellung.

5.1.10 Definition (Reguläre Abbildung)

Eine *k-reguläre Abbildung* zwischen zwei projektiven k-Varietäten $X \subset \boldsymbol{P}^n$ und $Y \subset \boldsymbol{P}^m$ ist eine Abbildung

$$g : X \longrightarrow Y,$$

mit folgender Eigenschaft: Zu jedem Punkt $p \in X$ existieren eine offene Umgebung U von p und $m+1$ homogene Polynome eines festen Grades d

$$g_i \in k[X_0, X_1, ..., X_n],\ \deg g_i = d, i = 0, 1, ..., m,$$

ohne gemeinsame Nullstelle in U mit

$$g(x_0 : ... : x_n) = (g_0(x_0, ..., x_n) : ... : g_m(x_0, ..., x_n)) \text{ für alle } (x_0 : ... : x_n) \in U.$$

5.1.11 Beispiel (Stereographische Projektion)

Die stereographische Projektion entspringt im Rellen, der Grundkörper ist $k = \boldsymbol{R}$. Statt über dem algebraischen Abschluß $K = \boldsymbol{C}$ werden wir in den ersten beiden Abschnitten dieses Beispiels die Nullstellengebilde als Teilmengen des reellen affinen Raumes

$$\boldsymbol{A}^{n+1} = \boldsymbol{A}_{\boldsymbol{R}}^{n+1} := \boldsymbol{R}^{n+1}$$

bzw. des rellen projektiven Raumes

$$\boldsymbol{P}^n = \boldsymbol{P}_{\boldsymbol{R}}^n := \left(\boldsymbol{R}^{n+1} - 0\right) / \sim$$

betrachten. Alle verwendeten Begriffe gelten analog auch für diesen Fall.

Bei der stereographischen Projektion des Einheitskreises auf eine Geraden handelt es sich um eine Abbildung, die auf einem offenen Teil einer affinen Varietät definiert ist und zu einer

regulären Abbildung zwischen den zugehörigen projektiven Varietäten fortgesetzt werden kann.

i) Es sei

$$C := \{(x, y) \in \boldsymbol{A}^2 : 1 = x^2 + y^2 \}$$

der reelle Einheitskreis mit einem ausgezeichneten Punkt

$$N := (0, 1) \in C .$$

Wir definieren als die stereographische Projektion des Kreises C vom Punkt N auf die x-Achse $\boldsymbol{A}^1$ die Abbildung

$$g : C - N \longrightarrow \boldsymbol{A}^1, (x, y) \mapsto \frac{x}{1-y}.$$

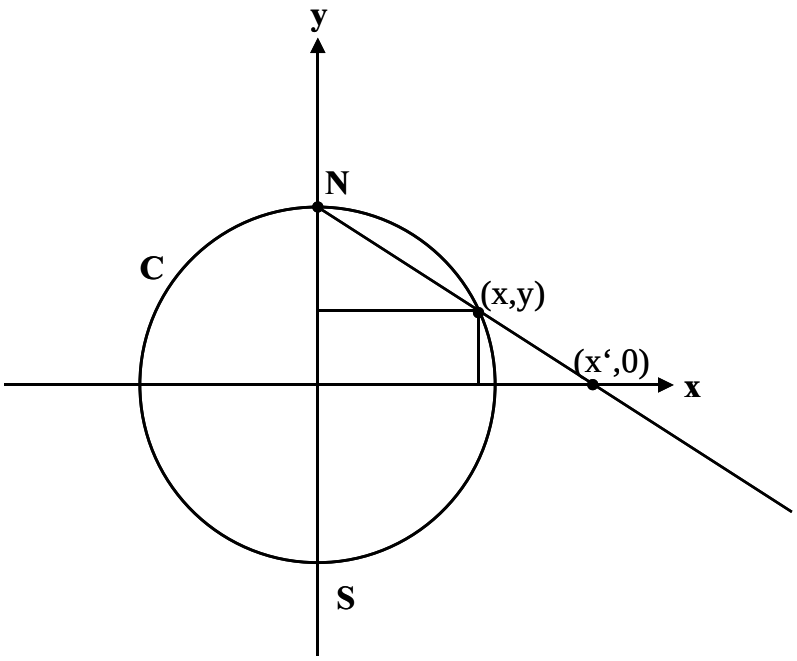


Abbildung 6: Stereographische Projektion

Nach dem Strahlensatz, siehe Abbildung 6, gilt

$$\frac{1-y}{1} = \frac{x}{x'},$$

also

$$x' = \frac{x}{1-y} \text{ und } x' = \frac{x}{1-y} = \frac{1+y}{x} \text{ für } (x, y) \neq S .$$

Der Funktionswert der Umkehrabbildung

$$h : \boldsymbol{A}^1 \longrightarrow C - N, x' \mapsto (x, y)$$

berechnet sich aus

$$x = x' \cdot (1 - y) = x' \cdot \left(1 - \sqrt{1 - x^2}\right)$$

als

$$x = \frac{2 \cdot x'}{x'^2 + 1},\ y = \frac{x'^2 - 1}{x'^2 + 1}.$$

ii) Die bisher im Affinen definierte stereographische Projektion läßt sich fortsetzen zu einer regulären Abbildung zwischen projektiven Varietäten. Gesucht werden eine projektive Varietät

$$Q \subset \boldsymbol{P}^2$$

und eine reguläre Abbildung zwischen projektiven Varietäten

$$G : Q \longrightarrow \boldsymbol{P}^1,$$

so daß folgendes Diagramm kommutiert:

$$\begin{array}{ccccc} \boldsymbol{A}^2 & \xleftarrow{\supset} & C - N & \xrightarrow{g} & \boldsymbol{A}^1 \\ \downarrow\subset & & \downarrow\subset & & \downarrow\subset \\ \boldsymbol{P}^2 & \xleftarrow{\supset} & Q & \xrightarrow{G} & \boldsymbol{P}^1 \end{array}$$

Dazu fassen wir im Definitionsbereich von G die affine Ebene als Teilmenge der projektiven Ebene auf

$$\boldsymbol{A}^2 \xrightarrow{\subset} \boldsymbol{P}^2,\ (x, y) \mapsto (1 : x : y)$$

und identifizieren den affinen Einheitskreis $C \subset \boldsymbol{A}^2$ mit seinem Bild, der projektiven Quadrik

$$Q := \left\{ (x_0 : x_1 : x_2) \in \boldsymbol{P}^2 : x_0^2 = x_1^2 + x_2^2 \right\} \subset \boldsymbol{P}^2.$$

Im Wertebereich von G fassen wir die affine x-Achse als Teilmenge der projektiven Geraden auf

$$\boldsymbol{A}^1 \xrightarrow{\subset} \boldsymbol{P}^1,\ v \mapsto (1 : v).$$

Wie läßt sich die gegebene Abbildung g zu einer regulären Abbildung

$$G : Q \longrightarrow \boldsymbol{P}^1$$

fortsetzen? Heuristik: Die stereographische Projektion

$$g : C - N \longrightarrow \boldsymbol{A}^1,\ (x, y) \mapsto \frac{x}{1 - y}$$

schreibt sich bzgl. der üblichen Einbettungen

$$C - N \xrightarrow{\subset} Q \subset \boldsymbol{P}^2 \text{ und } \boldsymbol{A}^1 \xrightarrow{\subset} \boldsymbol{P}^1$$

als

$$g : C - N \longrightarrow \boldsymbol{A}^1, (1 : x_1 : x_2) \mapsto \left(1 : \frac{x_1}{1 - x_2}\right) = (1 - x_2 : x_1).$$

Diese Definition wird nun „homogenisiert“, d.h. in homogenen Koordinaten und unter Verwendung homogener Polynome geschrieben:

$$g : C - N \longrightarrow \boldsymbol{A}^1, (x_0 : x_1 : x_2) \mapsto (x_0 - x_2 : x_1).$$

In dieser Form läßt sie sich in den Punkt $N = (1 : 0 : 1)$ hinein jedoch nicht fortsetzen.

Gemäß Definition 5.1.10 überdecken wir den Definitionsbereich Q durch die beiden offenen Teilmengen

$$U_0 := Q - N = Q - (1 : 0 : 1) \text{ und } U_1 := Q - S = Q - (1 : 0 : -1)$$

und definieren jeweils lokal

$$G_0 : U_0 \longrightarrow \boldsymbol{P}^1, (x_0 : x_1 : x_2) \mapsto (x_0 - x_2 : x_1),\ G_1 : U_1 \longrightarrow \boldsymbol{P}^1, (x_0 : x_1 : x_2) \mapsto (x_1 : x_0 + x_2).$$

Hierdurch ist eine reguläre Abbildung

$$G : Q \longrightarrow \boldsymbol{P}^1$$

wohldefiniert. Denn im Durchschnitt

$$U_0 \cap U_1 \subset Q$$

gilt unter Benutzung der definierenden Gleichung $x_0^2 = x_1^2 + x_2^2$:

$$\frac{x_1}{x_0 - x_2} = \frac{x_1 \cdot (x_0 + x_2)}{(x_0 - x_2) \cdot (x_0 + x_2)} = \frac{x_1 \cdot (x_0 + x_2)}{x_0^2 - x_2^2} = \frac{x_1 \cdot (x_0 + x_2)}{x_1^2} = \frac{x_0 + x_2}{x_1}.$$

Insbesondere gilt

$$G(S) = G_0(S) = (1 : 0)$$

und

$$G(N) = G_1(N) = (0 : 1), \text{ unendlich ferner Punkt.}$$

Die reguläre Abbildung

$$G : Q \longrightarrow \boldsymbol{P}^1$$

ist ein Isomorphismus der Quadrik auf die projektive Gerade mit der Umkehrabbildung

$$H : \boldsymbol{P}^1 \longrightarrow Q, (u : v) \mapsto (v^2 + u^2 : 2uv : v^2 - u^2).$$

Denn es gilt:

$$G \circ H = id_{\boldsymbol{P}^1} \text{ und } H \circ G = id_Q.$$

iii) Im projektiven Zusammenhang ist die Definition der regulären Abbildungen G und H sowie der zugehörigen Varietäten nicht mehr an die rellen Zahlen gebunden. Beide

Abbildungen lassen sich vielmehr durch die angegebenen Formeln für jeden Grundkörper k, $char\ k \neq 2$, und die zugehörigen Varietäten über $K = \bar{k}$ definieren. Beide Abbildungen sind zueinander inverse reguläre Abbildungen. Sie stellen einen regulären Isomorphismus der Quadrik und der projektiven Gerade dar. Dennoch sind die homogenen Koordinatenringe beider Varietäten

$$S(\boldsymbol{P}^1) = k[X_0, X_1] \text{ und } S(Q) = k[X_0, X_1, X_2] \Big/ \left\langle X_0^2 - X_1^2 - X_2^2 \right\rangle$$

nicht isomorph.

