ALGEBRAISCHE GEOMETRIE

Skript zur Vorlesung
Technische Universität Dortmund
Sommersemester 2016

Daniel Plaumann

Fassung vom 17. Juli 2016

VORWORT

Dies ist das Skript zu einer vierstündigen Vorlesung im Sommersemester 2016 an der TU Dortmund. Ziel ist eine Einführung in die Algebraische Geometrie, inklusive algorithmischer Aspekte. Vorausgesetzt werden nur Grundkenntnisse in Algebra. Aus den vielen Übungsaufgaben in diesem Skript werden auch die wöchentlichen Hausaufgaben ausgewählt. Nähere Informationen zur Veranstaltung finden sich auf meiner Homepage.

https://www.mathematik.tu-dortmund.de/sites/daniel-plaumann

Ein Skript ist kein Lehrbuch:

- Es wird kein Anspruch auf Originalität erhoben. Aus den im Literaturverzeichnis genannten Büchern und Vorlesungsskripten ist vieles mal mehr mal weniger wörtlich übernommen, ohne dass dies im Einzelnen kenntlich gemacht wird.
- Erläuterungen und Zwischentexte sowie Zeichnungen fehlen oft.
- Vorsicht vor Fehlern aller Art!

Literatur

Einige Lehrbücher, die ich als Ergänzung zum Vorlesungsskript empfehlen möchte.

[Hulek] K. Hulek, *Elementare algebraische Geometrie*. Springer Spektrum (2000) — Eine sehr gute Einführung. Zu Beginn abstrakter und weniger algorithmisch als diese Vorlesung.

[Kunz] E. Kunz, *Einführung in die algebraische Geometrie*. Vieweg Aufbaukurs Mathematik 87 (1997) — Noch ein deutschsprachiges Buch. Technisch anspruchsvoller.

[Reid] M. Reid, *Undergraduate Algebraic Geometry*. LMS Student Texts (1989) — mit viel Geometrie und motivierenden Beispielen.

[Cox-Little-O'Shea] D. Cox, J. Little, D. O'Shea, *Ideals, varieties and algorithms*. Springer UTM (1992) — Eine Einführung mit Schwerpunkt auf algorithmischen Aspekten. Sehr gut lesbar, inzwischen ein Klassiker.

[Harris] J. Harris, *Algebraic Geometry. A first course*. Springer GTM 133 (1992) — Haufenweise spannendes Material, starker Fokus auf der Geometrie, Schwierigkeitsgrad und Ausführlichkeit variieren erheblich.

[Hartshorne] R. Hartshorne, *Algebraic Geometry*. Springer GTM 52 (1977) — Die Bibel unter den Lehrbüchern zur modernen algebraischen Geometrie. Umfangreich, hervorragend geschrieben, technisch sehr anspruchsvoll.

[Shafarevich] I. Shafarevich, *Basic algebraic geometry 1*. Springer 1977 — Trotz des Titels sehr anspruchsvoll, aber weniger dicht geschrieben als Hartshorne.

[Atiyah-Macdonald] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*. Addison-Wesley (1969) — Ein weiterer Klassiker. Das wichtigste zur kommutativen Algebra knapp aber sehr klar dargestellt.

[Greuel-Pfister] G.-M. Greuel, G. Pfister, *A* Singular *Introduction to Commutative Algebra*. Springer (2008) — Umfassende Übersicht über algorithmische kommutative Algebra und ihre Umsetzung im Softwarepaket Singular.

[Eisenbud] D. Eisenbud, *Commutative Algebra. With a view toward algebraic geometry*. Springer GTM 150 (1995) — Umfangreiches Werk zur kommutativen Algebra. Gut lesbar, variiert stark im Schwierigkeitsgrad.

[Bosch] S. Bosch, *Algebra*. Springer-Lehrbuch, 8. Aufl. (2013) — Werde ich verwenden, wenn ich ein Ergebnis aus der Algebra-Vorlesung zitieren will.

Außerdem muss ich die Vorlesungsskripten von **Claus Scheiderer** (Universität Konstanz), **Marco Manetti** (Università di Roma I) und **Andreas Gathmann** (Universität Kaiserslautern) erwähnen, aus denen ich zum Teil hemmungslos abgeschrieben habe. Von Scheiderer kommen insbesondere große Teile des Kapitels über Gröbnerbasen. Bei Manetti habe ich mich beim Beweis des Nullstellensatzes und zum Teil bei den Grundlagen der projektiven Geometrie bedient.

Inhaltsverzeichnis

Daniel Plaumann
Technische Universität Dortmund
Sommersemester 2016
Fassung vom 17. Juli 2016

1. AFFINE VARIETÄTEN

1.1. Einführung

Die algebraische Geometrie untersucht die Lösungen von polynomialen Gleichungssystemen

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \dots, x_n) &= 0. \end{aligned}$$

Dabei sind $f_1, \dots, f_m$ Polynome in den Variablen $x_1, \dots, x_n$ mit Koeffizienten in einem Körper, z.B. $\mathbb{Q}$. Die Polynome sind die *Algebra*, in der Lösungsmenge steckt dagegen die *Geometrie*.

In der *linearen Algebra* lernt man alles über den Fall, dass die Gleichungen linear sind, die Polynome also vom Grad höchstens 1. Die Geometrie ist in diesem Fall die der linearen (oder affin-linearen) Unterräume. Dagegen lernt man in der *Algebra* , dass die Dinge bei Gleichungen höheren Grades viel komplizierter werden, schon bei einer Gleichung in einer Variablen. Die Lösungen, also die Nullstellen, liegen dann nicht mehr in $\mathbb{Q}$, sondern in Erweiterungskörpern. Für die allgemeine Gleichung vom Grad mindestens 5 ist es dabei nicht möglich, die Lösungen durch Wurzelziehen zu bestimmen (Satz von Abel-Ruffini). Von der Algebra darf man hier also keine Wunder erwarten! Wenn man andererseits diesen Aspekt erst einmal beiseite lässt und die Lösungen in einem algebraisch abgeschlossen Körper studiert, wie den komplexen Zahlen, dann zerfallen immerhin alle Polynome in einer Variablen in Linearfaktoren. Aber über den Fall mehrerer Gleichungen in mehreren Variablen ist damit immer noch gar nichts gesagt.

Einige grundlegende Fragen der algebraischen Geometrie sind die folgenden:

- Inwieweit lässt sich das Eliminationsverfahren für lineare Gleichungssysteme auch auf Systeme von höherem Grad übertragen?
- Wie kann man entscheiden, ob ein polynomiales Gleichungssystem über einem algebraisch abgeschlossenen Körper lösbar ist?
- Kann man die Lösungsmenge eines polynomialen Gleichungssystems parametrisieren?
- In welcher Weise lassen sich den Lösungsmengen geometrische Eigenschaften wie Dimension, Glattheit usw. zuordnen?
- Wenn es nur endlich viele Lösungen gibt, was kann man dann über ihre Anzahl sagen?
- Wie kommt die Algebra mit der klassischen Geometrie von Kurven und Flächen in der Ebene und im Raum zusammen?

Diese Liste sieht vielleicht erst mal nach viel Algebra und wenig Geometrie aus. Es zeigt sich aber, dass man auch auf der geometrischen Seite arbeiten muss, um algebraische Fragen zu beantworten. Insbesondere werden wir uns ausführlich mit der *projektiven Geometrie* beschäftigen.

1.2. Affine Varietäten

Im folgenden sei immer k ein Körper und K ein Erweiterungskörper von k. Wir setzen immer voraus, dass K **algebraisch abgeschlossen** ist. Bekanntlich bedeutet dies, dass über dem Körper K jedes Polynom in einer Variablen in Linearfaktoren zerfällt. Der Körper k wird der Körper sein, über dem die Polynome und damit Gleichungen definiert sind. Die Lösungen dagegen betrachten wir im algebraisch abgeschlossenen Körper K. Zum Beispiel kann $k = \mathbb{Q}$ und $K = \mathbb{C}$ sein (und fast alle Phänomene in dieser Vorlesung lassen sich an diesem Beispiel verstehen). Im allgemeinen setzen wir aber nichts über die Charakteristik von k und K voraus.

Der **affine Raum** der Dimension n über K ist die Menge K^n, in der algebraischen Geometrie mit $\mathbb{A}^n_K$ oder, bei fixiertem K, einfach $\mathbb{A}^n$ bezeichnet. Insbesondere heißt $\mathbb{A}^1$ die **affine Gerade** und $\mathbb{A}^2$ die **affine Ebene**. Ein Element $p \in \mathbb{A}^n$ heißt ein **Punkt**, und ist $p = (a_1, \dots, a_n)$, dann heißen die Einträge $a_i \in K$ die **Koordinaten** von p. Es sei $k[x_1, \dots, x_n]$ der Polynomring in n Veränderlichen über k. Ein Polynom f definiert eine Funktion $f\colon K^n \to K$, $p \mapsto f(p) = f(a_1, \dots, a_n)$, für $p = (a_1, \dots, a_n)$. Wir schreiben

$$\mathcal{V}(f) \;=\; \big\{p \in \mathbb{A}^n \colon f(p) = 0\big\}$$

für die Menge aller **Nullstellen** von f. Ist allgemeiner $T \subset k[x_1, \dots, x_n]$ irgendeine Menge von Polynomen, dann schreiben wir

$$\mathcal{V}(T) \;=\; \big\{p \in \mathbb{A}^n \colon f(p) = 0 \text{ für alle } f \in T\big\}$$

oder manchmal zur Verdeutlichung $\mathcal{V}_K(T) \subset \mathbb{A}^n_K$ für die gemeinsame Nullstellenmenge aller Polynome in T. Eine Teilmenge $V \subset \mathbb{A}^n$ heißt eine **affine k-Varietät**, wenn $V = \mathcal{V}(T)$ für irgendeine Menge T von Polynomen mit Koeffizienten in k gilt.

Beispiele 1.1. (1) Die leere Menge und der ganze Raum $\mathbb{A}^n$ sind affine k-Varietäten, denn es gilt $\mathcal{V}(1) = \varnothing$ und $\mathcal{V}(0) = \mathbb{A}^n$.

(2) Die affinen k-Varietäten $V \subsetneq \mathbb{A}^1$ sind endlich. Denn ein Polynom $f \in k[x]$, $f \neq 0$, hat nur endlich viele Nullstellen in $K = \mathbb{A}^1$.

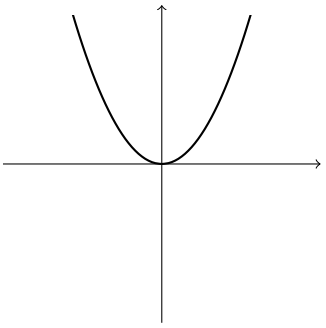
(3) Ist $k = K$, dann ist umgekehrt jede endliche Teilmenge von $\mathbb{A}^1$ eine affine K-Varietät. Denn ist $V = \{a_1, \dots, a_m\} \subset \mathbb{A}^1 = K$, dann gilt einfach

$$V = \mathcal{V}(f) \text{ mit } f = (x - a_1)\cdots(x - a_m).$$

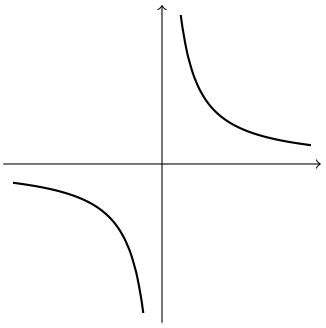
(4) Ist dagegen $k \subsetneq K$, dann gibt es in aller Regel endliche Teilmengen von $\mathbb{A}^1$, die keine affinen k-Varietäten sind. Ist z.B. $k = \mathbb{Q}$ und $K = \mathbb{C}$, dann ist $V = \{i\}$ (mit $i = \sqrt{-1}$) keine $\mathbb{Q}$-Varietät, denn für ein Polynom $f \in \mathbb{Q}[x]$ mit $f(i) = 0$ gilt immer auch $f(-i) = 0$. Mit anderen Worten, jede affine $\mathbb{Q}$-Varietät in $\mathbb{A}^1_{\mathbb{C}}$, die i enthält, muss auch $-i$ enthalten. Auch $V = \{\pi\}$ ist keine $\mathbb{Q}$-Varietät, da es gar kein Polynom $f \neq 0$ mit Koeffizienten in $\mathbb{Q}$ gibt, das in π verschwindet.[1]

(5) In der affinen Ebene sind unter den affinen k-Varietäten außer den endlichen Teilmengen zum Beispiel auch vertraute geometrische Figuren wie

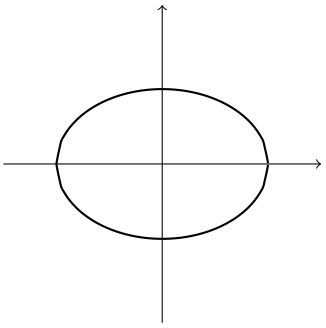
[1]Diese Tatsache ist recht bekannt aber keineswegs trivial; die Transzendenz von π wurde zuerst im Jahr 1882 von Ferdinand von Lindemann (1852–1939) bewiesen.