*5.1.12 **Beispiel** (Reguläre Abbildung)*

i) Die Projektivierung der affinen kubischen Kurve, siehe Beispiel 4.3.6, ist die projektive kubische Kurve *(twisted cubic curve)*

$$f : \boldsymbol{P}^1 \longrightarrow \boldsymbol{P}^3,$$

die global definiert ist durch die homogenen Polynome vom Grad 3

$$f(t_0 : t_1) := \left(t_0^3 : t_0^2 t_1 : t_0 t_1^2 : t_1^3 \right).$$

Denn die Einschränkung auf die affine Gerade

$$\boldsymbol{A}^1 = \left\{ (1 : t) \in \boldsymbol{P}^1 \right\}$$

ist die Abbildung

$$f \mid \boldsymbol{A}^1 \longrightarrow \boldsymbol{A}^3 \subset \boldsymbol{P}^3,\ (1 : t) \mapsto (1 : t : t^2 : t^3).$$

Zu den affinen Punkten kommt im Projektiven ein einziger weiterer Punkt hinzu:

$$f(0 : 1) := (0 : 0 : 0 : 1).$$

Das Bild

$$Z := f\left(\boldsymbol{P}^1\right) \subset \boldsymbol{P}^3$$

wird als projektive Varietät

$$Z = Var(I) \subset \boldsymbol{P}^3$$

durch das homogene Ideal

$$I = \left\langle X_2^2 - X_1 X_3,\ X_1 X_2 - X_0 X_3,\ X_1^2 - X_0 X_2 \right\rangle = \left\langle X_1 X_2 - X_0 X_3, X_1^2 - X_2 X_0 \right\rangle \subset k[X_0, \ldots, X_3]$$

definiert. Dieses Ideal wird erzeugt von den 2x2-Minoren der Matrix

$$\begin{pmatrix} X_0 & X_1 & X_2 \\ X_1 & X_2 & X_3 \end{pmatrix}.$$

Die Einschränkung

$$f : \boldsymbol{P}^1 \longrightarrow Z \subset \boldsymbol{P}^3$$

ist ein regulärer Isomorphismus: Die Umkehrabbildung ist die reguläre Abbildung

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

die auf der offenen Teilmenge

$$U_0 := \{ (x_0 : x_1 : x_2 : x_3) \in Z : x_0 \neq 0 \}$$

definiert ist als

$$g_0 : U_0 \longrightarrow \boldsymbol{P}^1, (x_0 : x_1 : x_2 : x_3) \mapsto (x_0 : x_1)$$

und auf der offenen Teilmenge

$$U_3 := \{ (x_0 : x_1 : x_2 : x_3) \in Z : x_3 \neq 0 \}$$

als

$$g_3 : U_3 \longrightarrow \boldsymbol{P}^1, (x_0 : x_1 : x_2 : x_3) \mapsto (x_2 : x_3).$$

Es gilt

$$Z = U_0 \cup U_3 \text{ und } g_0 \,|\, U_0 \cap U_3 = g_3 \,|\, U_0 \cap U_3 .$$

ii) Die *Veronese Abbildung*

$$f : \boldsymbol{P}^2 \longrightarrow \boldsymbol{P}^5$$

ist die reguläre Abbildung, die global durch die quadratischen homogenen Polynome

$$f(t_0 : t_1 : t_2) := (t_0^2 : t_0 t_1 : t_0 t_2 : t_1^2 : t_1 t_2 : t_2^2)$$

gegeben ist. Das Bild

$$Z := f(\boldsymbol{P}^2) \subset \boldsymbol{P}^5$$

wird als projektive Varietät

$$Z = Var(I) \subset \boldsymbol{P}^5$$

durch das homogene Ideal

$$I = \langle X_4^2 - X_3 X_5, X_2 X_4 - X_1 X_5, X_2 X_3 - X_1 X_4, X_2^2 - X_0 X_5, X_1 X_2 - X_0 X_4, X_1^2 - X_0 X_3 \rangle \subset k[X_0, ..., X_5]$$

definiert. Die Einschränkung

$$f : \boldsymbol{P}^2 \longrightarrow \mathrm{Z} \subset \boldsymbol{P}^5$$

ist ein regulärer Isomorphimus: Die reguläre Umkehrabbildung

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

wird lokal auf jeder der drei offenen Teilmengen

$$U_i := \{ (x_0 : x_1 : x_2 : x_3 : x_4 : x_5) \in Z : x_i \neq 0, \}, i = 0, 3, 5,$$

durch die zugehörige Abbildung

$$g_0 : U_0 \longrightarrow \boldsymbol{P}^2, (x_0 : x_1 : x_2 : x_3 : x_4 : x_5) \mapsto (x_0 : x_1 : x_2)$$

$$g_3 : U_3 \longrightarrow \boldsymbol{P}^2, (x_0 : x_1 : x_2 : x_3 : x_4 : x_5) \mapsto (x_1 : x_3 : x_4)$$

$$g_5 : U_5 \longrightarrow \boldsymbol{P}^2, (x_0 : x_1 : x_2 : x_3 : x_4 : x_5) \mapsto (x_2 : x_4 : x_5)$$

gegeben.

iii) Die global durch homogene quadratische Polynome definierte Abbildung

$$f : \boldsymbol{P}^n \times \boldsymbol{P}^m \longrightarrow \boldsymbol{P}^N, N = (n+1)\cdot(m+1)-1$$

$$((x_0 : \ldots : x_n), (y_0 : \ldots : y_m)) \mapsto (x_0 y_0 : \ldots : x_0 y_m : \ldots : x_n y_0 : \ldots x_n y_m) = (z_{ij} := x_i y_j)_{0 \le i \le n, 0 \le j \le m}$$

heißt *Segre Abbildung*. Sie dient dazu, das Produkt $\boldsymbol{P}^n \times \boldsymbol{P}^m$ zweier projektiver Räume als projektive Varietät in $\boldsymbol{P}^N$ darzustellen. Dazu zeigen wir, daß die Segre Abbildung eine injektive Abbildung mit abgeschlossenem Bild

$$Z := f(\boldsymbol{P}^n \times \boldsymbol{P}^m) \subset \boldsymbol{P}^N$$

ist. Wir fassen

$$\boldsymbol{P}^N := [M(n+1 \times m+1, K) - 0] / \sim$$

als den Quotienten aller von Null verschiedener Matrizen auf. Die Segre Abbildung wird dann von dem Matrizenprodukt zweier Vektoren

$$K^{n+1} \times K^{m+1} \longrightarrow M(n+1 \times m+1, K), (x, y) \mapsto x \cdot y^T .$$

durch Übergang zu den Äquivalenzklassen induziert. Nun sind für eine nichtverschwindende Matrix

$$A \in M(n+1 \times m+1, K)$$

äquivalent:

- $A = x \cdot y^T$ mit Vektoren $x,\ y \neq 0$
- $rang\ A = 1$

Die letzte Bedingung bedeutet, daß die Determinanten aller 2-Minoren von A verschwinden. Die Determinante eines gegebenen 2-Minors ist ein homogenes Polynom in den Koeffizienten der Matrix. Daher wird durch die Bedingung

$$rang\ A = 1$$

das Bild der Segre Abbildung

$$Z \subset \boldsymbol{P}^N := [M(n+1 \times m+1, K) - 0] / \sim$$

als projektive Varietät definiert.

Zur Injektivität der Segre Abbildung: Aus einer Gleichung

$$x \cdot y^T = \lambda \cdot x' \cdot y'^T \neq 0 \text{ für ein } \lambda \in K^*$$

folgt die Existenz eines Index i_0 mit

$$x \cdot y_{i_0} = \lambda \cdot x' \cdot y'_{i_0} \neq 0 \text{, also } x \cdot = \lambda \cdot \frac{y'_{i_0}}{y_{i_0}} \cdot x',$$

und die Existenz eines Index j_0 mit

$$x_{j_0} \cdot y = \lambda \cdot x'_{j_0} \cdot y' \neq 0 \text{, also } y \cdot = \lambda \cdot \frac{x'_{j_0}}{x_{j_0}} \cdot y'.$$

Vermöge der Segre Abbildung

$$f : \boldsymbol{P}^n \times \boldsymbol{P}^m \xrightarrow{\cong} Z \subset \boldsymbol{P}^N, N = (n+1) \cdot (m+1) - 1$$

überträgt man die Zariski Topologie der projektiven Varietät $Z \subset \boldsymbol{P}^N$ auf das Produkt der beiden projektiven Räume $\boldsymbol{P}^n \times \boldsymbol{P}^m$. Die resultierende Topologie heißt die *Zariski Topologie* des Produktes $\boldsymbol{P}^n \times \boldsymbol{P}^m$. Bezüglich dieser Topologie faßt man

$$\boldsymbol{P}^n \times \boldsymbol{P}^m$$

als projektive Varietät auf. Die Zariski Topologie des Produktes ist i.a. echt feiner als das Produkt der Zariski Topologien beider Faktoren.

Im Spezialfall $n = 1, m = 1$ hat die Segre Abbildung

$$f : \boldsymbol{P}^1 \times \boldsymbol{P}^1 \longrightarrow \boldsymbol{P}^3$$

die Gestalt

$$f((x_0 : x_1), (y_0 : y_1)) := (x_0 y_0 : x_0 y_1 : x_1 y_0 : x_1 y_1).$$

Ihr Bild ist die quadratische Hyperfläche

$$Z = Var(I) \subset \boldsymbol{P}^3$$

zum Ideal

$$I := \langle Z_0 Z_3 - Z_1 Z_2 \rangle \subset k[Z_0, Z_1, Z_2, Z_3],$$

Man erhält eine Darstellung des Produktes zweier projektiver Geraden als eine quadratische Hyperfläche

$$f : \boldsymbol{P}^1 \times \boldsymbol{P}^1 \xrightarrow{\cong} Z \subset \boldsymbol{P}^3.$$

iv) Die projektive Ebene $\boldsymbol{P}^2$ läßt sich gemäß Abbildung 5 veranschaulichen als Abschluß der affinen Ebene $\boldsymbol{A}^2$ durch die unendlich ferne Gerade

$$Var(\langle Z_0 \rangle) \subset \boldsymbol{P}^2.$$

Der Punkt $(1:0:0) \in \boldsymbol{P}^2$ ist der Nullpukt der affinen Ebene. In Verallgemeinerung des affinen Blow-up aus Beispiel 2.1.4, Teil iii) bilden die Geraden in der projektiven Ebene $\boldsymbol{P}^2$, welche durch den Punkt $(1:0:0) \in \boldsymbol{P}^2$ gehen, die projektive Varietät

$$Z := \{ ((x_0 : x_1 : x_2), (z_0 : z_1)) \in \boldsymbol{P}^2 \times \boldsymbol{P}^1 : z_0 \cdot x_2 - z_1 \cdot x_1 = 0 \},$$

das *Blow-up* von $\boldsymbol{P}^2$ im Punkt $(1:0:0)\in \boldsymbol{P}^2$. Die erste Projektion induziert eine reguläre Abbildung

$$f : Z \longrightarrow \boldsymbol{P}^2, (x,z) \mapsto x .$$

Das Urbild

$$E := f^{-1}(1:0:0) \subset Z$$

heißt die *exzeptionelle Gerade* des Blow-up. Sie läßt sich unter der zweiten Projektion

$$pr_2 : E \xrightarrow{\cong} \boldsymbol{P}^1, (x,z) \mapsto z$$

mit einer projektiven Geraden identifizieren. Die Punkte der exzeptionellen Geraden parametrisieren dabei die Geraden der projektiven Ebene durch den Punkt $(1:0:0)\in \boldsymbol{P}^1$

$$E \ni z = (z_0 : z_1) \mapsto L_z = \{ (x_0 : x_1 : x_2) \in \boldsymbol{P}^2 : z_0 x_2 - z_1 x_1 = 0 \} \subset \boldsymbol{P}^2 .$$

Die y-Achse hat dabei den Parameter

$$(0:1)\in \boldsymbol{P}^1,$$

und entspricht der fehlenden Geraden im affinen Beispiel 2.1.4, Teil iii). Die x-Achse hat den Parameter

$$(1:0)\in \boldsymbol{P}^1 .$$

Die wichtigste Eigenschaft einer regulären Abbildung zwischen projektiven Varietäten ist ihre Abgeschlossenheit. Der entsprechende Satz gilt im Affinen nur für endliche Abbildungen (Satz 3.2.9).

5.1.13 Satz (Projektionssatz)

i) Die Projektion

$$pr_2 : \boldsymbol{P}^n \times \boldsymbol{P}^m \longrightarrow \boldsymbol{P}^m, (x,y) \mapsto y ,$$

ist eine abgeschlossene Abbildung, d.h. das Bild einer Zariski-abgeschlossenen Teilmenge von $\boldsymbol{P}^n \times \boldsymbol{P}^m$ ist eine projektive Varietät von $\boldsymbol{P}^m$.

ii) Jede reguläre Abbildung

$$f : X \longrightarrow Y$$

zwischen projektiven Varietäten ist abgeschlossen.

Beweis. ad i) Gegeben sei eine projektive k-Varietät

$$X = \{ (x,y) \in \boldsymbol{P}^n \times \boldsymbol{P}^m : f_i(x,y) = 0 \ \textit{für}\ i = 1,...,N \},$$

welche definiert wird durch Polynome

$$f_i = f_i(X_0, X_1, ..., X_n, Y_0, Y_1, ..., Y_m) \in k[X_0, X_1, ..., X_n, Y_0, Y_1, ..., Y_m]$$

der Form

$$f_i = f_i(X_0, X_1, ..., X_n, Y_0, Y_1, ..., Y_m) = \sum_j a_j^i(X_0, X_1, ..., X_n) \cdot b_j^i(Y_0, Y_1, ..., Y_m).$$

Dabei sind die Polynome

$$a_j^i(X_0, X_1, ..., X_n) \in k[X_0, X_1, ..., X_n] \text{ homogen vom Grad } d_i$$

und

$$b_j^i(Y_0, Y_1, ..., Y_m) \in k[Y_0, Y_1, ..., Y_m] \text{ homogen.}$$

Für einen Punkt $y \in \boldsymbol{A}^{m+1} - 0$ und seine Äquivalenzklasse $[y] \in \boldsymbol{P}^m$ sind die folgenden beiden Aussagen äquivalent:

- $[y] \in pr_2(X)$
- Die Polynome

$$f_1(-, y), ..., f_N(-, y) \in k[X_0, X_1, ..., X_n]$$

haben eine gemeinsame Nullstelle in $\boldsymbol{A}^{n+1} - 0$.