Parabel $\mathcal{V}(x_2 - x_1^2)$



Hyperbel $\mathcal{V}(1 - x_1x_2)$



Ellipse $\mathcal{V}(x_1^2 + 2x_2^2 - 4)$

Genau betrachtet ergeben sich die 'vertrauten geometrischen Figuren' natürlich nur über den reellen Zahlen, also für $K = \mathbb{R}$, was wir ja andererseits verboten haben, da K algebraisch abgeschlossen sein soll, etwa $K = \mathbb{C}$. Trotzdem orientiert sich die Geometrie immer an reellen Bildern. Zum Beispiel denken wir uns $\mathbb{A}^1_K$ immer als Gerade und nicht z.B. als komplexe Zahlenebene.

Der Körper k, über dem die algebraischen Gleichungen definiert sind, ist beliebig, aber von vorne herein betrachten wir Varietäten, also Lösungsmengen, nur mit Koordinaten im algebraisch abgeschlossenen Körper K. Natürlich ist es mindestens genauso interessant, Lösungen in Körpern zu betrachten, die nicht algebraisch abgeschlossen sind, zum Beispiel die Fälle $K = \mathbb{R}$ oder $K/\mathbb{Q}$ endlich (Zahlkörper). Dafür braucht es aber fast immer ganz eigene Methoden, die wir in dieser Vorlesung nicht diskutieren.

Proposition 1.2. *Die Vereinigung endlich vieler affiner k-Varietäten ist wieder eine solche, ebenso der Durchschnitt beliebig vieler affiner k-Varietäten. Die leere Menge und der ganze Raum sind affine k-Varietäten.*

Beweis. Für die Aussage über endliche Vereinigungen reicht es zu beweisen, dass die Vereinigung von zwei affinen k-Varietäten wieder eine ist, dann folgt der allgemeine Fall per Induktion. Falls also $V_1 = \mathcal{V}(T_1)$ und $V_2 = \mathcal{V}(T_2)$, dann ist $V_1 \cup V_2 = \mathcal{V}(T_1T_2)$, wobei T_1T_2 aus allen Produkten f_1f_2, $f_1 \in T_1$, $f_2 \in T_2$ besteht. Um das zu beweisen, sei $p \in V_1 \cup V_2$, dann also $p \in V_1$ oder $p \in V_2$. Es verschwindet also jedes Polynom aus T_1 oder jedes Polynom aus T_2 in p und damit auch jedes Polynom aus T_1T_2. Ist umgekehrt $p \in \mathcal{V}(T_1T_2)$ und $p \notin V_1$, dann gibt es also $f_1 \in T_1$ mit $f_1(p) \neq 0$. Andererseits gilt für jedes $f_2 \in T_2$ nach Annahme $(f_1f_2)(p) = f_1(p)f_2(p) = 0$ und damit $f_2(p) = 0$. Also folgt $p \in V_2$.

Ist $V_i = \mathcal{V}(T_i)$ eine beliebig indizierte Familie von affinen k-Varietäten, so gilt $\bigcap_i V_i = \mathcal{V}(\bigcup_i T_i)$, wie man leicht sieht. Schließlich gilt $\mathcal{V}(1) = \varnothing$ und $\mathcal{V}(0) = \mathbb{A}^n$, wie schon bemerkt. ∎

Definition 1.3. Nach Prop. 1.2 verhalten sich die affinen k-Varietäten wie die abgeschlossenen Mengen einer Topologie auf dem affinen Raum. Diese heißt die k-**Zariski-Topologie**[2] auf $\mathbb{A}^n$. Die affinen k-Varietäten werden deshalb auch die k-**Zariski-abgeschlossenen** oder einfach die k-**abgeschlossenen Teilmengen** von $\mathbb{A}^n$ genannt.

Im Moment brauchen wir noch keine topologischen Konzepte und 'Zariski-abgeschlossene Menge' ist einfach nur ein anderes Wort für affine k-Varietät.

[2] Oscar Zariski (1899–1986), russisch-US-amerikanischer Mathematiker, berühmt für seine Beiträge zur kommutativen Algebra und algebraischen Geometrie

Eine grundlegende Frage, die wir in den folgenden Abschnitten untersuchen werden, ist:

> Gegeben zwei Mengen T, T' von Polynomen, wie kann man entscheiden, ob die durch sie bestimmten affinen k-Varietäten $\mathcal{V}(T)$ und $\mathcal{V}(T')$ übereinstimmen?

Wenn man $T' = \{1\}$ setzt, dann ist $\mathcal{V}(T') = \varnothing$. Eingeschlossen in die allgemeine Frage ist also der wichtige Spezialfall, wie man entscheiden kann, ob $\mathcal{V}(T)$ die leere Menge, das durch T bestimmte polynomiale Gleichungssystem also unlösbar ist.

Frage 1.4. Wie würden Sie entscheiden, ob zwei *lineare* Gleichungssysteme dieselben Lösungen haben?

Erinnerung an die Algebra: Ein **Ring** meint in dieser Vorlesung immer einen kommutativen Ring mit Einselement 1. Ein **Ideal** in einem Ring R ist eine Teilmenge $I \subset R$ mit den Eigenschaften

$$0 \in I, \quad I + I \subset I, \quad R \cdot I \subset I.$$

Ein Ringelement $r \in R$ heißt eine **Einheit**, wenn es $r^{-1} \in R$ mit $rr^{-1} = 1$ gibt. Die Menge der Einheiten wird mit $R^\times$ bezeichnet. Wenn ein Ideal I eine Einheit enthält, dann gilt $I = R$. Denn ist $r \in I \cap R^\times$, dann $s = (sr^{-1})r \in I$ für jedes $s \in R$. Insbesondere gilt $I = R$ genau dann, wenn $1 \in I$.

Gegeben $T \subset R$, dann schreiben wir $\langle T \rangle$ für das von T in R **erzeugte Ideal**. Jedes Element $f \in \langle T \rangle$ hat eine Darstellung

$$f = f_1 \cdot g_1 + \cdots + f_r \cdot g_r$$

wobei $f_1, \ldots, f_r \in R$ und $g_1, \ldots, g_r \in T$ ($r \geqslant 0$). Außerdem ist die 'leere Summe' 0, d.h. $\langle \varnothing \rangle = \{0\}$. Eine Teilmenge T eines Ideals I, die I erzeugt, wird **Erzeugendensystem** genannt oder auch **Basis** (obwohl im Unterschied zur Basis eines Vektorraums keinerlei Unabhängigkeit zwischen den Erzeugern gefordert ist, in welchem Sinn auch immer).

Im Polynomring gilt nun:

$$\mathcal{V}(T) = \mathcal{V}\big(\langle T \rangle\big) \qquad \text{für alle } T \subset K[x_1, \ldots, x_n].$$

Denn wegen $T \subset \langle T \rangle$ gilt $\mathcal{V}(\langle T \rangle) \subset \mathcal{V}(T)$. Ist umgekehrt $p \in \mathcal{V}(T)$, dann verschwindet jedes Polynom aus T in p und damit auch jedes Polynom aus $\langle T \rangle$.

Die Bedeutung von Idealen für die algebraische Geometrie ist immens. Die Erzeuger entsprechen den Ausgangsgleichungen. Das erzeugte Ideal enthält alle Vielfachen, Summen und Produkte der Erzeuger. Damit enthält es insbesondere jede elementare **Umformung** der ursprünglichen Gleichungen, wie man sie etwa aus der linearen Algebra kennt. Das Ideal verwaltet also alle möglichen Umformungen und Vereinfachungen der Gleichungen. Das schöne an Idealen ist, dass sie immer endlich erzeugt sind, selbst wenn man nicht mit endlich vielen Erzeugern startet:

> **Satz 1.5** (Hilbertscher[3] Basissatz)**.** *Jedes Ideal im Polynomring $k[x_1, \ldots, x_n]$ über einem Körper k ist endlich erzeugt. Genauer gilt: Für jede Teilmenge $T \subset k[x_1, \ldots, x_n]$ gibt es eine endliche Teilmenge T' von T mit $\langle T' \rangle = \langle T \rangle$.*

[3]David Hilbert (1862–1943) bewies den Basissatz im Jahr 1888.

Allgemeiner heißt ein Ring R **noethersch**[4], wenn jedes seiner Ideale endlich erzeugt ist. Die Aussage des Basissatzes ist also gerade, dass der Polynomring über einem Körper noethersch ist.[5] Der Hilbertsche Basissatz und sein Beweis sind wahrscheinlich aus der Vorlesung Algebra bekannt. Wir geben aber später auch noch einen unabhängigen Beweis.

Korollar 1.6. *Jede affine k-Varietät wird von endlich vielen Polynomen beschrieben. Genauer gibt es zu jeder Teilmenge T von $k[x_1, \dots, x_n]$ eine endliche Teilmenge T' von T mit $\mathcal{V}(T) = \mathcal{V}(T')$.* ■

Wir können also eine Menge von Polynomen immer durch das erzeugte Ideal ersetzen, und umgekehrt jedes Ideal durch eine endliche Menge von Erzeugern, ohne die zugehörige affine k-Varietät zu verändern.

Zu jedem Gleichungssystem gehört also ein Ideal. Es gehört aber auch zu jeder Teilmenge $M \subset \mathbb{A}^n$ ein Ideal, nämlich

$$\mathcal{I}_k(M) \;=\; \big\{f \in k[x_1, \dots, x_n] \colon f(p) = 0 \text{ für alle } p \in M\big\},$$

das k-**Verschwindungsideal** von M. Meistens lassen wir k weg und schreiben nur $\mathcal{I}(M)$.

Nach dem Basissatz ist das k-Verschwindungsideal einer Menge endlich erzeugt. Es ist aber alles andere als klar, wie man Erzeuger von $\mathcal{I}(M)$ finden kann. Ist I ein Ideal in $k[x_1, \dots, x_n]$, dann gilt per Definition immer

$$I \subset \mathcal{I}\big(\mathcal{V}(I)\big).$$

In wie weit hier Gleichheit gilt ist eine zentrale Frage, die auf den Hilbertschen Nullstellensatz führt. Damit befassen wir uns später in diesem Kapitel. Ist $I = \langle f_1, \dots, f_r \rangle$, dann enthält I also alle Gleichungen, die direkt durch Umformung aus den gegebenen Gleichungen $f_1 = \cdots = f_r = 0$ hervorgehen. Hingegen enthält das volle Verschwindungsideal $\mathcal{I}(V)$ alle Gleichungen, die sich überhaupt aus den Ausgangsgleichungen ergeben können.

Proposition 1.7. *(a) Die Zuordnungen $\mathcal{I}$ und $\mathcal{V}$ sind inklusionsumkehrend, d.h. aus $M_1 \subset M_2 \subset \mathbb{A}^n$ folgt $\mathcal{I}(M_2) \subset \mathcal{I}(M_1)$ und aus $T_1 \subset T_2 \subset k[x_1, \dots, x_n]$ folgt $\mathcal{V}(T_2) \subset \mathcal{V}(T_1)$.*

(b) Für $M_1, M_2 \subset \mathbb{A}^n$ gilt $\mathcal{I}(M_1 \cup M_2) = \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$.