Die letzte Eigenschaft wird nun mit Hilfe des Hilbertschen Nullstellensatzes in eine Aussage der Linearen Algebra umgeformt. Nach dem Hilbertschen Nullstellensatz sind äquivalent:

- $[y] \notin pr_2(X)$
- $Var(\langle f_1(-, y), ..., f_N(-, y) \rangle) = \{0\}$
- $\sqrt{\langle f_1(-, y), ..., f_N(-, y) \rangle} = \langle X_0, ..., X_n \rangle$
- Es gibt ein $d \in \boldsymbol{N}$ mit

$$\langle X_0, ..., X_n \rangle^d \subset \langle f_1(-, y), ..., f_N(-, y) \rangle.$$

Daher ist zu zeigen, daß die Teilmenge

$$\{ y \in \boldsymbol{A}^{m+1} : \textit{Es gibt kein } d \in \boldsymbol{N} \textit{ mit } \langle X_0, ..., X_n \rangle^d \subset \langle f_1(-, y), ..., f_N(-, y) \rangle \}$$

das Nullstellengebilde homogener Polynome ist. Wir bezeichnen mit

$$H(e) \subset k[X_0, X_1, ..., X_n]$$

den endlich-dimensionalen k-Vektorraum der homogenen Polynome vom Grad $e \in \boldsymbol{N}$ und betrachten für jedes $y \in \boldsymbol{A}^{m+1}$ und $d \in \boldsymbol{N}$ die k-lineare Abbildung

$$F(d, y): H(d - d_1) \oplus H(d - d_2) \oplus ... \oplus H(d - d_N) \longrightarrow H(d), (g_1, ..., g_N) \mapsto \sum_{i=1}^{N} f_i(-, y) \cdot g_i$$

Diese Abbildung ist genau dann surjektiv, wenn

$$\langle X_0, ..., X_n \rangle^d \subset \langle f_1(-, y), ..., f_N(-, y) \rangle.$$

Nach Wahl von Basen wird die lineare Abbildung $F(d,y)$ durch eine Matrix $M(F(d,y))$ beschrieben, deren Koeffizienten als Funktionen von $y \in \boldsymbol{A}^{m+1}$ homogene Polynome in den Veränderlichen $Y_0, Y_1, ..., Y_m$ sind. Es sind äquivalent:

- $F(d,y)$ nicht surjektiv
- Der Rang von $F(d,y)$ ist nicht maximal
- Alle maximalen Minoren der Matrix $M(F(d,y))$ haben eine verschwindende Determinante.

Die Determinante einer Matrix ist ein homogenes Polynom in den Koeffizienten der Matrix, und die Koeffizienten der Matrix $M(F(d,y))$ hängen homogen von den Veränderlichen $Y_0, Y_1, ..., Y_m$ ab. Daher bedeutet die letzte Bedingung das Verschwinden homogener Polynome in $Y_0, Y_1, ..., Y_m$ an der Stelle $y \in \boldsymbol{A}^{m+1}$, definiert also bei variablem $[y] \in \boldsymbol{P}^m$ eine projektive Varietät $Y(d) \subset \boldsymbol{P}^m$. Die Darstellung

$$pr_2(X) = \bigcap_{d \in \boldsymbol{N}} Y(d)$$

zeigt, daß auch

$$pr_2(X) \subset \boldsymbol{P}^m$$

eine projektive Varietät ist.

ad ii) Sind $X \subset \boldsymbol{P}^n$ und $Y \subset \boldsymbol{P}^m$ projektive Varietäten, so betrachtet man den Graphen von f

$$\Gamma_f := \{ (x,y) \in X \times Y : y = f(x) \} \subset \boldsymbol{P}^n \times \boldsymbol{P}^m$$

der ebenfalls eine projektive Varietät ist. Die erste Projektion

$$pr_1 : \Gamma_f \xrightarrow{\cong} X$$

ist ein regulärer Isomorphismus, sei

$$j := f^{-1} : X \longrightarrow \Gamma_f$$

die Umkehrabbildung. Die gegebene Abbildung faktorisiert als

$$f = \left[X \xrightarrow{j} \Gamma_f \xrightarrow{pr_2} Y \right]$$

Nach dem bereits bewiesenen Teil des Satzes ist

$$f(X) = pr_2(\Gamma_f)$$

als Teilmenge von $\boldsymbol{P}^m$ und damit auch als Teilmenge von Y abgeschlossen, q.e.d.

5.2 Das Hilbert Polynom

Die wichtigste numerische Invariante einer projektiven Varietät ist ihre Dimension. Sie läßt sich neben anderen numerischen Größen aus ihrem homogenen Koordinatenring ablesen.

5.2.1 Bemerkung *(Graduierung)*

i) Der Polynomring

$$R := k[X_1,...,X_n]$$

besitzt in natürlicher Weise eine *Graduierung*: Definiert man die additiven Abelschen Gruppen

$$R^s := \{ f \in R : f \text{ homogen und } \deg(f) = s \}, s \in \mathbf{N},$$

so gilt

$$R = \oplus_{s \in \mathbf{N}} R^s \text{ und } R^s \cdot R^t \subset R^{s+t}.$$

ii) Für ein *homogenes* Ideal $I \subset R$ überträgt sich die Graduierung auf den Quotienten: Für $s \in \mathbf{N}$ setzt man

$$I^s := I \cap R^s \text{ und } (R/I)^s := R^s / I^s.$$

iii) Für einen graduierten Ring R heißt ein R-Modul M ein *graduierter R-Modul*, wenn es eine Familie von Untermoduln $(M^s)_{s \in Z}$ von M gibt mit

$$M = \oplus_{s \in \mathbf{Z}} M^s \text{ und } R^s \cdot M^t \subset M^{s+t}.$$

5.2.2 Definition *(Hilbert Funktion)*

Es sei $I \subset k[X_0,...,X_n]$ ein homogenes Ideal. Die *Hilbert Funktion* des Quotientenringes

$$A := k[X_0,...,X_n]/I$$

ist definiert als

$$Hilb_A : \mathbf{Z} \longrightarrow \mathbf{N}, s \mapsto \begin{cases} \dim_k A^s & s \geq 0 \\ 0 & sonst \end{cases}.$$

Die *Hilbert Funktion* einer projektiven Varietät $X \subset \mathbf{P}^n$ ist die Hilbert Funktion ihres homogenen Koordinatenringes.

5.2.3 Beispiel *(Hilbert Funktion)*

Die Hilbert Funktion des projektiven Raumes

$$Hilb_{P^n} : \mathbf{Z} \longrightarrow \mathbf{N}$$

berechnet an der Stelle $s \in \mathbf{Z}$ die Anzahl der homogenen Polynome vom Grad s in $n+1$ Veränderlichen. Sie hat den Funktionswert

$$Hilb_{P^n}(s) = Hilb_{k[X_0,...,X_n]}(s) = \begin{cases} \binom{s+n}{s} & s \geq 0 \\ 0 & s < 0 \end{cases} .$$

Für $s \geq 0$ stimmt sie mit den Funktionswerten eines Polynoms vom Grad n mit Leitkoeffizient $\frac{1}{n!}$ überein:

$$\binom{s+n}{s} = \binom{s+n}{n} = \frac{s^n}{n!} + Terme\ niedrigeren\ Grades\ in\ s$$

Nach einem Satz von Macaulay kann man sich bei der Bestimmung der Hilbert Funktion auf monomiale Ideale beschränken.

5.2.4 Satz (Hilbert Funktion)

Ein homogenes Ideal

$$I \subset k[X_0, X_1, ..., X_n]$$

und das Ideal seiner Leitmonome

$$LT(I) \subset k[X_0, X_1, ..., X_n]$$

bzgl. einer beliebigen Monomordnung haben dieselbe Hilbert Funktion.

Beweis. [CLO 1997] Chap. 9, §3, Prop. 4.

Aus Satz 5.2.4 folgt, daß sich die Hilbert Funktion für genügend große Funktionswerte durch ein Polynom berechnen läßt:

5.2.5 Satz (Hilbert Polynom)

Für jede projektive Varietät $X \subset \boldsymbol{P}^n$ gibt es eine Konstante $s_0 \in \boldsymbol{N}$ und ein eindeutig bestimmtes Polynom P_X, das *Hilbert Polynom* von X, der Gestalt

$$P_X(s) = \frac{d}{m!} \cdot s^m + Terme\ niedrigeren\ Grades\ in\ s\ .$$

mit nicht-negativen ganzen Zahlen $d, m \in \boldsymbol{N}$, so daß

$$Hilb_X(s) = P_X(s)\ für\ alle\ s \geq s_0\ .$$

Beweis. [CLO 1997] Chap. 9, §3.

5.2.6 Definition (Hilbert Polynom und numerische Invarianten)

Es sei $X \subset \boldsymbol{P_n}$ eine projektive Varietät und

$$P_X(s) = d \cdot \frac{s^m}{m!} + \textit{Terme niedrigeren Grades in } s$$

ihr Hilbert Polynom. Man nennt

- den Grad $m \in \boldsymbol{N}$ die *Dimension* $dim(X)$ von X
- die Zahl

  $$d = m! \cdot \textit{Leitkoeffizient} \in \boldsymbol{N}$$

  den *Grad* $\deg(X, \boldsymbol{P}^n)$ der Einbettung $X \xrightarrow{\subset} \boldsymbol{P}^n$
- und den Funktionswert

  $$p_a(X) := (-1)^m \cdot (P_X(0) - 1)$$

  das *arithmetische Geschlecht* von X.

Für den projektiven Raum $\boldsymbol{P}^n$ gilt $m = n$, $d = 1$ und $p_a = 0$.

5.2.7 Tool-Beispiel (Hilbert Polynom und numerische Invarianten)

Macaulay2 berechnet in

- „MyExamples/HilbertPolynomial/Examples“

die folgenden Beispiele:

Getwistete Kubik

Veronese Fläche

Segre Einbettung

Elliptische Kurve

5.2.8 Bemerkung (Numerische Invarianten einer Varietät)

i) Der Grad der Einbettung einer projektiven Varietät ist eine positive ganze Zahl. Sie hängt nicht nur von der Varietät, sondern auch von der Art der Einbettung ab.

ii) Dimension und arithmetisches Geschlecht einer projektiven Varietät hängen dagegen nicht von der Einbettung ab, sind also intrinsische Größen der Varietät.

Das arithmetische Geschlecht ist eine nicht-negative ganze Zahl.

Neben dem hier definierten *arithmetischen* Geschlecht besitzt eine projektive Varietät auch noch ein *geometrisches* Geschlecht. Beide Größen entspringen aus verschiedenen Quellen: Das arithmetische Geschlecht aus den regulären Funktionen, das geometrische aus den regulären Diffentialformen. Im Falle einer nicht-singulären Kurve fallen beide numerischen Invarianten zusammen.

iii) Der Grad einer projektiven Hyperfläche

$$X = Var(f) \subset \boldsymbol{P}^n$$

stimmt überein mit dem Grad des definierenden homogenen Polynoms

$$f \in k[X_0, ..., X_n].$$

Eine der wichtigsten Anwendungen des Grades ist die Bestimmung der Schnittzahl zweier projektiver Kurven. Die Schwierigkeit besteht darin, lokal für jeden Schnittpunkt seine Vielfachheit zu definieren. Dann gilt:

5.2.9 Satz (Bezout)

Es sei $X_1, X_2 \subset \boldsymbol{P}^2$ zwei projektive Kurven, deren Durchschnitt

$$X = X_1 \cap X_2$$

keine irreduzible Komponente von X_1 oder von X_2 enthält. Dann besteht der Durchschnitt X aus endlich vielen Punkten. Ihre Anzahl – mit Vielfachheit – ist das Produkt der Grade

$$\deg(X_1) \cdot \deg(X_2).$$

Beweis. [CLO1997], Chap. 8, §7.