(c) Für jede Teilmenge $M \subset \mathbb{A}^n$ ist $\mathcal{V}(\mathcal{I}(M))$ die kleinste affine k-Varietät in $\mathbb{A}^n$, die M enthält. Insbesondere ist eine Teilmenge $V \subset \mathbb{A}^n$ genau dann eine affine k-Varietät, wenn gilt:

$$V = \mathcal{V}(\mathcal{I}(V)).$$

(d) Für zwei affine k-Varietäten $V_1, V_2 \subset \mathbb{A}^n$ gilt

$$V_1 = V_2 \quad \Longleftrightarrow \quad \mathcal{I}(V_1) = \mathcal{I}(V_2).$$

[4] Emmy Noether (1882–1935), deutsche Mathematikerin, Begründerin der modernen kommutativen Algebra

[5] Eine allgemeinere Version des Basissatzes sagt, dass der Polynomring $R[x]$ in einer Variablen über einem noetherschen Ring R wieder noethersch ist. Da jeder Körper ein noetherscher Ring ist, bekommt man daraus den Basissatz in der oben gegebenen Form durch Induktion nach der Anzahl der Variablen. Gleichzeitig erhält man die Aussage auch noch in weiteren Polynomringen, z.B. in $\mathbb{Z}[x_1, \dots, x_n]$, da auch $\mathbb{Z}$ ein noetherscher Ring ist.

Beweis. (a) und (b) sind trivial und (d) folgt aus (c); (c) Per Definition ist $\mathcal{V}(\mathcal{I}(M))$ eine affine k-Varietät und enthält M. Ist V eine affine k-Varietät, die M enthält, dann gibt es $T \subset k[x_1, \ldots, x_n]$ mit $V = \mathcal{V}(T)$. Dann also $T \subset \mathcal{I}(V) \subset \mathcal{I}(M)$ und somit $\mathcal{V}(\mathcal{I}(M)) \subset \mathcal{V}(T) = V$. ∎

Für jede Teilmenge $M \subset \mathbb{A}^n$ ist $\mathcal{V}(\mathcal{I}(M))$ also die kleinste k-abgeschlossene Menge, die M enthält und entspricht damit dem Abschluss in der k-Zariski-Topologie. Wir schreiben

$$\overline{M} = \mathcal{V}(\mathcal{I}_k(M))$$

und nennen diese Menge den k-**Zariski-Abschluss** von M. Eine Teilmenge $M \subset V$ heißt k-**Zariski-dicht** in der affinen k-Varietät V, wenn $\overline{M} = V$ gilt. Zum Beispiel haben wir schon bemerkt, dass jede in $\mathbb{A}^1$ echt enthaltene k-Varietät endlich ist. Deswegen ist jede unendliche Teilmenge von $\mathbb{A}^1$ Zariski-dicht in $\mathbb{A}^1$. Wenn es auf die Rolle von k ankommt, verwenden wir der Deutlichkeit halber die Notation $\mathrm{clos}_k(M)$.

Definition 1.8. Es sei V eine affine k-Varietät in $\mathbb{A}^n$. Die k-abgeschlossenen Teilmengen von V sind genau die affinen k-Varietäten in $\mathbb{A}^n$, die in V enthalten sind. Man nennt eine solche Teilmenge auch eine **abgeschlossene Untervarietät**. Die Varietät V heißt **reduzibel (über k)**, wenn sie die Vereinigung von zwei echten k-abgeschlossenen Teilmengen ist, es also abgeschlossene Untervarietäten $V_1, V_2 \subset V$ gibt mit

$$V = V_1 \cup V_2 \quad \text{und} \quad V_1, V_2 \neq V.$$

Es spielt dabei keine Rolle, ob der Durchschnitt $V_1 \cap V_2$ leer ist oder nicht. Die Varietät V heißt **irreduzibel (über k)**, wenn sie nicht leer und nicht reduzibel (über k) ist.

Proposition 1.9. *Eine affine k-Varietät ist genau dann irreduzibel über k, wenn ihr k-Verschwindungsideal ein Primideal ist.*

Beweis. Sei $V \subset \mathbb{A}^n$, $V \neq \varnothing$, und $I = \mathcal{I}(V) \subsetneq k[x_1, \ldots, x_n]$. Falls I nicht prim ist, dann gibt es also $f_1, f_2 \in k[x_1, \ldots, x_n]$ mit $f_1, f_2 \notin I$ aber $f_1 f_2 \in I$. Dann sind $V_1 = V \cap \mathcal{V}(f_1) \subsetneq V$ und $V_2 = V \cap \mathcal{V}(f_2) \subsetneq V$ zwei affine k-Varietäten mit $V = V_1 \cup V_2$, wegen $f_1 f_2 \in I$. Also ist V reduzibel.

Ist umgekehrt $V \neq \varnothing$ nicht irreduzibel, also $V = V_1 \cup V_2$ mit $V_1, V_2 \subsetneq V$, so wähle $p_i \in V \setminus V_i$ und ein Polynom $f_i \in \mathcal{I}(V_1)$ mit $f_i(p_i) \neq 0$, für $i = 1, 2$. Dann gilt also $f_1, f_2 \notin I$, aber $f_1 f_2 \in I$ wegen $V = V_1 \cup V_2$. Also ist I nicht prim. ∎

Beispiele 1.10. (1) Es sei $f \in k[x_1, \ldots, x_n]$ ein nicht-konstantes Polynom. Genau dann ist die Varietät $\mathcal{V}(f)$ irreduzibel, wenn f als Polynom irreduzibel ist. Denn ist $f = f_1 \cdots f_r$ die Zerlegung von f in seine irreduziblen Faktoren, dann ist

$$\mathcal{V}(f) = \mathcal{V}(f_1) \cup \cdots \cup \mathcal{V}(f_r).$$

Dabei ist jede der Varietäten $\mathcal{V}(f_i)$ irreduzibel. (Um das zu beweisen, müssen wir allerdings wissen, dass $\langle f_i \rangle = \mathcal{I}(\mathcal{V}(f_i))$ gilt, was aus dem Nullstellensatz folgt; siehe Cor. 1.38).

(2) Zum Beispiel hat das Polynom $f = x^3 + xy^2 - x^2 - y^2 - 4x + 4$ die Faktorisierung

$$f = f_1 f_2 \quad \text{mit} \quad f_1 = x^2 + y^2 - 4 \text{ und } f_2 = x - 1.$$

Die Varietät $\mathcal{V}(f)$ zerfällt also in zwei abgeschlossene Untervarietäten. Dabei beschreibt $\mathcal{V}(f_1)$ einen Kreis in der affinen Ebene und $\mathcal{V}(f_2)$ eine Gerade.

(3) Der Begriff der Irreduzibilität kann vom Grundkörper k abhängen. Betrachte zum Beispiel das Polynom $x^2 - 2 \in k[x]$, $k \subset \mathbb{C}$. Die zugehörige Varietät $\mathcal{V}(x^2 - 2) \subset \mathbb{A}^1$ besteht aus den beiden Punkten $\sqrt{2}, -\sqrt{2}$. Sie ist irreduzibel über $\mathbb{Q}$, denn $x^2 - 2$ ist ein über $\mathbb{Q}$ irreduzibles Polynom. Für $k = \mathbb{C}$ oder $k = \mathbb{R}$ gilt dagegen $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ und jeder der beiden Punkte $\sqrt{2}, -\sqrt{2}$ ist selbst eine irreduzible Varietät, ihre Vereinigung dagegen reduzibel.

Analog zu diesen Beispielen analysieren wir als nächstes die Zerlegung von Varietäten in irreduzible abgeschlossene Teilmengen. Dazu brauchen wir etwas Vorbereitung.

Lemma 1.11. *Ein Ring R ist genau dann noethersch, wenn er die aufsteigende Kettenbedingung für Ideale erfüllt: Ist $I_1 \subset I_2 \subset I_3 \subset \cdots$ eine unendlich aufsteigende Kette von Idealen in R, dann gibt es einen Index $m \in \mathbb{N}$ mit $I_j = I_m$ für alle $j \geqslant m$.*

Beweis. Sei R noethersch und eine aufsteigende Kette von Idealen wie in der Behauptung gegeben. Dann ist die Vereinigung $I = \bigcup_{j=1}^{\infty} I_j$ wieder ein Ideal in R. Da R noethersch ist, ist I endlich erzeugt. Also gibt es einen Index m derart, dass I_m die endlich vielen Erzeuger von I alle enthält. Dann folgt $I_j = I_m$ für alle $j \geqslant m$.

Umgekehrt sei die aufsteigende Kettenbedingung für Ideale erfüllt. Angenommen R wäre nicht noethersch. Sei dann I ein Ideal in R, das nicht endlich erzeugt ist. Wähle $f_1 \in I$ beliebig. Dann gilt $\langle f_1 \rangle \subsetneq I$ und wir wählen $f_2 \in I \smallsetminus \langle f_1 \rangle$. Allgemein definieren wir induktiv $I_j = \langle f_1, \ldots, f_j \rangle$ und wählen $f_{j+1} \in I \smallsetminus I_j$, für $j \geqslant 1$. Also ist $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ eine unendlich aufsteigende Kette von Idealen, die nicht stationär wird. Dieser Widerspruch zeigt die Behauptung. ∎

Korollar 1.12. *Jede nicht-leere Menge von k-Varietäten in $\mathbb{A}^n$ besitzt ein bezüglich Inklusion minimales[6] Element.*

Beweis. Sei $\mathcal{A}$ eine nicht-leere Menge von k-Varietäten in $\mathbb{A}^n$. Angenommen falsch. Sei $V_1 \in \mathcal{A}$. Da V_1 nicht minimal ist, gibt es also $V_2 \in \mathcal{A}$ mit $V_2 \subsetneq V_1$. Induktiv finden wir $V_{j+1} \in \mathcal{A}$ mit $V_{j+1} \subsetneq V_j$ für $j \geqslant 1$. Wir erhalten also eine unendlich absteigende Kette $V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots$ in $\mathcal{A}$. Dann ist

$$\mathcal{I}(V_1) \subsetneq \mathcal{I}(V_2) \subsetneq \mathcal{I}(V_3) \subsetneq \cdots$$

eine unendlich echt aufsteigende Kette von Idealen in $k[x_1, \ldots, x_n]$, im Widerspruch zum vorangehenden Lemma. ∎

Satz 1.13. *Jede affine k-Varietät V ist eine endliche Vereinigung*

$$V = V_1 \cup \cdots \cup V_m$$

von irreduziblen abgeschlossenen Untervarietäten $V_1, \ldots, V_m$ mit $V_i \not\subset V_j$ für $i \neq j$.
Dabei sind $V_1, \ldots, V_m$ bis auf Vertauschung eindeutig bestimmt.

Definition 1.14. Die Untervarietäten $V_1, \ldots, V_m$ heißen die **irreduziblen Komponenten** von V.

[6] *Erinnerung:* Ein Element a in einer partiell geordneten Menge $(A, \leqslant)$ heißt *minimal*, wenn für alle $b \in A$ gilt: $(b \leqslant a) \Rightarrow (b = a)$. Besitzt A hingegen die viel stärkere Eigenschaft $\forall b \in A\colon a \leqslant b$, so heißt a ein *kleinstes Element*.

Beweis. Wir zeigen zunächst, dass jede affine k-Varietät eine endliche Vereinigung von irreduziblen k-abgeschlossenen Teilmengen ist. Sei dazu $\mathcal{A}$ die Menge aller k-Varietäten in $\mathbb{A}^n$, die *nicht* die Vereinigung von endlich vielen irreduziblen k-abgeschlossenen Teilmengen sind. Wir wollen also zeigen, dass $\mathcal{A}$ die leere Menge ist. Angenommen falsch, dann enthält $\mathcal{A}$ nach dem vorangehenden Korollar ein minimales Element V. Nun kann V selbst nicht irreduzibel sein. Es gibt also k-Varietäten $W, W' \subsetneq V$ mit $V = W \cup W'$. Wegen der Minimalität von V folgt $W, W' \notin \mathcal{A}$. Also sind W und W' beide die Vereinigung von endlich vielen irreduziblen k-abgeschlossenen Teilmengen. Damit ist es aber auch V, ein Widerspruch.[7]

Sei nun V eine affine k-Varietät in $\mathbb{A}^n$ und $V = V_1 \cup \cdots \cup V_m$ eine Zerlegung in irreduzible k-abgeschlossene Teilmengen. Falls $V_i \subset V_j$ für irgendein Paar $i \neq j$ gilt, dann können wir V_i natürlich einfach weglassen. Wir können also annehmen, dass zwischen den $V_1, \ldots, V_m$ keine solchen Inklusionen bestehen. Ist nun

$$V = W_1 \cup \cdots \cup W_\ell$$

eine weitere solche Zerlegung in irreduzible abgeschlossene Teilmengen, dann gilt

$$V_i = V_i \cap V = (V_i \cap W_1) \cup \cdots \cup (V_i \cap W_\ell)$$

für jedes $i = 1, \ldots, m$. Da V_i irreduzibel ist, gibt es ein r mit $V_i \subset W_r$. Andererseits können wir dasselbe Argument umgekehrt mit W_r machen. Es gibt also j mit $W_r \subset V_j$ und damit $V_i \subset W_r \subset V_j$. Es folgt $i = j$ und $V_i = W_r$. Also kommt jedes V_i auch unter den $W_1, \ldots, W_\ell$ vor, insbesondere $m \leqslant \ell$. Indem wir die beiden Zerlegungen vertauschen, erhalten wir $m = \ell$. ∎

Frage 1.15. Warum ist die Bedingung $V_i \not\subset V_j$ für $i \neq j$ entscheidend für die Eindeutigkeit der Zerlegung in irreduzible Komponenten?

Sind f, g irreduzible Elemente in einem Ring R, dann schreiben wir $f \sim g$, wenn es eine Einheit $a \in R^\times$ mit $f = ag$ gibt und entsprechend $f \nsim g$, wenn das nicht der Fall ist. Sind f und g irreduzible Polynome in $k[x_1, \ldots, x_n]$, dann bedeutet $f \sim g$ also gerade, dass es eine Konstante $a \in k^\times$ mit $f = ag$ gibt. Ein Polynom $f \in k[x_1, \ldots, x_n]$ heißt **reduziert**, wenn f keinen mehrfachen irreduziblen Faktor enthält, d.h. es gibt irreduzible Polynome $f_1, \ldots, f_r$ mit

$$f = f_1 \cdots f_r \qquad \text{und} \qquad f_i \nsim f_j \text{ (für alle } i \neq j).$$

Beispiel 1.16. Es sei $f \in k[x_1, \ldots, x_n]$ ein reduziertes Polynom und $f = f_1 \cdots f_r$ die Zerlegung von f in seine irreduziblen Faktoren, wie oben. Dann ist

$$\mathcal{V}(f) = \mathcal{V}(f_1) \cup \cdots \cup \mathcal{V}(f_r)$$

die Zerlegung von $\mathcal{V}(f)$ in seine irreduziblen Komponenten. Um das zu sehen, müssen wir allerdings noch beweisen, dass zwischen den Untervarietäten $\mathcal{V}(f_i)$ keine Inklusionen bestehen. Das zeigen wir in Kürze als Konsequenz des Hilbertschen Nullstellensatzes (Kor. 1.38).

Definition 1.17. Eine Varietät der Form $\mathcal{V}(f) \subset \mathbb{A}^n$, die also durch ein einziges nicht-konstantes Polynom $f \in k[x_1, \ldots, x_n]$ definiert ist, heißt eine **affine Hyperfläche**. Speziell heißt eine affine Hyperfläche im Fall $n = 2$ eine **affine ebene Kurve**, im Fall $n = 3$ eine **affine Fläche**.

[7] Das hier angewendete Beweisprinzip wird oft als *noethersche Induktion* bezeichnet.

Diese Terminologie suggeriert natürlich eine Dimensionsaussage: Kurven sind 1-dimensional, Flächen 2-dimensional, Hyperflächen $n-1$-dimensional. Im Moment haben wir noch keinen formalen Dimensionsbegriff und verwenden die Namen nur für Varietäten, die durch eine einzige Gleichung definiert sind.

Kann man sich eine vollständige Übersicht über alle affinen k-Varietäten in $\mathbb{A}^n$ verschaffen? Für $n = 1$ haben wir schon gesehen, dass außer $\mathbb{A}^1$ selbst nur endliche Teilmengen Varietäten sind. Für $n = 2$ ist es schon schwieriger, aber noch machbar. Zunächst eine Hilfsaussage.

Lemma 1.18. *Seien $f, g \in k[x, y]$ zwei teilerfremde Polynome. Dann ist $\mathcal{V}(f, g) \subset \mathbb{A}^2$ endlich.*

Beweis. Da f und g teilerfremd sind, sind sie nach dem Gaußschen Lemma auch teilerfremd im Ring $k(x)[y]$ (siehe [Bosch], §2.7, Kor. 6) . Weil das ein Polynomring in einer Variablen über einem Körper (und damit ein Hauptidealring) ist, gibt es Polynome $\widetilde{p}, \widetilde{q} \in k(x)[y]$ mit

$$\widetilde{p}f + \widetilde{q}g = \mathrm{ggT}(f, g) = 1.$$

Die Koeffizieten von $\widetilde{p}$ und $\widetilde{q}$ sind rationale Funktionen in x, haben also eventuell Nenner. Wenn wir die Gleichung mit allen in $\widetilde{p}$ und $\widetilde{q}$ vorkommenden Nennern durchmultiplizieren, erhalten wir eine neue Gleichung

$$pf + qg = r, \qquad \text{mit } p, q \in k[x, y], r \in k[x], r \neq 0.$$

Für alle $(a, b) \in \mathcal{V}(f, g)$ ist also $r(a) = 0$. Also nimmt die erste Koordinate in $\mathcal{V}(f, g)$ höchstens endlich viele Werte an, die den endlich vielen Nullstellen von r entsprechen. Dasselbe können wir für die zweite Koordinate zeigen, so dass $\mathcal{V}(f, g)$ insgesamt endlich ist. ∎

Lemma 1.19. *Sei R ein faktorieller Integritätsring und P ein Primideal in R. Falls je zwei Elemente in P einen gemeinsamen Teiler haben, dann ist P ein Hauptideal.*

Beweis. Übung 1.9. ∎

Satz 1.20. *Es sei V eine irreduzible affine k-Varietät in der Ebene $\mathbb{A}^2$. Dann tritt genau einer der folgenden drei Fälle ein:*

(1) V enthält höchstens endlich viele Punkte;
(2) $V = \mathbb{A}^2$;
(3) V ist eine Kurve in $\mathbb{A}^2$, also $V = \mathcal{V}(f)$ für ein $f \in k[x_1, \ldots, x_n]$, $f \notin k$.

Beweis. Es sei $P = \mathcal{I}(V)$ das Verschwindungsideal von V. Da V irreduzibel ist, ist P ein Primideal nach Prop. 1.9. Falls $V = \mathbb{A}^2$, so ist $P = \langle 0 \rangle$ (siehe Übung 1.3). Wir nehmen also $P \neq \langle 0 \rangle$ an. Falls V endlich ist, sind wir im Fall (1). Wir nehmen also an, dass V unendlich ist. Sind $f, g \in P$, so folgt $V \subset \mathcal{V}(f, g)$. Nach Lemma 1.18 haben f und g damit einen gemeinsamen Teiler. Nach Lemma 1.19 ist P deshalb ein Hauptideal. Also gibt es $f \in k[x_1, \ldots, x_n]$ mit $P = \langle f \rangle$ und damit $V = \mathcal{V}(f)$. Schließlich bemerken wir noch, dass sich die Fälle (1),(2) und (3) wie behauptet ausschließen. Da K ein algebraisch abgeschlossener Körper ist, gilt $|K| = \infty$ und damit auch $|\mathbb{A}^2| = \infty$. Außerdem enthält jede Kurve unendlich viele Punkte (siehe Übung 1.4). ∎

Übungen

Übung 1.1. Sei $k = K$. Zeigen Sie, dass jede endliche Teilmenge von $\mathbb{A}^n$ eine affine k-Varietät ist.

Übung 1.2. Erzeugendensysteme von Idealen werden auch als *Basen* bezeichnet. Im Gegensatz zu den Basen der linearen Algebra gibt es aber im allgemeinen keine Unabhängigkeit zwischen den Erzeugern.
(a) Sei $I = \langle f_1, f_2 \rangle$ mit $f_1, f_2 \in k[x_1, \ldots, x_n] \setminus \{0\}$. Auf welche Weisen kann 0 im Ideal I dargestellt werden?
(b) Zeigen Sie, dass $\{x\}$ und $\{x + x^2, x^2\}$ zwei minimale Basen desselben Ideals in $k[x]$ sind.

Übung 1.3. Es sei $I \subset k[x_1, \ldots, x_n]$ ein Ideal, $I \neq \langle 0 \rangle$. Zeigen Sie, dass $\mathcal{V}(I) \neq \mathbb{A}^n$ gilt.

Übung 1.4. Sei $f \in k[x_1, \ldots, x_n]$, $n \geqslant 2$, $f \notin k$. Zeigen Sie, dass die Hyperfläche $\mathcal{V}_K(f)$ nicht endlich ist.

Übung 1.5. Bestimmen Sie für die folgenden affinen Varietäten in $\mathbb{A}^3$ jeweils ihre irreduziblen Komponenten und deren Verschwindungsideale. Beschreiben Sie die Komponenten geometrisch. Sie dürfen auch mit dem Computer arbeiten (siehe unten).
(a) $V = \mathcal{V}(x^2 - yz, xz - x)$;
(b) $V = \mathcal{V}(x^2 - yz, x^3 - y^3)$;
(c) $V = \mathcal{V}(x^2 + y^2 + z^2, x^2 - y^2 - z^2 + 1)$;

Übung 1.6. Es sei $X = \{(x, x) \in \mathbb{A}^2 : x \neq 1\} \subset \mathbb{A}^2$. Zeigen Sie, dass X keine affine k-Varietät ist.

Übung 1.7. Seien $V_1 \subset \mathbb{A}^m$ und $V_2 \subset \mathbb{A}^n$ affine k-Varietäten. Zeigen Sie:
(a) $V_1 \times V_2 \subset \mathbb{A}^{m+n}$ ist wieder eine affine k-Varietät.
(b) Sind V_1 und V_2 irreduzibel über k, so auch $V_1 \times V_2$. (Sie dürfen $k = K$ annehmen.)

Übung 1.8. Sei V eine affine k-Varietät. Zeigen Sie: Eine k-abgeschlossene Teilmenge $W \subset V$ ist genau dann eine irreduzible Komponente von V, wenn W irreduzibel, jede größere Teilmenge von V jedoch reduzibel ist.

Übung 1.9. Beweisen Sie Lemma 1.19. (*Zusatz:* Gilt das auch, wenn R irgendein noetherscher Ring ist?)

1.3. Computer-Algebra

Es gibt verschiedene Software-Pakete, die mit Polynomen in mehreren Variablen rechnen können und mehr oder weniger stark auf Anwendungen in der algebraischen Geometrie zugeschnitten sind. Die wichtigsten, die mir einfallen, sind:

(1) Die großen kommerziellen Pakete Maple und Mathematica. Der gesamte Funktionsumfang dieser Systeme ist beeindruckend, aber für speziellere Fragen der algebraischen Geometrie und kommutativen Algebra sind sie nur bedingt geeignet.
(2) Die freien Computer-Algebra-Systeme CoCoA, Macaulay2 und Singular. Am beliebtesten unter Mathematikern, die sich mit algebraischer Geometrie beschäftigen.
(3) Das kommerzielle Computer-Algebra-System Magma. Gilt als sehr leistungsfähig, aber ich bin nicht damit vertraut.
(4) Das freie Computer-Algebra-System SAGE, in das verschiedene andere Systeme integriert sind (u.a. Singular).
(5) Das Bertini-System für numerische algebraische Geometrie. Das ist methodisch etwas völlig anderes, hat aber in den letzten Jahren sehr an Bedeutung gewonnen.

Die Arbeit mit dem Computer wird in dieser Vorlesung keine zentrale Rolle spielen. Es ist aber eine gute Idee, sich nebenbei damit vertraut zu machen und zum Beispiel Übungsaufgaben

wenn möglich mit dem Computer zu lösen. Ab und zu werden dazu auch gesonderte Aufgaben gestellt. Außerdem werden im zweiten Kapitel einige der mathematischen Methoden eingeführt, die der Computer-Algebra zugrunde liegen.