Der Satz von Bezout läßt sich auf höherdimensionale Varietäten verallgemeinern.

5.2.10 Satz (Grad und Geschlecht ebener projektiver Kurven)

Bei einer projektiven Kurve, die sich als Hyperfläche $X \subset \boldsymbol{P}^2$ in die projektive Ebene einbetten läßt, stehen Geschlecht

$$p = p_a(X)$$

und Grad

$$d = d(X)$$

in folgender Beziehung

$$p = \frac{(d-1)\cdot(d-2)}{2}.$$

Beweis. Die Kurve werde durch das Ideal

$$I = \langle f \rangle \subset R := k[X_0, X_1, X_2]$$

mit einem homogenen Polynom $f \in R$ vom Grad d definiert. Dann gibt es eine exakte Sequenz

$$0 \longrightarrow R \xrightarrow{f} R \longrightarrow R/I = k[X] \longrightarrow 0,$$

die zweite Abbildung ist die Multiplikation mit f, die dritte die kanonische Restklassenabbildung. Die Hilbert Funktion ist additiv. Es gilt:

$$Hilb_R(s) = Hilb_R(s-d) + Hilb_{k[X]}(s), s \in \boldsymbol{Z},$$

also

$$Hilb_{k[X]}(s) = Hilb_R(s) - Hilb_R(s-d) = \binom{2+s}{2} - \binom{2-d+s}{2}$$

$$= d \cdot s + 1 + \frac{(d-2)\cdot(d-1)}{2}.$$

Hieraus liest man ab

$$m = dim(X) = 1,\ deg(X) = d \text{ und } p(X) = \frac{(d-2)\cdot(d-1)}{2}, \text{ q.e.d.}$$

6 Basiswechsel

Dieses Kapitel zeigt die enge Verbindung der Algebraischen Geometrie zu zwei anderen Gebieten der Mathematik, zur Zahlentheorie und zur Theorie der Riemannschen Flächen. Das Kapitel gibt dabei einen Ausblick auf einige der tiefsten Resultate der Mathematik im 20. Jahrhundert.

Eine k-Varietät wird auf Seiten der Algebra durch ein Ideal

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

in einem Polynomring über dem Körper k definiert. Der Körper k enthält zumindest alle Koeffizienten der definierenden Polynome. Auf der Seite der Geometrie betrachtet man das Nullstellengebilde im affinen Raum über dem algebraischen Abschluß $K = \bar{k}$:

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

Mit demselben Recht kann man aber auch das Nullstellengebilde in einem Raum

$$\boldsymbol{A}_L^n := L^n$$

über einem beliebigen Erweiterungskörper $L \supset k$ betrachten, der nicht notwendig algebraisch-abgeschlossen ist. Bei einer Varietät X spielen also zumindest zwei Körper eine Rolle:

- Der Körper k, über dem X definiert ist (Algebra)
- Der Körper L, über dem man das Nullstellengebilde betrachtet (Geometrie).

Um auszudrücken, daß X über k *definiert* ist, schreibt man X / k, d.h.

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

Dagegen schreibt man für die Menge der L*-wertigen Punkte* von X

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

Bei dieser Betrachtung stellt sich der algebraische Aspekt einer Varietät als wesentlich allgemeiner heraus als der geometrische: Denn aus der einen algebraischen Definition X / k entspringt für eine ganze Schar von Körpern $L \supset k$ die Untersuchung der jeweiligen Nullstellengebilde $X(L)$. Man sagt, daß $X(L)$ aus X / k durch einen *Basiswechsel*

$$R_1 \longrightarrow R_2$$

vom Ring $R_1 = k$ zum Ring $R_2 = L$ hervorgeht.

Alle Überlegungen gelten nicht nur für affine Varietäten, sondern genauso für projektive Varietäten.

6.1 Zahlentheorie

Wenn man die Zahlentheorie in der Sprache der Algebraischen Geometrie formuliert, so sind zunächst die Fälle

$$k = \boldsymbol{Q} \text{ und } L \supset \boldsymbol{Q} \text{ eine algebraische Körpererweiterung}$$

interessant.

Desweiteren studiert man sogar den Fall, daß die Koeffizienten der definierenden Polynome aus einem kommutativen Ring stammen, der kein Körper ist. Daß die Varietät also z.B. über dem Ring der ganzen Zahlen $\boldsymbol{Z}$ definiert ist, d.h. durch ein Ideal

$$I \subset \boldsymbol{Z}[X_1,...,X_n],$$

dessen Elemente Polynome mit ganzzahligen Koeffizienten sind. Hier sind interessant die Basiswechsel

$$\boldsymbol{Z} \longrightarrow \boldsymbol{F}_q$$

zu den endlichen Restklassenkörpern $\boldsymbol{F}_p$ mit einer Primzahl p, die Basiswechsel

$$\boldsymbol{Z} \xrightarrow{\subset} \boldsymbol{Q}_p$$

zu den p-adischen Körpern $\boldsymbol{Q}_p$, und der Basiswechsel

$$\boldsymbol{Z} \xrightarrow{\subset} \boldsymbol{R}$$

zum Körper der reellen Zahlen.

Eine erste Unterscheidung der bei einem Basiswechsel auftretenden Erscheinungen läßt sich anhand des Grades bzw. des dahinter stehenden Geschlechtes durchführen.

6.1.1 Bemerkung *(Linearer Teilraum)*

Eine *lineare* projektive Varietät X / k wird durch ein Ideal $I \subset k[X_0,...,X_n]$ definiert, das von homogenen Polynomen 1. Grades, d.h. linearen Polynomen erzeugt wird. Die Menge der L-wertigen Punkte, $L \supset k$, bildet unabhängig von L immer einen linearen Unterraum fester Dimension des projektiven Raums:

$$X(L) \cong \boldsymbol{P}^d(L) \subset \boldsymbol{P}^n(L).$$

6.1.2 Bemerkung *(Quadrik)*

Eine *Quadrik* ist eine projektive Varietät X / k, deren Ideal durch ein homogenes Polynom 2. Grades, d.h. ein quadratisches Polynom erzeugt wird. Die Menge der L-wertigen Punkte hängt stark von $L \supset k$ ab.

Beispielsweise hat die projektive Kurve $X / \boldsymbol{Q}$, die durch das Polynom

$$f(X_0, X_1, X_2) = X_0^2 + X_1^2 + X_2^2 \in k[X_0, X_1, X_2]$$

definiert ist, keinen $\boldsymbol{Q}$-wertigen (d.h. rationalen) oder $\boldsymbol{R}$-wertigen (d.h. reellen) Punkt. Sie hat aber viele $\boldsymbol{C}$-wertige (d.h. komplexe) Punkte, es gilt sogar

$$X(\boldsymbol{C}) \cong \boldsymbol{P}^1(\boldsymbol{C}).$$

Der folgende Satz stellt ein Lokal-Global Prinzip dar. Man betrachtet seine Aussage über dem Zahlkörper $\boldsymbol{Q}$ als eine globale Aussage und seine Aussagen über die Komplettierungen von $\boldsymbol{Q}$ bzgl. der verschiedenen Bewertungen als eine lokale Aussage. Als weiterführende Literatur siehe [Maz1993].

6.1.3 Satz *(Hasse-Minkowski, 1920)*

Eine Quadrik $X / \boldsymbol{Q}$ hat genau dann einen rationalen Punkt, wenn sie

- für den Körper $L = \boldsymbol{R}$
- und für alle Primzahlen p für den Körper $L = \boldsymbol{Q}_p$ der p-adischen Zahlen

jeweils einen L-wertigen Punkt besitzt.

Beweis. Für einen Beweis siehe [Fre1984], Kap. V, Satz 3.9.

6.1.4 Definition *(Elliptische Kurve)*

Eine *elliptische Kurve* E / k ist eine nicht-singuläre projektive Kurve mit Geschlecht $g = 1$, zusammen mit einem ausgezeichneten k-wertigen Punkt $0 \in E(k)$.

6.1.5 Bemerkung *(Elliptische Kurve)*

Jede elliptische Kurve E / k läß sich schon als Hyperfläche in der projektiven Ebene realisieren:

$$E = Var(f) \subset \boldsymbol{P}^2$$

mit einem homogenen Polynom

$$f \in k[X, Y, Z].$$

Nach Satz 5.2.10 hat f den Grad $\deg f = 3$. Im Falle Charakteristik $char\ k \neq 2, 3$ kann man erreichen, daß f die Homogenisierung eines Polynoms g in Weierstraß Normalform ist

$$g(X, Y) = Y^2 - X^3 - A \cdot X - B \in k[X, Y]$$

und daß der ausgezeichnete Punkt der unendlich ferne Punkt ist

$$0 := (0:1:0) \in E(k) \subset \boldsymbol{P}^2 .$$

Das Nichtverschwinden der Diskriminante

$$\Delta := -16\left(4 \cdot A^3 + 27 \cdot B^2\right) \neq 0$$

garantiert, daß die projektive Kurve nicht-singulär ist.

Für jeden Erweiterungskörper $L \supset k$ bildet die Menge $E(L)$ eine Abelsche Gruppe mit dem ausgezeichneten Punkt als neutralem Element 0.

Hinweis. Das grundlegende Lehrbuch über elliptische Kurven ist [Sil1986].

6.1.6 Tool-Beispiel (Elliptische Kurve und Diskriminante)

Pari-Beispiel

- MyExamples/Example1

i) Die elliptische Kurve $E/\boldsymbol{Q}$ mit der Weierstraß Normalform

$$Y^2 = X^3 + X$$

hat die Diskriminante

$$\Delta = -64.$$

Die Kurve hat eine relle Nullstelle

$$x_1 = 0$$

und die beiden konjugiert-komplexen Nullstellen

$$x_{2,3} = +/- i.$$

Die relle Nullstelle definiert einen rationalen Punkt

$$p := (0, 0) \in E(\boldsymbol{Q}),$$

der in der Abelschen Gruppe $(E(\boldsymbol{Q}), +)$ die Ordnung 2 hat und damit die Torsionsuntergruppe erzeugt.

ii) Die elliptische Kurve $E/\boldsymbol{Q}$ mit der Weierstraß Normalform

$$Y^2 = X^3 + 1$$

hat die Diskriminante

$$\Delta = -432.$$

Die Kurve hat eine reelle Nullstelle

$$x_1 = -1$$

und zwei konjugiert-komplexe Nullstellen. Die relle Nullstelle definiert einen rationalen Punkt

$$p := (-1, 0) \in E(\boldsymbol{Q}),$$

der in der Abelschen Gruppe $(E(\boldsymbol{Q}), +)$ die Ordnung 2 hat. Der Punkt

$$q := (2, 3) \in E(\boldsymbol{Q})$$

hat die Ordnung 6 und erzeugt damit die Torsionsuntergruppe.

6.1.7 Satz (Mordell, 1922)

Es sei k ein Zahlkörper und E/k eine elliptische Kurve. Die Abelsche Gruppe $E(k)$ der k-wertigen Punkte ist endlich erzeugt, d.h.

$$E(k) \cong \boldsymbol{Z}^r \oplus E_{tors}(k),$$

wobei $r \in \boldsymbol{N}$ ihren Rang und $E_{tors}(k)$ ihre Torsionsuntergruppe bezeichnet.

Beweis. [Sil1986], Chap. VIII, Theor. 6.7.

Der Rang einer elliptischen Kurve ist eine subtile arithmetische Charakteristik. Es wird vermutet, daß elliptische Kurven mit beliebig großem Rang existieren.

6.1.8 Tool-Beispiel (Eliptische Kurve mit positivem Rang)

Pari-Beispiel

- MyExamples/Example2

Die elliptische Kurve $E/\boldsymbol{Q}$ mit der Weierstraß Normalform

$$Y^2 = X^3 - 7 \cdot X + \frac{25}{4}$$

hat die Diskriminante

$$\Delta = 5077 .$$

Die Torsionuntergruppe der rationalen Punkte von $E(\boldsymbol{Q})$ ist trivial. Die Gruppe $E(\boldsymbol{Q})$ enthält jedoch zahlreiche Punkte, hat also positiven Rang. Es ist bekannt, daß der Rang $= 3$ ist.