Welche Software man auswählt, hängt immer vom konkreten Problem und vom persönlichen Geschmack ab. Einige Systeme sind in ihrer Syntax näher an der Mathematik (z.B. Maple und Macaulay2) und damit vielleicht schneller zu erlernen und leichter zu lesen. Andere sind näher an Programmiersprachen und deshalb besser für umfangreichere Arbeiten (z.B. Singular und SAGE, die sich an C bzw. an Python orientieren).

Für die Beispiele in dieser Vorlesung werde ich Macaulay2 verwenden. Die Software kann für verschiedene Betriebssysteme von der Seite http://www.math.uiuc.edu/Macaulay2/ heruntergeladen werden.[8] Starten wir Macaulay2 für eine ganz kurze Einführung

```
Macaulay2, version 1.8.2
```

Wir reproduzieren Beispiel 1.10(2). Als erstes müssen wir Macaulay2 immer sagen, in welchem Ring es arbeiten soll.

```
i1 : R = QQ[x,y]
o1 = R
o1 : PolynomialRing
```

Dabei sind die Zeilen, die mit *i* anfangen die *Input*-, die mit *o* die *Output*-Zeilen.

```
i2 : f = x^3 + x*y^2 - x^2 - y^2 - 4*x + 4
      3      2    2    2
o2 = x  + x*y  - x  - y  - 4x + 4
o2 : R
```

(Die Multiplikation muss man ausschreiben, also `x*y`, nicht `xy`).
Sei I das von f erzeugte Ideal.

```
i3 : I = ideal(f);
o3 : Ideal of R
```

Ist f irreduzibel, also I prim?

```
i4 : isPrime(I)
o4 = false
```

Bestimme die irreduziblen Komponenten:

```
i5 : decompose(I)
             2    2
o5 = {ideal(x  + y  - 4), ideal(x - 1)}
o5 : List
```

Das sind die beiden Komponenten, die den beiden Faktoren von f entsprechen.
Wenn einem der Output zu sperrig ist, kann man ihn vereinfacht formatieren:

```
i6 : toString(oo)
```

[8] Wenn Sie Schwierigkeiten mit der Installation haben (vor allem unter Windows), können Sie Macaulay2 auch online auf dem Sagemath cloud server benutzen; siehe http://www.math.uiuc.edu/Macaulay2/TryItOut/.
Eine weitere Alternative (nämlich eine virtuelle Maschine) mit Anleitung finden Sie auf der Homgepage von Anton Leykin (GeorgiaTech): http://people.math.gatech.edu/~aleykin3/M2/index.html.

```
o6 = {ideal(x^2+y^2-4), ideal(x-1)}
```

Dabei bezeichnet oo immer den vorhergehenden Output.
Zu jedem Befehl kann man übrigens innerhalb von Macaulay2 eine kurze Beschreibung bekommen, indem man ein Fragezeichen voranstellt, z.B.

```
i16 : ?decompose
  * Usage:minimalPrimes Idecompose I
  * Inputs:
      * I, an ideal
  * Outputs:
      * a list, whose entries are the minimal associated primes of I .
  ...
```

Noch ein weiteres, etwas interessanteres Beispiel. Wir betrachten den Raum $\mathbb{A}^9 = \mathbb{A}^{3\times 3}$ aller 3×3-Matrizen. Dazu gehört der Ring:

```
i1 : R = QQ[x_(1,1)..x_(3,3)];
```

Das Semikolon am Ende unterdrückt dabei den Output. Aus den Variablen $x_{1,1}, \ldots, x_{3,3}$ formen wir eine Matrix $A = (x_{ij})$.

```
i2 : A = matrix(for i from 1 to 3 list (for j from 1 to 3 list x_(i,j)))
o2 = | x_(1,1) x_(1,2) x_(1,3) |
     | x_(2,1) x_(2,2) x_(2,3) |
     | x_(3,1) x_(3,2) x_(3,3) |
             3       3
o2 : Matrix R  <--- R
```

und dann das Ideal im Ring R, das von allen 2×2-Minoren dieser Matrix erzeugt wird.

```
i3 : I = minors(2,A); toString(I)
o3 : Ideal of R
o4 = ideal(-x_(1,2)*x_(2,1)+x_(1,1)*x_(2,2),-x_(1,2)*x_(3,1)+x_(1,1)*x_(3,2),
           -x_(2,2)*x_(3,1)+x_(2,1)*x_(3,2),-x_(1,3)*x_(2,1)+x_(1,1)*x_(2,3),
           -x_(1,3)*x_(3,1)+x_(1,1)*x_(3,3),-x_(2,3)*x_(3,1)+x_(2,1)*x_(3,3),
           -x_(1,3)*x_(2,2)+x_(1,2)*x_(2,3),-x_(1,3)*x_(3,2)+x_(1,2)*x_(3,3),
           -x_(2,3)*x_(3,2)+x_(2,2)*x_(3,3))
```

Wir sehen also die 9 Determinanten der 2×2-Matrizen, die durch Streichung einer Zeile und einer Spalte aus A entstehen.

Das Ideal I aller 2×2-Minoren ist prim:

```
i5 : isPrime(I)
o5 = true
```

Wenn die Determinante einer Matrix verschwindet, dann ist sie nicht invertierbar, also vom Rang höchstens 2. Wenn alle 2×2-Minoren einer Matrix verschwinden, dann bedeutet das gerade, dass die Matrix vom Rang höchstens 1 ist (siehe Übung 1.14). Die durch I definierte Varietät $V = \mathcal{V}(I)$ ist also die Menge aller 3×3-Matrizen vom Rang höchstens 1 mit Einträgen in K. Wir wissen nun also, dass diese Varietät irreduzibel über $\mathbb{Q}$ ist. Außerdem gilt $\det(A) \in \mathcal{I}(V)$. Gilt auch $\det(A) \in I$?

```
i6 : f = det(A); isSubset(ideal(f),I)
o6 = true
```

Die Antwort ist ja. Das kann man auch leicht allgemein beweisen, indem man die Determinante nach einer Zeile oder Spalte entwickelt.

Übungen

Die folgenden Übungen sollen Sie ermuntern, noch etwas weiter mit Macaulay2 zu experimentieren. Die Dokumentation finden Sie auf der Macaulay2-Homepage

http://www.math.uiuc.edu/Macaulay2/

Natürlich sind die Aufgaben auch für andere Computer-Algebra-Systeme sinnvoll.

Übung 1.10. (a) Definieren Sie in Macaulay2 einen Polynomring in drei Variablen über dem Körper $\mathbb{F}_8$.
(b) Definieren Sie den Ring $\mathbb{Q}(a,b,c)[x,y,z]$. Setzen Sie $f = (ax^3+by^2+cz^2)(ac-bc)$ und vereinfachen Sie den Ausdruck f^2/c^2.

Übung 1.11. Definieren Sie in einem Polynomring in mehreren Variablen über $\mathbb{Q}$ zwei Ideale I, J ihrer Wahl. Finden Sie heraus, wie man testet, ob $I = J$, $I = \langle 1 \rangle$ oder $I \subset J$ gelten.

Übung 1.12. Wiederholen Sie das oben angegebene Beispiel mit Minoren von Matrizen im Fall $n = 4$. Finden Sie heraus, wie Sie sich ein einzelnes Element einer Liste anzeigen lassen können. Finden Sie heraus, wie Sie sich die Erzeuger eines Ideals anzeigen lassen können. Modifizieren Sie das Beispiel für den Fall symmetrischer Matrizen.

Übung 1.13. Schreiben Sie Macaulay2-Code, der im Körper $\mathbb{F}_p$ (p prim) alle Polynome $f(x) \in \mathbb{F}_p[x]$ von gegebenem Grad d mit der Eigenschaft $f(a) = 0$ für alle $a \in \mathbb{F}_p$ auflistet.

Übung 1.14. Zeigen Sie die folgenden Aussagen, die wir im Macaulay2-Beispiel verwendet haben.
(a) Genau dann hat eine $m \times n$-Matrix A mit Einträgen in K den Rang höchstens $r-1$, wenn alle ihre $r \times r$-Minoren verschwinden ($r \leqslant \min\{m,n\}$), also die Determinanten aller Matrizen, die durch Streichung von $m - r$ Zeilen und $n - r$ Spalten aus A entstehen.
(b) Genau dann hat eine symmetrische $n \times n$-Matrix A mit Einträgen in K den Rang höchstens $r-1$, wenn alle ihre symmetrischen $r \times r$-Minoren verschwinden ($r \leqslant n$), also die Determinanten aller Matrizen, die durch Streichung von $n - r$ Zeilen und Spalten, jeweils mit denselben Indizes, entstehen.

1.4. Abbildungen zwischen Varietäten

Es sei $V \subset \mathbb{A}^m$ eine affine k-Varietät. Jedes Polynom $f \in k[x_1, \ldots, x_n]$ können wir durch Einschränkung auf V als eine Funktion $V \to K$ auffassen. Allgemeiner gibt jedes n-Tupel $\varphi = (f_1, \ldots, f_n)$ von Polynomen eine Abbildung $\varphi\colon V \to \mathbb{A}^n$. Ist außerdem W eine affine k-Varietät in $\mathbb{A}^n$ und gilt $\varphi(V) \subset W$, dann haben wir sogar eine Abbildung

$$\varphi\colon V \to W.$$

Jede Abbildung $V \to W$, die in dieser Weise durch Polynome gegeben ist, heißt ein **Morphismus von k-Varietäten** (oder kurz ein k-Morphismus).

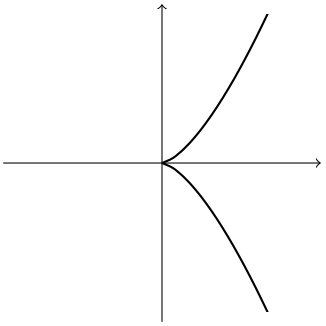
Beispiele 1.21. (1) Betrachte die Abbildung

$$\varphi: \begin{cases} \mathbb{A}^1 & \to & \mathbb{A}^2 \\ t & \mapsto & (t^2, t^3) \end{cases}.$$

Das Bild $\varphi(\mathbb{A}^1)$ ist dann gerade die affine k-Varietät

$$C = \mathcal{V}(x^3 - y^2)$$

genannt die **Neilsche**[9] **Parabel**.



Denn ist $(x, y) \in \varphi(\mathbb{A}^1)$, dann gibt es $t \in \mathbb{A}^1$ mit $x = t^2$, $y = t^3$, also $x^3 = t^6 = y^2$ und damit $(x, y) \in C$. Sei umgekehrt $(x, y) \in C$ und sei $t_0 = \sqrt{x}$ eine Quadratwurzel von x. Dann sind $\pm t_0^3$ die beiden Quadratwurzeln von x^3. Da auch y eine Quadratwurzel von x^3 ist, gilt also $y = t_0^3$ oder $y = (-t_0)^3$. Setzt man entsprechend $t = t_0$ oder $t = -t_0$, so folgt $(x, y) = \varphi(t)$. Der Übergang von der Parametrisierung zur Beschreibung durch eine Gleichung wird **Implizitisierung** genannt.

(2) Das Bild des Morphismus

$$\varphi: \begin{cases} \mathbb{A}^1 & \to & \mathbb{A}^3 \\ t & \mapsto & (t, t^2, t^3) \end{cases}$$

ist die **verdrehte Kubik**[10]

$$C = \mathcal{V}(y - x^2, z - x^3)$$

Das Bild von C unter der Projektion $(x, y, z) \mapsto (y, z)$ auf die letzten beiden Koordinaten ist die Neilsche Parabel aus dem vorigen Beispiel.

(3) Das Bild einer affinen k-Varietät braucht keine Varietät zu sein. Sei $V = \mathcal{V}(1 - xy)$ die Hyperbel in der affinen Ebene und sei $\pi: \mathbb{A}^2 \to \mathbb{A}^1$ die Projektion $(x, y) \mapsto y$. Offenbar gilt

$$\pi(V) = \mathbb{A}^1 \setminus \{0\}.$$

Dies ist aber keine affine k-Varietät in $\mathbb{A}^1$ (denn die sind alle endlich oder gleich $\mathbb{A}^1$).

Proposition 1.22. *Es sei $I \subset k[x_1, \ldots, x_m, y_1, \ldots, y_n]$ ein Ideal und sei $V = \mathcal{V}(I) \subset \mathbb{A}^m \times \mathbb{A}^n$. Sei*

$$\pi: \mathbb{A}^m \times \mathbb{A}^n \to \mathbb{A}^n,\ (p, q) \mapsto q$$

die Projektion auf die letzten n Koordinaten. Dann gilt

$$\pi(V) \subset \mathcal{V}(I \cap k[y_1, \ldots, y_n]).$$

[9] William Neile (1637–1670), englischer Mathematiker

[10] Es ist nicht ganz leicht, ein aussagekräftiges reelles Bild dieser Kurve zu zeichnen. Sie sieht tatsächlich aus wie die ebene Kubik $y = x^3$, die im Raum 'verdreht' wurde.

Beweis. Ist $f \in I \cap k[y_1, \dots, y_n])$ und $q \in \pi(V)$, dann gibt es $p \in \mathbb{A}^m$ mit $(p, q) \in V$. Also gilt $f(p, q) = f(q) = 0$. ∎

Das Ideal $I \cap k[y_1, \dots, y_n]$ wird das **Eliminationsideal** von I bezüglich $x_1, \dots, x_m$ genannt, weil in ihm die Variablen $x_1, \dots, x_m$ eliminiert wurden.

Beispiel 1.23. Sei $I = \langle y - x^2, z - x^3 \rangle$ das Ideal der getwisteten Kubik (Beispiel 1.21(2)). Es gilt

$$I \cap k[y, z] = \langle y^3 - z^2 \rangle.$$

Dies entspricht der Tatsache, dass die Projektion der getwisteten Kubik auf die letzten beiden Koordinaten die Neilsche Parabel ist. Es ist aber etwas mühsam, selbst in diesem Beispiel, die Gleichheit der Ideale direkt nachzuprüfen. Wir werden uns im nächsten Kapitel mit Verfahren zur Berechnung von Eliminationsidealen befassen.

In Beispiel 1.21(3) gilt dagegen $\langle xy - 1 \rangle \cap k[y] = \langle 0 \rangle$, denn es gibt kein Vielfaches ungleich 0 von $xy - 1$ in $k[x, y]$, das die Variable x nicht enthält. Dies entspricht der Tatsache, dass es keine echte k-abgeschlossene Teilmenge von $\mathbb{A}^1$ gibt, die das Bild der Projektion enthält.

Der Projektion von Varietäten entspricht die Elimination von Variablen.

Im Moment wissen wir allerdings nur, dass die Elemente des Eliminationsideals auf der Projektion einer Varietät verschwinden. Unser nächstes Ziel ist zu verstehen, wann das Eliminationsideal genau das Bild der Projektion definiert, also den Unterschied zwischen den beiden Beispielen in 1.23 zu verstehen.

Übungen

Übung 1.15. Es sei C die ebene Kurve $\mathcal{V}(y^2 - x^3 + x^2)$. Finden Sie eine Parametrisierung von C, also einen Morphismus $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^2$ mit $\varphi(\mathbb{A}^1) = C$.

Übung 1.16. Es sei $\mathbb{A}^4$ der Raum aller 2×2-Matrizen mit Einträgen in K und sei $V = \mathcal{V}(x_{11}x_{22} - x_{12}x_{21})$ die Menge aller Matrizen vom Rang höchstens 1. Finden Sie einen Morphismus $\varphi\colon \mathbb{A}^n \to \mathbb{A}^4$ (für geeignetes n) mit $\varphi(\mathbb{A}^n) = V$.

Übung 1.17. Es sei $c \in k$ und $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^2$ der Morphismus

$$\varphi(t) = \big(c - t^2, t(c - t^2)\big).$$

Zeigen Sie, dass das Bild $\varphi(\mathbb{A}^1)$ die ebene Kurve $C = \mathcal{V}(y^2 + x^3 - cx^2)$ ist. Zeichnen Sie das reelle Bild dieser Kurve für $c = 1$.

Übung 1.18. Es sei $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^2, t \mapsto \big(f(t), g(t)\big)$ ein Morphismus, gegeben durch $f, g \in k[t]$. Zeigen Sie:

(a) Es gibt eine Zahl $m \geqslant 0$ derart, dass die Familie von Polynomen

$$\big(f(t)^a g(t)^b : a, b \in \mathbb{Z}_+, a + b \leqslant m\big)$$

in $k[t]$ linear abhängig ist.

(b) Es gibt ein Polynom $h \in k[x, y]$, $h \neq 0$, mit $\varphi(\mathbb{A}^1) \subset \mathcal{V}(h)$.

1.5. Resultanten

Resultanten sind ein klassisches Werkzeug der Eliminationstheorie. Seit ihrer Blütezeit im 19. Jahrhundert sind sie ein bißchen aus der Mode gekommen und durch modernere Konzepte der kommutativen Algebra verdrängt worden, zum Beispiel durch Gröbnerbasen (siehe nächstes Kapitel). Die Einfachheit von Resultanten macht aber manche Beweise klarer.

In diesem Abschnitt sei stets R ein Integritätsring. Seien

$$f = \sum_{i=0}^{d} a_i z^i \qquad \text{und} \qquad g = \sum_{i=0}^{e} b_i z^i$$

zwei Polynome vom Grad d bzw. e (mit $a_d, b_e \neq 0$) in einer Variablen z mit Koeffizienten in R. Wir suchen ein Kriterium dafür, wann f und g einen gemeinsamen Faktor haben.

Lemma 1.24. *Genau dann haben f und g einen gemeinsamen Faktor von positivem Grad in $R[z]$, wenn es Polynome $p, q \in R[z]$ gibt derart, dass*

$$pf + qg = 0, \qquad \deg(p) < e,\ \deg(q) < d.$$

Beweis. Angenommen f und g haben einen gemeinsamen Faktor, etwa

$$f = f_1 h \qquad \text{und} \qquad g = g_1 h$$

mit $\deg(h) > 0$. Dann folgt also $\deg(f_1) < \deg(f)$ und $\deg(g_1) < \deg(g)$. Dann setzen wir einfach $p = g_1$ und $q = -f_1$ und erhalten

$$pf + qg = (g_1 f_1 - f_1 g_1)h = 0.$$

Seien umgekehrt p und q wie oben gegeben, so dass $pf = -qg$. Es sei $f = c \cdot f_1 \cdots f_m$ die Zerlegung von f in seine irreduziblen Faktoren von positivem Grad, $c \in R$. Dann ist $-qg$ durch alle Faktoren $f_1, \ldots, f_m$ teilbar. Wegen $\deg(q) < d$ können aber nicht alle diese Faktoren Teiler von q sein. Mindestens einer teilt also g und ist damit ein gemeinsamer Faktor von f und g. ∎

Aus der Aussage des Lemmas machen wir nun eine berechenbare Bedingung für die Existenz von p und q. Wir machen den Ansatz

$$p = p_{e-1} z^{e-1} + p_{e-2} z^{e-2} + \cdots + p_0, \quad q = q_{d-1} z^{d-1} + q_{d-2} z^{d-2} + \cdots + q_0.$$

Das Polynom $pf + qg$ hat höchstens Grad $d + e - 1$. Die Gleichheit $pf + qg = 0$ besagt, dass die $d + e$ Koeffizienten von $pf + qg$ alle 0 sind, was sich in die $d + e$ linearen Gleichungen

$$\begin{array}{cccccccc}
a_0 p_0 & & & & +b_0 q_0 & & & = 0 \\
a_1 p_0 & +a_0 p_1 & & & +b_1 q_0 & +b_0 q_1 & & = 0 \\
\vdots & \vdots & & & \vdots & \vdots & & \vdots \\
 & & a_d p_{e-2} & +a_{d-1} p_{e-1} & & & +b_e q_{d-2} & +b_{e-1} q_{d-1} = 0 \\
 & & & a_d p_{e-1} & & & & +b_e q_{d-1} = 0
\end{array}$$

in den unbekannten Koeffizienten von p und q übersetzt. Genau dann haben f und g einen gemeinsamen Faktor, wenn dieses homogene lineare Gleichungssystem eine nicht-triviale Lösung

in R besitzt. Die transponierte $(d+e)\times(d+e)$-Koeffizientenmatrix

$$\mathrm{Syl}_{d,e}(f,g) = \begin{bmatrix} a_0 & a_1 & \cdots & \cdots & \cdots & a_{d-1} & a_d & & & \\ & a_0 & a_1 & \cdots & \cdots & \cdots & a_{d-1} & a_d & & \\ & & \ddots & \ddots & & & & \ddots & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & \cdots & \cdots & b_{e-1} & b_e & & & & \\ & b_0 & b_1 & \cdots & \cdots & b_{e-1} & b_e & & & \\ & & \ddots & \ddots & & & \ddots & \ddots & & \\ & & & \ddots & \ddots & & & \ddots & \ddots & \\ & & & & b_0 & b_1 & \cdots & \cdots & b_{e-1} & b_e \end{bmatrix}$$

des Gleichungssystems heißt die **Sylvestermatrix**[11] von f und g. Wir setzen

$$\mathrm{Res}_{d,e}(f,g) = \det\big(\mathrm{Syl}_{d,e}(f,g)\big),$$

die **Resultante von f und g**. Das zugehörige homogene Gleichungssystem hat genau dann eine nicht-triviale Lösung, wenn die Determinante $\mathrm{Res}_{d,e}(f,g)$ gleich 0 ist.[12] Wir haben bewiesen:

Satz 1.25. *Genau dann haben zwei Polynome in $R[z]$ einen gemeinsamen Faktor von positivem Grad, wenn ihre Resultante* 0 *ist.* ■

Für später halten wir noch fest:

Lemma 1.26. *Es seien $f, g \in R[z]$ Polynome vom Grad d bzw. e. Dann gibt es Polynome $p, q \in R[z]$ mit $\mathrm{Res}_{d,e}(f,g) = pf + qg$ und $\deg(p) < e$, $\deg(q) < d$. Insbesondere gilt*

$$\mathrm{Res}_{d,e}(f,g) \in \langle f, g\rangle.$$

Beweis. Multipliziere in der Sylvestermatrix $\mathrm{Syl}_{d,e}(f,g)$ die i-te Spalte mit z^{d+e-i} und addiere sie zur letzten Spalte, für $i = 1, \ldots, d+e-1$. Dies ändert bekanntlich die Determinante nicht, aber die Sylvestermatrix sieht anschließend so aus:

$$\begin{bmatrix} a_0 & a_1 & \cdots & \cdots & \cdots & a_{d-1} & a_d & & & z^{e-1}f \\ & a_0 & a_1 & \cdots & \cdots & \cdots & a_{d-1} & a_d & & z^{e-2}f \\ & & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ & & & a_0 & a_1 & \cdots & \cdots & \cdots & a_{d-1} & f \\ b_0 & b_1 & \cdots & \cdots & b_{e-1} & b_e & & & & z^{d-1}g \\ & b_0 & b_1 & \cdots & \cdots & b_{e-1} & b_e & & & z^{d-2}g \\ & & \ddots & \ddots & & & \ddots & \ddots & & \vdots \\ & & & \ddots & \ddots & & & \ddots & \ddots & zg \\ & & & & b_0 & b_1 & \cdots & \cdots & b_{e-1} & g \end{bmatrix}$$

Die Behauptung folgt nun, indem man die Determinante nach der letzten Spalte entwickelt. ■

[11] James Joseph Sylvester (1814–1897), englischer Mathematiker

[12] Aus der linearen Algebra wissen wir das nur für lineare Gleichungssysteme über Körpern. Aber jede Lösung über dem Quotientenkörper $\mathrm{Quot}(R)$ von R gibt durch Bereinigen der Nenner auch eine Lösung über R.

Mit Hilfe der Algebra kann man eine andere Beschreibung der Resultanten geben, die wir nicht brauchen, die aber häufig als Definition genommen wird.

Satz 1.27. *Es seien*

$$f = (z-\lambda_1)\cdots(z-\lambda_d) \qquad \textit{und} \qquad g = (z-\mu_1)\cdots(z-\mu_e)$$

zwei normierte Polynome, die über R in Linearfaktoren zerfallen. Dann gilt

$$\mathrm{Res}_{d,e}(f,g) = \prod_{i,j}(\lambda_i - \mu_j).$$

Beweis. siehe z.B. [Bosch], §4.4, Kor. 9. ∎

In Macaulay2 kann man die Resultante von zwei Polynomen f und g in einem Polynomring $R[x]$ mit dem Befehl `resultant(f,g,x)` ausrechnen.