6.1.9 Beispiel (Selmer, 1951)

Für Kurven 3. Grades gilt das Analogon des Satzes von Hasse-Minkowski nicht mehr: Die projektive Kurve $X/\boldsymbol{Q}$, welche durch das homogene Polynom

$$f(X_0, X_1, X_2) = 3 \cdot X_0^3 + 4 \cdot X_1^3 + 5 \cdot X_2^3 \in k[X_0, X_1, X_2]$$

definiert ist, hat keinen rationalen Punkt. Sie enthält aber den reellen Punkt

$$\left(\sqrt[3]{3} : -1 : -1\right) \in X(\boldsymbol{R}).$$

Außerdem gilt nach einem Satz von Hasse für die Anzahl der $\boldsymbol{F}_p$-wertigen Punkte

$$\left| \# X(\boldsymbol{F}_p) - p \right| \leq 2 \cdot \sqrt{p}$$, p eine Primzahl.

Insbesondere hat $X/\boldsymbol{Q}$ also neben dem ausgezeichneten Punkt noch weitere $\boldsymbol{F}_p$ -wertige Punkte. Nach dem Hensel Lemma hat $X/\boldsymbol{Q}$ dann auch weitere $\boldsymbol{Q}_p$ -wertige Punkte.

Hinweis. Als weiterführende Literatur siehe [Maz1993].

Projektive Kurven $X/\boldsymbol{Q}$ höheren Geschlechtes haben immer nur endlich viele rationale Punkte, diese Eigenschaft wurde 1922 von Mordell vermutet.

6.1.10 Satz (Faltings, 1983)

Eine projektive nicht-singuläre Kurve $X/\boldsymbol{Q}$ vom Geschlecht $g \geq 2$ hat nur endlich viele rationale Punkte, d.h.

$$\#X(\boldsymbol{Q}) < \infty .$$

Hinweis. Für eine Übersicht siehe [Fal1984], für eine fortgeschrittene Darstellung siehe den Tagungsband [CS1986].

Das bisher wichtigste Ergebnis aus der Theorie elliptischer Kurven ist der Beweis der Taniyama-Weil Vermutung. Aus ihr ergibt sich die Fermat Vermutung (1637).

6.1.11 Satz (Wiles, 1994)

Die projektive Varietät $X/\boldsymbol{Q}$, die durch das Polynom

$$f(X_0, X_1, X_2) = -X_0^d + X_1^d + X_2^d \in \boldsymbol{Q}[X_0, X_1, X_2]$$

definiert ist, hat für $d \geq 3$ keinen rationalen Punkt, d.h. $X(\boldsymbol{Q}) = \varnothing$.

Hinweis. Für eine Übersicht siehe [Fal1995], für eine fortgeschrittene Darstellung siehe den Tagungsband [CSS1995].

6.2 Riemannsche Flächen

Der Basiswechsel

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

führt in die Funktionentheorie, die Theorie der Riemannschen Flächen oder allgemeiner in die Komplexe Analysis. Die Komplexe Analysis untersucht „Komplexe Mannigfaltigkeiten“ bzw. „Komplexe Räume“ mit holomorphen Abbildungen als zugehörigen Morphismen. Diese werden lokal durch konvergente Potenzreihen gegeben.

Die komplexwertigen Punkte

$$X(\boldsymbol{C})$$

einer Varietät, versehen mit der Euklidischen Topologie, sind komplexe Räume bzw. im nicht-singulären Fall komplexe Mannigfaltigkeiten. Komplexe Mannigfaltigkeiten der Dimension 1 heißen Riemannsche Flächen:

6.2.1 Bemerkung *(Riemannsche Flächen)*

Ein topologischer Hausdorff Raum, der jeweils lokal homöomorph ist zu einer offenen Menge in der komplexen Zahlenebene $\boldsymbol{C}$, zusammen mit einem Atlas biholomorph verträglicher Karten, heißt *Riemannsche Fläche*.

Hinweis. Als Literatur siehe [For1977].

6.2.2 Satz *(Kompakte Riemannsche Flächen)*

Jede kompakte Riemannsche Fläche ist projektiv algebraisch, d.h. zu jeder kompakten Riemannschen Fläche Y existiert eine nicht-singuläre projektive Kurve $X / \boldsymbol{C}$ und ein biholomorpher Isomorphismus

$$Y \cong X(\boldsymbol{C}).$$

Beweis. [Har1977] Chap. IV, Sect. 3.

Dieser Satz ist unter anderem deswegen bemerkenswert, weil Riemannsche Flächen durch holomorphe Funktionen, also lokal durch konvergente Potenzreihen, definiert werden. Die Varietäten der Algebraischen Geometrie sind dagegen immer durch Polynome definiert.

6.2.3 Bemerkung *(Geschlecht kompakter Riemannscher Flächen)*

Die wichtigste numerische Invariante einer kompakten Riemannschen Fläche ist ihr *Geschlecht*. Dieses ist über die holomorphe Struktur definiert und stimmt mit der Anzahl der linear unabhängigen holomorphen Differentialformen überein; siehe [For1977] Bem. 17.10. Als Geschlecht treten alle nicht-negativen ganzen Zahlen auf.

Das Geschlecht stellt sich als eine topologische Invariante heraus und liefert sogar eine topologische Klassifizierung: Zwei kompakte Riemannsche Flächen sind als topologische Mannigfaltigkeiten genau dann isomorph, wenn sie dasselbe Geschlecht haben.

In Satz 6.2.2 stimmt das Geschlecht der Riemannschen Fläche Y mit dem arithmetischen Geschlecht der projektiven Kurve $X / \boldsymbol{C}$ überein.

Alle nicht-singulären projektiven Kurven X / k lassen sich bereits in einem 3-dimensionalen projektiven Raum realisieren

$$X \xrightarrow{\subset} \boldsymbol{P}^3,$$

nicht-singuläre Kurven vom Geschlecht $g \leq 1$ sogar schon als Hyperflächen in der projektiven Ebene $\boldsymbol{P}^2$.

6.2.4 Definition (Torus)

Ein *Torus* ist der Quotient $(\boldsymbol{C}, +)/\Gamma$ der additiven Gruppe der komplexen Zahlen nach einem Gitter

$$\Gamma = \boldsymbol{Z} \cdot \omega_1 + \boldsymbol{Z} \cdot \omega_2 \text{ mit } \omega_1, \omega_2 \in \boldsymbol{C} \text{ linear unabhängig über } \boldsymbol{R}.$$

Man nennt Γ das *Periodengitter* und $\omega_1, \omega_2 \in \boldsymbol{C}$ die *Perioden* des Torus.

Jeder Torus ist eine kompakte Riemannsche Fläche vom Geschlecht $g = 1$. Außerdem ist ein Torus eine Abelsche Gruppe bezüglich der von $(\boldsymbol{C}, +)$ induzierten Addition.

Die Isomorphieklassen von Tori unter biholomorphen Abbildungen sind wohlbekannt. Sie entsprechen bijektiv den Äquivalenzklassen der Operation der Modulgruppe auf der oberen Halbebene $\boldsymbol{H}$. Nach einem klassischen Resultat aus der Theorie der Modulfunktionen läßt sich die Menge dieser Äquivalenzklassen durch die absolute Modulfunktion bijektiv auf die komplexen Zahlen abbilden. Grundlage dieser Theorie sind die auf der oberen Halbebene für jedes $k > 1$ definierten Eisenstein Reihen

$$G_k(\tau) := \sum_{\omega \in \Gamma(\tau) - 0} \frac{1}{\omega^{2k}}, \ \tau \in \boldsymbol{H}, \ \Gamma(\tau) := \boldsymbol{Z} \cdot 1 + \boldsymbol{Z} \cdot \tau.$$

6.2.5 Lemma (Isomorphieklassen von Tori)

i) Jeder Torus ist isomorph unter einer holomorphen Abbildung zu einem Torus mit einem normierten Periodengitter

$$\Gamma(\tau), \tau \in \boldsymbol{H}.$$

ii) Zwei normierte Periodengitter $\Gamma(\tau_1)$ und $\Gamma(\tau_2)$ definieren genau dann isomorphe Tori, wenn es eine Matrix gibt

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \boldsymbol{Z}) \text{ mit } \tau_2 = \frac{a \cdot \tau_1 + b}{c \cdot \tau_1 + d},$$

d.h. die Äquivalenzklassen isomorpher Tori entsprechen bijektiv den Bahnen der Gruppenoperation

$$SL(2,\boldsymbol{Z})\times\boldsymbol{H}\longrightarrow\boldsymbol{H},\ (A,\tau)\mapsto\frac{a\cdot\tau+b}{c\cdot\tau+d}.$$

iii) Die absolute Modulfunktion

$$j:\boldsymbol{H}\longrightarrow\boldsymbol{C}\ \text{ mit }\ j:=1728\cdot\frac{g_2^{\,3}}{\Delta}$$

$$g_2:=60\cdot G_2,\ g_3:=140\cdot G_3,\ \Delta:=g_2^{\,3}-27\cdot g_3^{\,2}$$

ist invariant unter dieser Operation und induziert eine bijektive Abbildung des Bahnenraumes

$$\boldsymbol{H}/SL(2,\boldsymbol{Z})\xrightarrow{\cong}\boldsymbol{C}.$$

Hinweis. Zur Literatur siehe [Gun1972], [Ser1973].

6.2.6 Satz (Tori und elliptische Kurven)

i) Es sei $X=\boldsymbol{C}/\Gamma$ ein Torus mit einem normierten Periodengitter $\Gamma(\tau),\tau\in\boldsymbol{H}$. Dann definieren seine Weierstraß'sche $\wp$-Funktion

$$\wp(z):=\frac{1}{z^2}+\sum_{\omega\in\Gamma-0}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

und ihre Ableitung

$$\wp'(z)=-2\cdot\sum_{\omega\in\Gamma}\frac{1}{(z-\omega)^3}$$

eine injektive holomorphe Abbildung

$$\boldsymbol{C}/\Gamma\xrightarrow{\subset}\boldsymbol{P}^2,\ [z]\mapsto\begin{cases}\left(\wp(z):\frac{1}{2}\wp'(z):1\right) & z\notin\Gamma\\ (0:1:0) & z\in\Gamma\end{cases}.$$

Diese bildet den Torus biholomorph ab auf die komplexen Punkte der elliptischen Kurve $E/\boldsymbol{C}$ mit der Weierstraß Normalform

$$g(X,Y)=Y^2-X^3-A\cdot X-B\in\boldsymbol{C}[X,Y],\ A:=-15\cdot G_2(\tau),\ B:=-35\cdot G_3(\tau).$$

Die Abbildung ist zudem ein Isomorphismus Abelscher Gruppen

$$(\boldsymbol{C}/\Gamma,+)\xrightarrow{\cong}(E(\boldsymbol{C}),+).$$

ii) Jede Isomorphieklasse einer elliptische Kurve $E/\boldsymbol{C}$ tritt auf diese Art als Bild eines Torus auf.

Beweis. ad i) Die Aussage folgt aus der Differentialgleichung der Weierstraß'schen $\wp$-Funktion

$$\wp'^2 = 4 \cdot \wp^3 - g_2 \cdot \wp - g_3$$

und den Additionstheoremen der $\wp$-Funktion; siehe [Ahl1966].

ad ii) Jede über dem algebraisch-abgeschlossenen Körper $\boldsymbol{C}$ definierte elliptische Kurve $E/\boldsymbol{C}$ läßt sich auch durch eine Gleichung 3. Grades in Legendre Normalform definieren:

$$Y^2 = X \cdot (X-1) \cdot (X-\lambda) \in \boldsymbol{C}[X,Y]$$

mit einer eindeutig bestimmten komplexen Zahl $\lambda \in \boldsymbol{C}$ mit

$$|\lambda| < 1 \ \textit{und} \ |1-\lambda| < 1 .$$

Die beiden elliptischen Integrale

$$\omega_1 := \int_{-\infty}^{0} \frac{dx}{\sqrt{x \cdot (x-1) \cdot (x-\lambda)}} \text{ und } \omega_2 := \int_{1}^{\infty} \frac{dx}{\sqrt{x \cdot (x-1) \cdot (x-\lambda)}}$$

definieren ein Gitter

$$\Gamma = \boldsymbol{Z} \cdot \omega_1 + \boldsymbol{Z} \cdot \omega_2 , \ \frac{\omega_1}{\omega_2} \in \boldsymbol{H} \text{ oder } \frac{\omega_2}{\omega_1} \in \boldsymbol{H} .$$

Es bleibt zu zeigen: Mit

$$\tau := \frac{\omega_1}{\omega_2} , \text{ o.E. } \tau \in \boldsymbol{H} ,$$

erhält man einen Torus $X = \boldsymbol{C}/\Gamma(\tau)$, der unter der Abbildung von Teil i) biholomorph auf eine zu $E(\boldsymbol{C})$ isomorphe Varietät abgebildet wird; siehe [Sil1986] Chap. VI, q. e. d.

6.2.7 Tool-Beispiel (Tori und elliptische Kurven)

Pari-Beispiel

- MyExamples/Example3

Berechung der elliptischen Kurven zu Tori mit vorgebenen normierten Periodengittern.

7 Skripte ausgewählter Tool-Beispiele

Dieses Kapitel enthält die Skripte aller mit den Tools Singular, Macaulay2 und Pari in dieser Vorlesung behandelten Beispiele. Die Skripte der Beispiele aus Kapitel 1.2 für das Tool Surf sind nicht wiedergegeben.

7.1 Singular-Skripte

Ein Singular-Skript in der Datei „file“ im Arbeitsverzeichnis von Singular wird mit dem Befehl

< „file“;

ausgeführt.

7.1.1 Singular-Skript (Tool-Beispiel 2.2.7)

```
// Singular
// Maps between coordinate rings
print ("============================================================");
LIB "all.lib";

// Coordinate ring of affine line
ring       Q_T      = 0, T, dp;

print ("------------------------------------------------------------");
print ("Projecting Neil parabola");
// Neil parabola
ring       Q_XY     = 0, ( X, Y ), dp;
// define basering
setring ( Q_XY );

// projection onto x-axis
// as map from Q_T to basering
map phi1 = Q_T, X;
ideal      I1       = Y^2 - X^3 ;
print ("Projecting Neil parabola onto x-axis has dense image?");
is_injective ( phi1, Q_T, I1 );
print ("Projecting Neil parabola onto x-axis is isomorphism onto closed image?");
is_surjective ( phi1, Q_T, I1 );
print ("Projecting Neil parabola onto x-axis is finite?");
mapIsFinite ( phi1, Q_T, I1);

// projection onto y-axis
setring ( Q_XY );
```

```
map phi2 = Q_T, Y;
print ("Projecting Neil parabola onto y-axis has dense image?");
is_injective ( phi2, Q_T, I1 );
print ("Projecting Neil parabola onto y-axis is isomorphism onto closed image?");
is_surjective ( phi2, Q_T, I1 );
print ("Projecting Neil parabola onto y-axis is finite?");
mapIsFinite ( phi2, Q_T, I1);

print ("------------------------------------------------------------");
print ("Projecting hyperbola");

// Hyperbola
setring ( Q_XY );
map phi3 = Q_T, X;
ideal I3 = X*Y - 1;
print ("Projecting hyperbola onto x-axis has dense image?");
is_injective ( phi3, Q_T, I3 );
print ("Projecting hyperbola onto x-axis is isomorphism onto closed image?");
is_surjective ( phi3, Q_T, I3 );
print ("Projecting hyperbola onto x-axis is finite?");
mapIsFinite ( phi3, Q_T, I3);

print ("------------------------------------------------------------");
print ("Blow up");

// Blow up
ring Q_XY  = 0, ( X, Y ), dp;
ring Q_XYZ = 0, ( X, Y, Z ), dp;

setring ( Q_XYZ );
ideal I4 = Y - Z*X;
map phi4 = Q_XY, X, Y;
print ("Projecting blow-up onto x-y-plane has dense image?");
is_injective ( phi4, Q_XY, I4 );
print ("Projecting blow-up onto x-y-plane is isomorphism onto closed set?");
is_surjective ( phi4, Q_XY, I4 );
print ("Projecting blow-up onto x-y-plane is finite?");
mapIsFinite ( phi4, Q_XY, I4 );

ring Q_XZ  = 0, ( X, Z ), dp;
setring ( Q_XYZ );
// Coordinate ring of blow-up
```

```
qring blow_up = std (I4);
map phi5 = Q_XZ, X, Z;
print ("Projecting blow-up onto x-z-plane is isomorphism?");
is_bijective (phi5, Q_XZ);

print ("=========================================================");
```

7.1.2 Singular-Skript (Tool-Beispiel 3.2.10)

```
// Singular
// Normalization
print ("-----------------------------------------------");
LIB "all.lib";

print ("Normalization of Neil parabola");
// Neil parabola
ring Q_XY = 0, ( X, Y ), dp;
ideal I1 = Y^2 - X^3  ;

// check if ideal is prime
list primaryComponent = primdecGTZ( I1 );
if (            size (primaryComponent)  != 1
   or size ( reduce( primaryComponent[1][2], std( primaryComponent[1][1] ), 1 ) ) != 0 )
{
   print ("Ideal ");
   print ( I1 );
   print (" not prime") ;
   ERROR ("==> Computation cancelled");
}

qring neil_Parabola = std ( I1 );
setring Q_XY;
list nor1 = normal (I1);
show (nor1);
def R = nor1 [1];
setring R;
qring normalization = std ( norid ) ;
setring R;
normap;
is_bijective ( normap, neil_Parabola );

print ("-------------------------");
print ("Normalization of Whitney umbrella");
ring Q_XYZ = 0, ( X, Y, Z ),dp;
ideal I2 = Y^2 - Z*X^2;

// check if ideal is prime
list primaryComponent = primdecGTZ( I2 );
```

```
if (          size (primaryComponent)  != 1
   or size ( reduce( primaryComponent[1][2], std( primaryComponent[1][1] ), 1 ) ) != 0 )
{
   print ("Ideal ");
   print ( I2 );
   print (" not prime") ;
   ERROR ("==> Computation cancelled");
}
qring whitney_Umbrella = std ( I2 );
setring Q_XYZ;
list nor2 = normal (I2);
// show (nor2);
def R = nor2 [1];
setring R;
qring normalization = std ( norid ) ;
setring R;
normap;
is_bijective ( normap, whitney_Umbrella );

print ("-------------------------");
print ("Normalization of 5-nodal curve");
// Neil parabola
ring Q_XY = 0, ( X, Y ), dp;
ideal I3 =
  32*X^2 - 2097152*Y^11 + 1441792*Y^9 - 360448*Y^7 + 39424*Y^5 - 1760*Y^3 + 22*Y - 1;

// check if ideal is prime
list primaryComponent = primdecGTZ( I3 );
if (          size (primaryComponent)  != 1
   or size ( reduce( primaryComponent[1][2], std( primaryComponent[1][1] ), 1 ) ) != 0 )
{
   print ("Ideal ");
   print ( I3 );
   print (" not prime") ;
   ERROR ("==> Computation cancelled");
}

qring fiveNodalCurve = std ( I3 );
setring Q_XY;
list nor1 = normal (I3);
show (nor1);
def R = nor1 [1];
```

```
setring R;
qring normalization = std ( norid ) ;
setring R;
normap;
is_bijective ( normap, fiveNodalCurve );

print ("-------------------------");
print ("Normalization of hyperbola");
// Neil parabola
ring Q_XY = 0, ( X, Y ), dp;
ideal I4 = X*Y - 1;

// check if ideal is prime
list primaryComponent = primdecGTZ( I4 );
if (            size (primaryComponent)  != 1
   or size ( reduce( primaryComponent[1][2], std( primaryComponent[1][1] ), 1 ) ) != 0 )
{
   print ("Ideal ");
   print ( I4 );
   print (" not prime") ;
   ERROR ("==> Computation cancelled");
}

qring hyperbola = std ( I4 );
setring Q_XY;
list nor4 = normal (I4);
show (nor4);
def R = nor4 [1];
setring R;
qring normalization = std ( norid ) ;
setring R;
normap;
is_bijective ( normap, hyperbola );
print ("-----------------------------------------------");
```

7.1.3 Singular-Skript (Tool-Beispiel 3.2.12)

```
// Singular
// Noether Normalization
print ("-----------------------------------------------");
LIB "all.lib";
print ("Noether normalization of hyperbola");
// Hyperbola
ring Q_XY = 0, ( X, Y ), dp;
ideal I1 =X*Y - 1;
list noethNorm1 = noetherNormal ( I1 );
show ( noethNorm1 );

// Tranformation of coordinates
map phi1 = basering, noethNorm1[1];
print ("Is coordinate transformation ");
phi1;
print ("bijective?");
is_bijective ( phi1, basering );

// Transform ideal
ideal J1 = phi1 ( I1 );
print ("Ideal");
I1;
print("is transformed into ideal: ");
J1;

// Basering of Noether normalization
print ("Coordinate ring of Noether normalization: ");
noethNorm1[2];
print ("--------------------------------");

print ("Noether normalization of blow up");
// blow up
ring Q_XYZ = 0, ( X, Y, Z ), dp;
ideal I2 = Y - Z*X;
list noethNorm2 = noetherNormal ( I2 );
show ( noethNorm2 );

// Tranformation of coordinates
map phi2 = basering, noethNorm2[1];
```

```
print ("Is coordinate transformation ");
phi2;
print ("bijective?");
is_bijective ( phi2, basering );

// Transform ideal
ideal J2 = phi2 ( I2 );
print ("Ideal");
I2;
print("is transformed into ideal: ");
J2;

// Basering of Noether normalization
print ("Coordinate ring of Noether normalization: ");
noethNorm2[2];
print ("---------------------------------");

print ("Affine plane and additional line in 3-space");
// plane and line
ring Q_XYZ = 0, ( X, Y, Z ), dp;
ideal I3 = X*Y, X*Z;
list noethNorm3 = noetherNormal ( I3 );
show ( noethNorm3 );

// Tranformation of coordinates
map phi3 = basering, noethNorm3[1];
print ("Is coordinate transformation ");
phi3;
print ("bijective?");
is_bijective ( phi3, basering );

// Transform ideal
ideal J3 = phi3 ( I3 );
print ("Ideal");
I3;
print("is transformed into ideal: ");
J3;

// Basering of Noether normalization
print ("Coordinate ring of Noether normalization: ");
noethNorm3[2];
print ("-----------------------------------------------");
```

7.1.4 Singular-Skript (Tool-Beispiel 3.3.3)

```
// Singular
// Primary decomposition of ideals
print ("-----------------------------------------------");
print ("Primary decomposition of ideals");
LIB "all.lib";

print ("2 dimensions --------------------------");
// ring of polynomials over field of rationals
ring Q_xy = 0,(x,y),lp;
short = 0;

int i;
int j;
list primaryComponent;

list idealList;

// plane coordinate axes
ideal I1 = x*y;
idealList = insert (idealList, I1);

// Two lines
ideal I2 = x^2 - 1;
idealList = insert (idealList, I2, 1);

// Double lines
ideal I3 = x^2 ;
idealList = insert (idealList, I3, 2);

// Embedded component
ideal I4 = x^2, x*y;
idealList = insert (idealList, I4, 3);

// Loop through different ideals and output their primary decomposition
for ( i = 1; i <= size (idealList); i++ )
{
   primaryComponent = primdecGTZ( idealList[i] );
   print ("Ideal: <" + print(idealList[i],"%") + ">" );
   for ( j = 1; j <= size (primaryComponent); j++ )
```

```
   {
        print (    "Primary component: <"    + print( primaryComponent[j][1], "%") + ">"
        +          " with radical: <" + print( primaryComponent[j][2], "%") + ">" );
   }
   print("");
}

print ("3 dimensions ---------------------------");
// Plane and transversal line

ring Q_xyz = 0,(x,y,z ),lp;
int i;
int j;
list primaryComponent;

list idealList;

ideal I5 = x*y, x*z;
idealList = insert (idealList, I5);

// Loop through different ideals and output their primary decomposition
for ( i = 1; i <= size (idealList); i++ )
{
   primaryComponent = primdecGTZ( idealList[i] );
   print ("Ideal: <" + print(idealList[i],"%") + ">" );
   for ( j = 1; j <= size (primaryComponent); j++ )
   {
        print (    "Primary component: <"    + print( primaryComponent[j][1], "%") + ">"
        +          " with radical: <" + print( primaryComponent[j][2], "%") + ">" );
   }
   print("");
}
print ("-----------------------------------------------");
```

7.2 Macaulay2-Skripte

Ein Macaulay2-Skript in der Datei „file“ im Arbeitsverzeichnis von Macaulay2 wird mit dem Befehl

load „file“

ausgeführt.