Übungen

Übung 1.19. Berechnen Sie die Resultante zweier Polynome vom Grad 2 als Polynom in den Koeffizienten.

Übung 1.20. Es sei R ein Intergritätsring und seien $f, g \in R[x]$, $f = \sum_{i=0}^{d} a_i z^i$, $g = \sum_{i=0}^{e} b_i z^i$. Beweisen Sie die folgenden Eigenschaften der Resultante:

(a) $\mathrm{Res}_{d,e}(f,g) = (-1)^{de}\mathrm{Res}(g,f)$;
(b) Falls $b_e = 0$, so gilt $\mathrm{Res}_{d,e}(f,g) = a_d\mathrm{Res}_{d,e-1}(f,g)$;
(c) $\mathrm{Res}_{d,e}(x^d, g) = g(0)^d$;
(d) Für jedes Polynom $h \in R[x]$ mit $\deg(h) \leqslant d-e$ gilt $\mathrm{Res}_{d,e}(f,g) = \mathrm{Res}_{d,e}(f+hg, g)$.
(e) $\mathrm{Res}_{d+1,e}(xf, g) = g(0)\mathrm{Res}_{d,e}(f,g)$;
(f) Für alle $a, b \in R$ gilt $\mathrm{Res}_{d,e}(af, bg) = a^e b^d \mathrm{Res}_{d,e}(f,g)$.

Übung 1.21. Verwenden Sie Resultanten, um einen anderen Beweis von Lemma 1.18 zu geben.

Übung 1.22. Es sei K ein Körper und es bezeichne V_d den Vektorraum der Polynome in $K[x]$ vom Grad höchstens d. Seien $f, g \in K[x]$, $\deg(f) \leqslant d$, $\deg(g) \leqslant e$.

(a) Zeigen Sie, dass die Sylvestermatrix $\mathrm{Syl}_{d,e}(f,g)$ gerade die lineare Abbildung

$$V_e \oplus V_d \to V_{d+e},\ (p,q) \mapsto pf + qg$$

bezüglich der Standardbasis $\{1, x, \ldots, x^m\}$ von V_m beschreibt.

(b) Zeigen Sie, dass

$$\mathrm{Res}_{d,e}(f(x-a), g(x-a)) = \mathrm{Res}_{d,e}(f(x), g(x))$$

für alle $a \in K$ gilt. (*Vorschlag:* Benutzen Sie (a).)

Bemerkung. Die Aussagen in (a) und (b) gelten auch (und lassen sich identisch beweisen), wenn man K durch einen Integritätsring R ersetzt und 'freier R-Modul' statt 'K-Vektorraum' sagt.

Übung 1.23. Es sei R ein Integritätsring, $f, g \in R[x]$ mit $\deg(f) = d$, $\deg(g) = e$ und sei $r \in \langle f, g\rangle \cap R$. Zeigen Sie, dass

$$r^3 \in \langle f^2, g^2\rangle \cap R \qquad \text{und} \qquad \mathrm{Res}_{2d,2e}(f^2, g^2) = \mathrm{Res}_{d,e}(f,g)^4$$

gelten. Folgern Sie, dass die Resultante das Ideal $\langle f, g\rangle \cap R$ im allgemeinen nicht erzeugt.

1.6. Der Nullstellensatz

Der Nullstellensatz ist einer der fundamentalen Sätze der algebraischen Geometrie. Er beantwortet zunächst die Frage, wie man feststellt, ob ein polynomiales Gleichungssystem unlösbar ist.

Satz 1.28 (Hilbertscher Nullstellensatz — schwache Form)**.** *Es sei I ein Ideal in $k[x_1, \dots, x_n]$. Genau dann gilt $\mathcal{V}(I) = \varnothing$, wenn $1 \in I$ gilt.*

Vom praktischen Standpunkt aus gesehen kommt es damit also darauf an, wie man entscheidet, ob $1 \in I$ gilt. Dazu später mehr.

Bemerkung 1.29. Für $n = 1$ und $f \in k[x]$ gilt $1 \in \langle f \rangle$ genau dann, wenn $f \in k$. Der schwache Nullstellensatz sagt also gerade, dass jedes nicht-konstante Polynom in K eine Nullstelle hat. Er spiegelt also wider, dass K algebraisch abgeschlossen ist und gilt entsprechend auch wirklich nur in diesem Fall.

Für den Beweis des Nullstellensatzes brauchen wir noch etwas Vorbereitung.

Lemma 1.30. *Es sei I ein Ideal in $k[x_1, \dots, x_n]$ mit $\mathcal{V}(I) \subsetneq \mathbb{A}^n$ und seien $p_1, \dots, p_d \in \mathbb{A}^n \setminus \mathcal{V}(I)$. Dann gibt es ein Polynom $f \in I$ mit $f(p_i) \neq 0$ für alle $i = 1, \dots, d$.*

Beweis. Wir beweisen die Aussage durch Induktion nach d. Für $d = 1$ ist ist sie klar. Sei $d \geqslant 2$. Nach Induktionsannahme gibt es für jedes $i \in \{1, \dots, d\}$ ein f_i mit $f_i(p_j) \neq 0$ für alle $j \neq i$. Falls $f_i(p_i) \neq 0$ für ein i, dann sind wir fertig. Es gelte also $f_i(p_i) = 0$ für alle i. Dann hat

$$f = f_1 + f_2 \cdots f_d.$$

die gewünschte Eigenschaft. ∎

Wir sagen ein Polynom $f \in k[x_1, \dots, x_n]$ ist **normiert bezüglich der Variablen** x_n, wenn das Monom $x_n^{\deg(f)}$ in f den Koeffizienten 1 hat. Ein einzelnes Polynom können wir durch Koordinatenwechsel in der Regel als normiert annehmen, wie das folgende Lemma zeigt.

Lemma 1.31. *Es sei k ein unendlicher Körper und $f \in k[x_1, \dots, x_n]$ ein nicht-konstantes Polynom.*

(1) Es gibt einen Punkt $a \in k^n$ mit $f(a) \neq 0$.

(2) Es gibt einen linearen Koordinatenwechsel, also eine invertierbare Matrix $A \in \mathrm{GL}_n(k)$, und eine Konstante $c \in k^\times$ derart, dass $cf(Ax)$ bezüglich x_n normiert ist.

Beweis. (1) Induktion nach n: Für $n = 1$ ist die Aussage klar, da f nur endlich viele Nullstellen in k hat. Für $n \geqslant 2$, sei $d = \deg(f)$ und schreibe $f = \sum_{i=0}^{d} g_i(x_1, \dots, x_{n-1}) x_n^i$. Wähle nach Induktionsannahme ein $a \in k^{n-1}$ derart, dass $g_0(a), \dots, g_d(a)$ nicht alle 0 sind. Dann ist $f(a, x_n) \in k[x_n]$ nicht das Nullpolynom, hat also nur endlich viele Nullstellen in k.

(2) Es sei f_d der homogene Teil höchsten Grades von f. Nach (1) gibt es einen Punkt $a \in k^n$ mit $f_d(a) \neq 0$. Dann gibt es ein $A \in \mathrm{GL}_n(k)$ mit $Ae_n = a$. Dass Polynom $f_d(Ax)$ ist also ein homogenes Polynom vom Grad d, das im Punkt $e_n = (0, \dots, 0, 1)$ nicht verschwindet. Also hat das Monom x_n^d in $f(Ax)$ einen Koeffizienten $c' \neq 0$. Mit $c = 1/c'$ folgt die Behauptung. ∎

Sei $I \subset k[x_1, \dots, x_n]$ ein Ideal. Nach Prop. 1.22 induziert die Projektion $\pi\colon (x_1, \dots, x_n) \mapsto (x_1, \dots, x_{n-1})$ auf die ersten $n-1$ Koordinaten einen Morphismus $\mathcal{V}(I) \to \mathcal{V}(I \cap k[x_1, \dots, x_{n-1}])$.

Als Vorbereitung auf den Nullstellensatz beweisen wir jetzt ein nützliches Kriterium dafür, wann diese Projektion surjektiv ist (vgl. Beispiel 1.23).

Lemma 1.32. *Es sei $I \subset k[x_1, \dots, x_n]$ ein Ideal. Falls I ein Polynom enthält, das bezüglich x_n normiert ist, dann ist die Projektion*

$$\pi\colon \mathcal{V}(I) \to \mathcal{V}(I \cap k[x_1, \dots, x_{n-1}])$$

auf die ersten $n-1$ Koordinaten surjektiv.

Beweis. Setze $J = I \cap k[x_1, \dots, x_{n-1}]$ und sei $a = (a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$. Betrachte die Gerade

$$L = \{(a_1, \dots, a_{n-1}, t)\colon t \in K\} \subset \mathbb{A}^n$$

über dem Punkt a. Angenommen $a \notin \pi(\mathcal{V}(I))$, d.h. es gelte $L \cap \mathcal{V}(I) = \varnothing$. Nach Voraussetzung gibt es ein Polynom $g \in I$, das bezüglich x_n normiert ist. Dann ist also

$$g(a, t) = g(a_1, \dots, a_{n-1}, t) \in K[t].$$

ein normiertes Polynom. Setze $d = \deg_{x_n}(g)$ und seien $c_1, \dots, c_d \in K$ die Nullstellen von $g(a, t)$. Da $L \cap \mathcal{V}(I) = \varnothing$, gibt es nach Lemma 1.30 ein $f \in I$ mit $f(a_1, \dots, a_{n-1}, c_i) \neq 0$ für alle $i = 1, \dots, d$. Also haben f und g auf L keine gemeinsame Nullstelle. Sei $r = \operatorname{Res}(f, g) \in k[x_1, \dots, x_{n-1}]$ die Resultante von f und g bezüglich der Variablen x_n. (Das heißt, wir fassen f und g als Polynome in x_n mit Koeffizienten in $k[x_1, \dots, x_{n-1}]$ auf.) Da $\mathcal{V}(f) \cap \mathcal{V}(g) \cap L = \varnothing$ gilt, folgt

$$r(a_1, \dots, a_{n-1}) \neq 0.$$

Andererseits gilt $r \in J$ nach Lemma 1.26. Also folgt $a \notin \mathcal{V}(J)$ und das Lemma ist bewiesen. ∎

Beweis des schwachen Nullstellensatzes. Wenn 1 in I enthalten ist, dann folgt natürlich $\mathcal{V}(I) \subset \mathcal{V}(1) = \varnothing$. Es sei umgekehrt $1 \notin I$. Dann liegt 1 auch nicht im Ideal, das von I in $K[x_1, \dots, x_n]$ erzeugt wird (Übung 1.24). Deshalb können wir annehmen, dass $k = K$ gilt (oder, was ausreicht, dass k unendlich ist). Falls $I = \langle 0 \rangle$, dann ist $\mathcal{V}(I) = \mathbb{A}^n \neq \varnothing$. Es gelte also $\langle 0 \rangle \subsetneq I \subsetneq K[x_1, \dots, x_n]$. Wir zeigen die Behauptung durch Induktion nach n. Falls $n = 1$, dann ist I also ein Ideal im Hauptidealring $K[x]$, d.h. es gibt ein nicht-konstantes Polynom f mit $I = \langle f \rangle$. Da K algebraisch abgeschlossen ist, hat f in K mindestens eine Nullstelle und somit ist $\mathcal{V}(I)$ nicht leer.

Sei $n \geqslant 2$ und sei $f \in I$ mit $\deg(f) > 0$, $f \neq 0$. Nach einem Koordinatenwechsel und Skalieren können wir annehmen, dass f normiert bezüglich x_n ist (Lemma 1.31). Setze $J = I \cap k[x_1, \dots, x_n]$. Nach Induktionsvoraussetzung ist $\mathcal{V}(J)$ nicht leer. Nach dem vorangehenden Lemma ist die Projektion $\mathcal{V}(I) \to \mathcal{V}(J)$ auf die ersten $n-1$ Koordinaten surjektiv. Also ist auch $\mathcal{V}(I)$ nicht leer. ∎

Als nächstes diskutieren wir die sogenannte starke Form des Nullstellensatzes. Gegeben eine Menge von Polynomen $T \subset k[x_1, \dots, x_n]$, wie sieht dann das Verschwindungsideal $\mathcal{I}(\mathcal{V}(T))$ aus? Per Definition enthält dieses Ideal T und damit auch das erzeugte Ideal $\langle T \rangle$. Es gilt also

$$\langle T \rangle \subset \mathcal{I}(\mathcal{V}(T)),$$

aber im allgemeinen gilt keine Gleichheit.