7.2.1 Macaulay2-Skript *(Tool-Beispiel 4.1.11)*

```
-- Macaulay2
-- Division in ring of polynomials

division = ( numerator, listDenom ) -> (
   targetRing       := class numerator;
   use targetRing;
   k                := #listDenom;
   i                := 0;
   debug                    := false;
   if ( debug == true ) then
   (
         print ("Division: Start");
         << "Division: " << numerator << " :" << endl;
         i = 0;
         while i < k do
         (
               << "denominator " << i << ": " << listDenom_i << endl;
               i = i + 1;
         );
   );

   p                := numerator;
   r                := 0;
   quotient       := new MutableHashTable;

   -- initialize hash table of quotients
   i = 0;
   while i < k do
   (
         quotient#i          = 0;
         i                   = i + 1;
   );

   -- check if leading term of reduced dividend is divisible by leading term of one of divisors
```

```
while ( p != 0 ) do
(
        i = 0;
        divisionOccurred = false;

        -- loop through divisors
        while ( ( i < k ) and ( divisionOccurred == false ) ) do
        (
                -- check if  leading term of current divisor divides
                -- leading term of reduced dividend
                if ( denominator ( leadTerm p / leadTerm listDenom_i  ) == 1 ) then
                (
                        -- subscript quotient with index of denominator
                        if ( debug == true ) then
                        (
                                << "Division: Divide by " << listDenom_i << endl;
                                << "Division: p: " << p << "; listDenom" << i << ": ";
                                << listDenom_i << endl;
                        );
                        a = substitute (leadTerm p / leadTerm listDenom_i, targetRing );
                        quotient#i = quotient#i + a;
                        p = substitute ( p - a * listDenom_i, targetRing );
                        divisionOccurred = true;
                )
                else
                (
                        i = i + 1 ;
                );
        );
        if ( divisionOccurred == false ) then
        (
                -- move leading term of current dividend to rest
                r = r + leadTerm p;
                p = p - leadTerm p;
        );
);

-- output result
<< "(" << numerator << ") : "      << endl;
<< listDenom << " = " << endl    << endl;
i = 0;
while  i < k do
```

```
   (
        << "+ (" << quotient#i << ") * (" << listDenom_i << ")" << endl;
        i = i + 1;
   );
   << endl << "Rest: " << r << endl;

   if ( debug == true ) then
   (
        << "Division: End" << endl;
   );
);
<< "-----------------------------------" << endl;
R = QQ [ X,Y, MonomialOrder => Lex];
-- example 1
 g1 = X*Y + 1;
 g2 = Y^2 - 1;
 f = X*Y^2 - X;
 lden = { g2, g1 };
division ( f, lden);
<< "-----------------------------------" << endl;
-- example 2
lden = { g1, g2 };
division ( f, lden);
<< "-----------------------------------" << endl;
-- example 3
-- g1 = X*Y + 1;
-- g2 = Y + 1;
-- f = X*Y^2 + 1;
-- lden = {g1, g2};
-- division ( f, lden);
-- << "-----------------------------------" << endl;
-- example 4
-- g1 = X*Y - 1;
-- g2 = Y^2 - 1;
-- f = X^2*Y + X*Y^2 + Y^2;
-- lden = {g1, g2};
-- division ( f, lden);
-- << "-----------------------------------" << endl;
```

7.2.2 Macaulay2-Skript (Tool-Beispiel 4.2.11)

```
-- Macaulay2
-- Computation of Groebner bases
-- << "-----------------------------------" << endl;
R = QQ [ X,Y, MonomialOrder => Lex];
-- example 1
g1 = X*Y + 1;
g2 = Y^2 - 1;
I1 = ideal (  g1, g2 );
G1 = gb I1;
<<  I1 << " has Groebner base  with respect to Lex with "<<  endl;
<< rank source gens G1 << " elements:" << endl;
<< transpose gens G1 << endl;
<< "-----------------------------------" << endl;
R = QQ [ X,Y, Z, MonomialOrder => Lex];
-- example 2
g3 = X^5 + Y^4 + Z^3 - 1;
g4 = X^3 + Y^2 + Z^2 - 1;
I2 = ideal (  g3, g4 );
G2 = gb I2;
<<  I2 << " has Groebner base  with respect to Lex with "<<  endl;
<< rank source gens G2 << " elements:" << endl;
<< transpose gens G2 << endl;
<< "-----------------------------------" << endl;
R = QQ [ X,Y, Z, MonomialOrder => GRevLex];
-- example 3
g5 = X^5 + Y^4 + Z^3 - 1;
g6 = X^3 + Y^2 + Z^2 - 1;
I3 = ideal (  g5, g6 );
G3 = gb I3;
<<  I3 << " has Groebner base  with respect to GRevLex with "<<  endl;
<< rank source gens G3 << " elements:" << endl;
<< transpose gens G3 << endl;
<< "-----------------------------------" << endl;
```

7.2.3 Macaulay2-Skript (Tool-Beispiel 4.3.6)

```
-- Macaulay2
-- Twisted cubic curve
-- Define parametrization of twisted cubic curve by map
-- from affine line to affine space
<< "-------------------------------------------------------" << endl;
<< "Twisted cubic curve: Start " << endl;

-- Graph of twisted cubic curve
-- Monomial order for graph
R3 = QQ [ T, X,Y,Z, MonomialOrder => Lex ]
short = 0;
J = ideal ( X - T, Y -  T^2, Z - T^3 );
<< "Graph:" << J << endl;
<< "has Groebner base (Lex): " << gb (J) << endl;

-- Suitable elimination order for graph
R4 = QQ [ T, X,Y,Z, MonomialOrder => Eliminate 1 ]
short = 0;
J = substitute ( J, R4);
<< "Graph:" << J << endl;
<< "has Groebner base (Eliminate 1): " << gb (J) << endl;
<< endl;

-- Affine line
R1 = QQ[ T, MonomialOrder => Lex ]
-- Affine space
R2 = QQ [ X, Y, Z, MonomialOrder => Lex ]

phi = map ( R1, R2, { T, T^2, T^3 } )
<< phi << endl;
idealCubicCurve = kernel phi;

<<  "Twisted CubicCurve has ideal: " <<idealCubicCurve << endl;
<< "Is " <<  idealCubicCurve << " equal to " <<  ideal ( X^2 - Y, Z - X^3 ) << "? "
<< idealCubicCurve ==  ideal ( X^2 - Y, Z - X^3 ) << endl;

<< "Twisted cubic curve: End " << endl;
<< "-------------------------------------------------------" << endl;
```

7.2.4 Macaulay2-Skript (Tool-Beispiel 4.3.11)

```
-- Macaulay2
-- Quotient of ideals
<< "--------------------------------------------------------------------------" << endl;
<<  "Quotient of ideals. Start" << endl;
R1 = QQ[ X,Y,Z, MonomialOrder => Lex ];
<< "Base ring: " << describe R1 << endl;
<< endl;
-- ideal of y-z plane union x-axis
I = ideal ( X*Y, X*Z );

-- ideal of x-axis
J =  ideal ( Y, Z );

<< I << ": " << J << " = " << I:J << endl;
<< endl;
<<  "Quotient of ideals. End" << endl;
<< "--------------------------------------------------------------------------" << endl;
```

7.2.5 Macaulay2-Skript (Tool-Beispiel 5.2.7)

```
-- Macaulay2
-- Hilbert polynomial
-- base field
KK = QQ;
<< "--------------------------------------------------------------------" << endl;
<< "Twisted cubic: Start" << endl;
R1 = KK [ T0, T1 ];
R2 = KK [ X0, X1, X2, X3 ];
phiCubic = map ( R1, R2, { T0^3, T0^2*T1, T0*T1^2, T1^3 } );
describe phiCubic;
idealCubic = kernel phiCubic;
coordinateRingCubic = R2 / idealCubic;
-- evaluate projective Hilbert polynomial
-- the values dim and degree refering to the projective variety
cubicHilbertPolynomial = hilbertPolynomial (coordinateRingCubic);
cubicDimension = dim (cubicHilbertPolynomial);
cubicDegree =  degree (cubicHilbertPolynomial);
cubicArithmeticGenus = (-1)^cubicDimension * ( (cubicHilbertPolynomial 0) - 1);

<< "Twisted cubic curve has" << endl;
<< "ideal: " << transpose mingens idealCubic << endl;
<< "in ring: " << describe R2 << endl;
<< "Hilbert polynomial: " << cubicHilbertPolynomial << endl;
<< "dimension: " << cubicDimension << endl;
<< "degree: " << cubicDegree << endl;
<< "arithmetic genus: " << cubicArithmeticGenus << endl;

<< "Twisted cubic: End" << endl << endl;
<< "--------------------------------------------------------------------" << endl;
<< "Veronese surface: Start" << endl;
R1 = KK [ T0, T1, T2 ];
R2 = KK [ X0, X1, X2, X3, X4, X5 ];
phiVeronese = map ( R1, R2, { T0^2, T0*T1, T0*T2, T1^2, T1*T2, T2^2 } );
describe phiVeronese;
idealVeronese = kernel phiVeronese;
coordinateRingVeronese = R2 / idealVeronese;
veroneseHilbertPolynomial = hilbertPolynomial (coordinateRingVeronese);
veroneseDimension = dim (veroneseHilbertPolynomial);
```

```
veroneseDegree =  degree (veroneseHilbertPolynomial);
veroneseArithmeticGenus = (-1)^veroneseDimension * ( (veroneseHilbertPolynomial 0) - 1);

<< "Veronese surface has" << endl;
<< "ideal: " << transpose mingens idealVeronese << endl;
<< "in ring: " << describe R2 << endl;
<< "Hilbert polynomial: " << veroneseHilbertPolynomial << endl;
<< "dimension: " << veroneseDimension << endl;
<< "degree: " << veroneseDegree << endl;
<< "arithmetic genus: " << veroneseArithmeticGenus << endl;

<< "Veronese surface: End" << endl << endl;
<< "----------------------------------------------------------------------" << endl;
<< "Segre embedding: Start" << endl;
R1 = KK [ X0, X1 ];
R2 = KK [ Y0, Y1 ];
domainOfDefinition = R1 ** R2;
R3 = KK [ Z00, Z01, Z10, Z11 ];
phiSegre = map ( domainOfDefinition, R3, { X0*Y0, X0*Y1, X1*Y0, X1*Y1 } );
describe phiSegre;
idealSegre = kernel phiSegre;
coordinateRingSegre = R3 / idealSegre;
segreHilbertPolynomial = hilbertPolynomial (coordinateRingSegre);
segreDimension = dim (segreHilbertPolynomial);
segreDegree =  degree (segreHilbertPolynomial);
segreArithmeticGenus = (-1)^segreDimension * ( (segreHilbertPolynomial 0) - 1);

<< "Segre embedding has" << endl;
<< "ideal: " << transpose mingens idealSegre << endl;
<< "in ring: " << describe R3 << endl;
<< "Hilbert polynomial: " << segreHilbertPolynomial << endl;
<< "dimension: " << segreDimension << endl;
<< "degree: " << segreDegree << endl;
<< "arithmetic genus: " << segreArithmeticGenus << endl;

<< "Segre embedding: End" << endl << endl;
<< "----------------------------------------------------------------------" << endl;
<< "Elliptic Curve: Start" << endl;
R2 = KK [ X0, X1, X2 ];
idealEllipticCurve = ideal ( X0*X2^2 - X1^3 - X0^3 );
coordinateRingElliptic = R2 / idealEllipticCurve;
ellipticHilbertPolynomial = hilbertPolynomial (coordinateRingElliptic);
```

```
ellipticDimension = dim (ellipticHilbertPolynomial);
ellipticDegree =  degree (ellipticHilbertPolynomial);
ellipticArithmeticGenus = (-1)^ellipticDimension * ( (ellipticHilbertPolynomial 0) - 1);

<< "Elliptic Curve has" << endl;
<< "ideal: " << transpose mingens idealEllipticCurve << endl;
<< "in ring: " << describe R2 << endl;
<< "Hilbert polynomial: " << ellipticHilbertPolynomial << endl;
<< "dimension: " << ellipticDimension << endl;
<< "degree: " << ellipticDegree << endl;
<< "arithmetic genus: " << ellipticArithmeticGenus << endl;

<< "Elliptic Curve: End" << endl << endl;
<< "------------------------------------------------------------------------" << endl;
```

7.3 Pari-Skripte

Ein Pari-Skript in der Datei <file> im Arbeitsverzeichnis von Pari wird mit dem Befehl

\r <file>

ausgeführt. Dabei wird der Name der Datei, ohne „“ eingegeben.

7.3.1 Pari-Skript *(Tool-Beispiel 6.1.6)*

```
/* Pari
/* Elliptic curves in Weierstrass normal form y^2 = x^3 + A*x + B */
default(format, "f0.3" );
print ("-----------------------------------------------------------------");
A = 1;
B = 0;
E = [ 0, 0, 0, A, B];
E = ellinit (E);
print ( "Elliptic curve:  y^2 = x^3 + ",E[4], "*x + ",E[5] );
print ( "Discr.: ", E.disc,);
print ( "j(E): ", E.j );
print ( "Root 1: ", E[14][1] );
print ( "Root 2: ", E[14][2] );
print ( "Root 3: ", E[14][3] );
print ( "Order of torsion group: ", elltors(E)[1] );
print ( "period tau: ", E[16]/E[15] );

p = [ E[14][1], 0];
print ( "Rational point p = ", p );
print ( "p + p = ", elladd(E, p, p) );
print ( p, " has order ", ellorder(E, p) );

print ("-----------------------------------------------------------------");
A = 0;
B = 1;
E = [ 0, 0, 0, A, B];
E = ellinit (E);
print ( "Elliptic curve:  y^2 = x^3 + ",E[4], "*x + ",E[5] );
print ( "Discr.: ", E.disc,);
print ( "j(E): ", E.j );
print ( "Root 1: ", E[14][1] );
print ( "Root 2: ", E[14][2] );
print ( "Root 3: ", E[14][3] );
```

```
print ( "Order of torsion group: ", elltors(E)[1] );
print ( "period tau: ", E[16]/E[15] );
p = [ E[14][1], 0];
print ( "Rational point p = ", p );
print ( "2p = ", ellpow(E, p, 2) );
print ( p, " has order ", ellorder(E, p) );

q = [2, 3];
print (  q, " is on curve? ", ellisoncurve(E, q) );
print ( "2q = ", ellpow(E, q, 2) );
print ( "3q = ", ellpow(E, q, 3) );
print ( "4q = ", ellpow(E, q, 4) );
print ( "5q = ", ellpow(E, q, 5) );
print ( "6q = ", ellpow(E, q, 6) );
print ( q, " has order ", ellorder(E, q) );

print ("----------------------------------------------------------------------");
```

7.3.2 Pari-Skript (Tool-Beispiel 6.1.8)

```
/* Pari
/* Elliptic curve with positive rank
/* Weierstrass normal form y^2 = x^3 + A*x + B */
default(format, "f0.3" );
print ("------------------------------------------------------------------");
A = -7;
B = 25/4;
E = [ 0, 0, 0, A, B];
E = ellinit (E);
print ( "Elliptic curve:  y^2 = x^3 + ",E[4], "*x + ",E[5] );
print ( "Discr.: ", E.disc,);
print ( "j(E): ", E.j );
print ( "Root 1: ", E[14][1] );
print ( "Root 2: ", E[14][2] );
print ( "Root 3: ", E[14][3] );
print ( "Order of torsion group: ", elltors(E)[1] );
print ( "period tau: ", E[16]/E[15] );



{
   for ( x = -3, 1000,
            s = ellordinate ( E, x);
            if ( length (s),
                                 y = s[1];
                                 print ( [x,    y    ] )  ;
                                 print ( [-x, -y-1 ] ) ;
            )
   );
}
print ("------------------------------------------------------------------");
```

7.3.3 Pari-Skript (Tool-Beispiel 6.2.7)

```
/* Pari */
/* Tori and corresponding elliptic curves in Weierstrass normal form y^2 = x^3 + A*x + B */
default(format, "f0.6" );
print ("-----------------------------------------------------------------");
/* create lattice */
omega_1 = 1;
omega_2 = -1/2 + (1/2)*I;
l = [ omega_1 , omega_2 ];
tau = omega_2/omega_1;
print ( "Torus belonging to lattice with periods");
print ("Omega_1: " polcoeff ( l, 1) );
print ("Omega_2: " polcoeff ( l, 2) );
print ( "j of lattice: ", ellj ( tau ) ) ;
print();

/* attach elliptic curve to torus */
wp_torus =  ellwp (l);
eisenstein_2 = 1/3 * polcoeff ( wp_torus, 2 );
eisenstein_3 = 1/5 * polcoeff ( wp_torus, 4 );
A_comp = -15 * eisenstein_2;
B_comp = -35 * eisenstein_3;
print ("Attached elliptic curve has Weierstrass normal form Y^2=X^3 + A*X + B with");
print ("A: ", A_comp);
print ("B: ", B_comp);

/* compare with elliptic curve */
A = 1;
B = 0;
E = [ 0, 0, 0, A, B];
E = ellinit (E);
print ();
print ( "Elliptic curve:  Y^2 = X^3 + ",E[4], "*X + ",E[5] );
print ( "has period: ", E[16]/E[15] );
print ( "j of curve: ", E.j  ) ;

print ("-----------------------------------------------------------------");
/* create lattice */
omega_1 = 1;
omega_2 = -1/2 + 0.288675*I;
l = [ omega_1 , omega_2 ];
```

```
tau = omega_2/omega_1;
print ( "Torus belonging to lattice with periods");
print ("Omega_1: " polcoeff ( l, 1) );
print ("Omega_2: " polcoeff ( l, 2) );
print ( "j of lattice: ", ellj ( tau ) ) ;
print();

/* attach elliptic curve to torus */
wp_torus =  ellwp (l);
eisenstein_2 = 1/3 * polcoeff ( wp_torus, 2 );
eisenstein_3 = 1/5 * polcoeff ( wp_torus, 4 );
A_comp = -15 * eisenstein_2;
B_comp = -35 * eisenstein_3;
print ("Attached elliptic curve has Weierstrass normal form Y^2=X^3 + A*X + B with");
print ("A: ", A_comp);
print ("B: ", B_comp);

/* compare with elliptic curve */
A = 0;
B = 1;
E = [ 0, 0, 0, A, B];
E = ellinit (E);
print ();
print ( "Elliptic curve:  Y^2 = X^3 + ",E[4], "*X + ",E[5] );
print ( "has period: ", E[16]/E[15] );
print ( "j of curve: ", E.j  ) ;

print ("-----------------------------------------------------------------");
/* create lattice */
omega_1 = 1;
omega_2 = 0.713227*I;
l = [ omega_1 , omega_2 ];
tau = omega_2/omega_1;
print ( "Torus belonging to lattice with periods");
print ("Omega_1: " polcoeff ( l, 1) );
print ("Omega_2: " polcoeff ( l, 2) );
print ( "j of lattice: ", ellj ( tau ) ) ;
print();

/* attach elliptic curve to torus */
wp_torus =  ellwp (l);
eisenstein_2 = 1/3 * polcoeff ( wp_torus, 2 );
```

```
eisenstein_3 = 1/5 * polcoeff ( wp_torus, 4 );
A_comp = -15 * eisenstein_2;
B_comp = -35 * eisenstein_3;
print ("Attached elliptic curve has Weierstrass normal form Y^2=X^3 + A*X + B with");
print ("A: ", A_comp);
print ("B: ", B_comp);

/* compare with elliptic curve */
A = -7;
B = 25/4;
E = [ 0, 0, 0, A, B];
E = ellinit (E);
print ();
print ( "Elliptic curve:  Y^2 = X^3 + ",E[4], "*X + ",E[5] );
print ( "has period: ", E[16]/E[15] );
print ( "j of curve: ", E.j , " rounded as ", 1.0 * E.j) ;

print ("-----------------------------------------------------------------");
```

8 Literatur

8.1 Kommutative Algebra

[AM1969] *Atiyah, M. F.; Macdonald, I. G.*: Introduction to Commutative Algebra. Addison Wesley, Reading 1969

[BW1998] *Becker, Thomas; Weispfenning, Volker*: Gröbner Bases: A Computational Approach to Commutative Algebra. Springer, Berlin et al. 1998

[Buc1998] *Buchberger, Bruno*: Introduction to Gröbner Bases. In: *Buchberger, Bruno; Winkler, Franz* (Hrsg.): Gröbner Bases and Appplications. Cambridge University Press, Cambridge 1998

[Eis1995] *Eisenbud, David*: Commutative algebra with a view toward algebraic geometry. Springer, New York 1995

8.2 Algebraische Geometrie

[CLO1997] *Cox, David; Little, John; O'Shea, Donal*: Ideals, Varieties, and Algorithms. Springer, New York 1997

[CLO1998] *Cox, David; Little, John; O'Shea, Donal*: Using Algebraic Geometry. Springer, New York 1998

[Die1974] *Dieudonné, Jean*: Cours de Géométrie Algébrique. Presses Universitaires de France, 1974

[EH2000] *Eisenbud, David; Harris, Joseph*: The Geometry of Schemes. Springer, New York 2000

[Har1977] *Hartshorne, Robin*: Algebraic Geometry. Springer, New York et al. 1977

[Mum1976] *Mumford, David*: Algebraic Geometry I. Complex Projective Varieties. Springer Berlin et al. 1976

[Sch2003] *Schenck, Henry*: Computational Algebraic Geomery. Cambridge University Press, Cambridge 2003

8.3 Zahlentheorie

[CS1986] *Cornell, Gary; Silverman, Joseph* (Hrsg.): Arithmetic Geometry. Springer, New York 1986

[CSS1995] *Cornell, Gary; Silverman, Joseph; Stevens, Glenn* (Hrsg.): Modular Forms and Fermat's Last Theorem. Springer, New York 1997

[Fal1984] *Faltings, Gerd*: Die Vermutungen von Tate und Mordell. Jahresber. Deutsch. Math.-Verein. Vol. 86 (1984), p. 1-13

[Fal1995] *Faltings, Gerd*: Der Beweis der Fermat-Vermutung durch R. Taylor und A. Wiles. Mitteilungen der Deutsch. Math.-Verein. Heft 2 (1995), p. 6-8

[For1996] *Forster, Otto*: Algorithmische Zahlentheorie. Vieweg, Braunschweig/Wiesbaden 1996

[Fre1984] *Frey, Gerhard*: Elementare Zahlentheorie. Vieweg, Braunschweig/Wiesbaden 1984

[IR1982] *Ireland, Kenneth; Rosen, Michael*: A Classical Introduction to modern Number Theory. Springer, New York 1982

[Maz1993] *Mazur, Barry*: On the Passage from Local to Global in Number Theory. Bulletin of the American Mathematical Society, Vol. 29 (1993)

[Ser1973] *Serre, Jean-Pierre*: A Course in Arithmetic. Sprnger. New York 1973

[Sil1986] *Silvermann, Joseph*: The Arithmetic of Elliptic Curves. Springer, New York 1986

8.4 Riemannsche Flächen

[Ahl1966] *Ahlfors, Lars*: Complex Analysis. An Introdution to the Theory of Analytic Functions of one Complex Variable. McGraw-Hill, Tokyo 1966

[For1977] *Forster, Otto*: Riemannsche Flächen. Springer, Berlin 1977

[Gun1972] *Gunning, Robert*: Vorlesungen über Riemannsche Flächen. Bibliographisches Institut, Heidelberg 1972

[Wey1913] *Weyl, Hermann*: Die Idee der Riemannschen Fläche. Nachdruck der Originalausgabe von 1913. Teubner, Leipzig 1977

8.5 Tools

8.5.1 Surf

Surf: http://surf.sourceforge.net/doc/manual.html

8.5.2 Singular

SINGULAR: http://www.singular.uni-kl.de

[GP2002] *Greuel, Gert-Martin; Pfister, Gerhard*: A Singular Introduction to Commutative Algebra. Springer, Berlin et al. 2002

8.5.3 Macaulay2

Macaulay2: http://www.math.uiuc.edu/Macaulay2

[EGS2002] *Eisenbud, David; Grayson, Daniel; Stillman, Michael; Sturmfels, Bernd* (Eds.): Computations in Algebraic Geometry with Macaulay2. Springer, Berlin et al. 2002

8.5.4 Pari

PARI. http://www.parigp-home.de

[COH1993] *Cohen, Henri*: A course in Computational Algebraic Number Theory. Springer, Berlin et al. 1993

[COH2000] *Cohen, Henri*: Advanced topics in Computational Algebraic Number Theory. Springer, Berlin et al. 2000