Beispiel 1.33. Sei $n = 1$ und $T = \{x^2\} \subset K[x]$, dann ist also $\mathcal{V}(x^2) = \{0\}$. Andererseits gilt $\mathcal{I}(\{0\}) = \langle x\rangle$. Denn ein Polynom f verschwindet genau dann im Ursprung, wenn sein konstanter Term 0 ist und dann kann man x ausklammern, also $f = g \cdot x \in \langle x\rangle$ für ein $g \in K[x]$. Andererseits besteht $\langle x^2\rangle$ aus den Polynomen, bei denen der konstante und auch der lineare Term 0 sind. Es ist also $\langle x^2\rangle \subsetneq \langle x\rangle = \mathcal{I}(\mathcal{V}(x^2))$.

Ist I ein Ideal in einem Ring R, so ist

$$\sqrt{I} = \big\{f \in R\text{: Es gibt eine natürliche Zahl } m \text{ mit } f^m \in I\big\}$$

wieder ein Ideal, genannt das **Radikal** von I (siehe Übung 1.25). Per Definition gilt immer $I \subset \sqrt{I}$. Ein Ideal I heißt ein **Radikalideal**, wenn Gleichheit gilt, also $I = \sqrt{I}$.

Das k-Verschwindungsideal $\mathcal{I}(M)$ einer Teilmenge $M \subset \mathbb{A}^n$ ist ein Radikalideal: Denn wenn eine Potenz einer Funktion verschwindet, dann verschwindet auch die Funktion selbst. (Ausführlich: Ist $f \in \sqrt{\mathcal{I}(M)}$, dann gibt es also $m \geqslant 1$ mit $f^m \in \mathcal{I}(M)$, also $f^m(p) = f(p)^m = 0$ für alle $p \in M$. Aber dann ist auch schon $f(p) = 0$ für alle $p \in M$ und damit $f \in \mathcal{I}(M)$.)

Wir sehen also, dass für jede Menge T von Polynomen stets $\sqrt{\langle T\rangle} \subset \mathcal{I}(\mathcal{V}(T))$ gelten muss. Hier gilt nun tatsächlich Gleichheit:

Satz 1.34 (Hilbertscher Nullstellensatz — starke Form)**.**
Für jedes Ideal I von $k[x_1, \ldots, x_n]$ gilt

$$\mathcal{I}_k(\mathcal{V}(I)) = \sqrt{I}.$$

Beweis. Die Inklusion ($\supset$) haben wir schon festgestellt. Die umgekehrte Inklusion zeigen wir mit dem sogenannten „Trick von Rabinowitsch[13]“. Sei $f \in \mathcal{I}(\mathcal{V}(I))$ und sei

$$J = \langle tf - 1\rangle + \langle I\rangle \subset k[x_1, \ldots, x_n, t].$$

Dann gilt $\mathcal{V}(J) = \varnothing$, somit $1 \in J$ nach dem schwachen Nullstellensatz. Es gibt also eine Identität

$$1 = a \cdot (tf - 1) + \sum_{i=1}^{r} b_i f_i$$

mit $a, b_1, \ldots, b_r \in k[x_1, \ldots, x_n, t]$ und $f_1, \ldots, f_r \in I$. Jetzt setzen wir $t = \frac{1}{f}$ ein und erhalten

$$1 = \sum_{i=1}^{r} b_i\big(x_1, \ldots, x_n, \frac{1}{f}\big) f_i.$$

Nun stehen Potenzen von f rechts im Nenner, d.h. es gibt Polynome $a_1, \ldots, a_r \in k[x_1, \ldots, x_n]$ und Exponenten $e_1, \ldots, e_r \geqslant 0$ mit $b_i(x_1, \ldots, x_n, 1/f) = \frac{a_i}{f^{e_i}}$. Setze $e = \max\{e_1, \ldots, e_r\}$, dann folgt

$$f^e = \sum_{i=1}^{r} a_i f^{e-e_i} f_i \in I. \qquad \blacksquare$$

Wir halten fest, dass die allgemeine Frage, die wir zu Anfang gestellt haben, mit dem Nullstellensatz grundsätzlich beantwortet ist.

[13] J. L. Rabinowitsch, „Zum Hilbertschen Nullstellensatz“, *Math. Ann.* 102 (1929); Rabinowitsch lebte und publizierte später unter dem Namen George Yuri Rainich (1868–1968).

Korollar 1.35. *Für zwei Mengen T_1, T_2 von Polynomen gilt $\mathcal{V}(T_1) = \mathcal{V}(T_2)$ genau dann, wenn $\sqrt{\langle T_1\rangle} = \sqrt{\langle T_2\rangle}$ gilt.* ∎

Vom praktischen Standpunkt kommt es nun also wieder darauf an, wie man das Radikal eines Ideals konkret berechnet und wie man überprüfen kann, ob zwei Ideale gleich sind. Darauf kommen wir, zumindest zum Teil, im nächsten Kapitel zurück.

In Macaulay2 kann man das Radikal eines Ideals I mit dem Befehl `radical(I)` ausrechnen lassen. Ob ein Ideal ein Radikalideal ist, überprüft entsprechend der Befehl `radical(I)==I`. Die Berechnung des Radikals kann allerdings schnell aufwändig werden und entsprechend lang dauern.

Bemerkung 1.36. Aus dem starken Nullstellensatz erhält man den schwachen leicht als Korollar zurück, denn es gilt

$$1 \in \langle T\rangle \quad\Longleftrightarrow\quad 1 \in \sqrt{\langle T\rangle} \quad\Longleftrightarrow\quad \langle T\rangle = k[x_1,\dots,x_n].$$

Korollar 1.37. *Es seien $f, g \in k[x_1,\dots,x_n]$ zwei irreduzible Polynome. Dann gilt $\mathcal{I}(\mathcal{V}(f)) = \langle f\rangle$ und falls $\mathcal{V}(f) \subset \mathcal{V}(g)$, dann folgt $f \sim g$ und damit $\mathcal{V}(f) = \mathcal{V}(g)$.*

Beweis. Da f irreduzibel ist, ist $\langle f\rangle$ ein Primideal und somit gilt $\langle f\rangle = \sqrt{\langle f\rangle} = \mathcal{I}(\mathcal{V}(f))$. Falls $\mathcal{V}(f) \subset \mathcal{V}(g)$, so folgt $g \in \mathcal{I}(\mathcal{V}(f)) = \sqrt{\langle f\rangle}$ gelten. Also gibt es $h \in k[x_1,\dots,x_n]$ und $m \geqslant 1$ mit $g^m = hf$. Da f und g irreduzibel sind, impliziert das $f|g$ und $g|f$ und damit die Behauptung. ∎

Korollar 1.38. *Es sei $f = k[x_1,\dots,x_n]$ ein reduziertes Polynom, $f = f_1\cdots f_r$ seine Zerlegung in irreduzible Faktoren. Dann gilt*

$$\mathcal{V}(f) = \mathcal{V}(f_1) \cup \cdots \cup \mathcal{V}(f_r)$$

und $\mathcal{V}(f_1),\dots,\mathcal{V}(f_r)$ sind die irreduziblen Komponenten von $\mathcal{V}(f)$. ∎

Erinnerung an die Algebra: Ein Ideal M in einem Ring R heißt **maximal**, wenn es kein Ideal I von R mit $M \subsetneq I \subsetneq R$ gibt. Genau dann ist ein Ideal M maximal, wenn der Restklassenring R/M ein Körper ist. (Auf die Rolle von Restklassenringen in der algebraischen Geometrie gehen wir im nächsten Abschnitt ein.) Insbesondere ist jedes maximale Ideal ein Primideal.

Ist $p \in \mathbb{A}^n$ ein Punkt, dann schreiben wir $m_p = \mathcal{I}_k(\{p\})$ für das Verschwindungsideal von p.

Lemma 1.39. *Für jeden Punkt $p = (a_1,\dots,a_n) \in k^n$ ist m_P ein maximales Ideal von $k[x_1,\dots,x_n]$ und es gilt*

$$m_P = \langle x_1 - a_1,\dots,x_n - a_n\rangle.$$

Beweis. Sei $I = \langle x_1-a_1,\dots,x_n-a_n\rangle$. Im Restklassenring $k[x_1,\dots,x_n]/I$ gilt $\overline{x_i - a_i} = 0$ und damit $\overline{x_i} = \overline{a_i}$. Daraus folgert man $k[x_1,\dots,x_n]/I \cong k$, so dass das Ideal I maximal ist. Außerdem gilt offenbar $I \subset m_P$ und damit Gleichheit, da I maximal ist. ∎

Korollar 1.40. *Zu jedem maximalen Ideal M von $k[x_1,\dots,x_n]$ gibt es einen Punkt $p \in \mathbb{A}^n$ mit $M = m_p$. Ist $k = K$, so ist p durch M eindeutig bestimmt.*

Beweis. Sei M ein maximales Ideal von $k[x_1, \dots, x_n]$. Nach dem Hilbertschen Nullstellensatz gilt $\mathcal{V}(M) \neq \varnothing$. Für jedes $p \in \mathcal{V}(M)$ gilt also $M \subset \mathcal{I}(\{p\}) = m_p$. Wegen Maximalität von M folgt $M = m_p$. Für $k = K$ folgt die Eindeutigkeit aus der Beschreibung von m_P in Lemma 1.39. ∎

Bemerkung. Ist $k \subsetneq K$, so ist der zu einem maximalen Ideal gehörende Punkt i.a. nicht mehr eindeutig. Zum Beispiel gehören zum maximalen Ideal $\langle x^2 + 1\rangle \subset \mathbb{R}[x]$ die beiden Punkte i und $-i$ in $\mathbb{A}^1_{\mathbb{C}}$. Es ist aber immer noch wahr, dass die Verschwindungsideale m_p alle maximal sind.

Korollar 1.41. *Die Zuordnungen $V \mapsto \mathcal{I}(V)$ und $I \mapsto \mathcal{V}(I)$ sind zwischen den Mengen*

$$\big\{\textit{affine } k\textit{-Varietäten in } \mathbb{A}^n\big\} \leftrightarrow \big\{\textit{Radikalideale in } k[x_1, \dots, x_n]\big\}$$
$$\big\{\textit{irreduzible affine } k\textit{-Varietäten in } \mathbb{A}^n\big\} \leftrightarrow \big\{\textit{Primideale in } k[x_1, \dots, x_n]\big\}$$

zueinander invers und definieren jeweils eine Bijektion. Falls $k = K$ algebraisch abgeschlossen ist, dann induzieren dieselben Zuordnungen auch eine Bijektion

$$\big\{\textit{Punkte in } \mathbb{A}^n\big\} \leftrightarrow \big\{\textit{Maximale Ideale in } k[x_1, \dots, x_n]\big\}. \qquad ∎$$

Wir kommen auf den Zusammenhang zwischen Projektion und Eliminationsideal zurück. Mit Hilfe des Nullstellensatzes können wir dazu jetzt die folgende allgemeine Aussage treffen.

Satz 1.42. *Sei $I \subset k[x_1, \dots, x_m, y_1, \dots, y_n]$ ein Ideal und $W = \mathcal{V}(I) \subset \mathbb{A}^m \times \mathbb{A}^n$ die durch I definierte affine k-Varietät. Sei*

$$\pi\colon \mathbb{A}^m \times \mathbb{A}^n \to \mathbb{A}^n,\ (p, q) \mapsto q$$

die Projektion auf den zweiten Faktor. Dann gilt

$$\overline{\pi(W)} = \mathcal{V}\big(I \cap k[y_1, \dots, y_n]\big).$$

Das heruntergeschnittene Ideal $I \cap k[y_1, \dots, y_n]$ definiert also die kleinste affine k-Varietät, die die projizierte Menge $\pi(W)$ enthält.

Beweis. Es sei $q \in \pi(W)$. Dann gibt es also $p \in \mathbb{A}^m$ mit $(p, q) \in W$ und jedes Polynom $f \in I$ verschwindet in (p, q). Dann verschwindet insbesondere jedes $f \in I \cap k[y_1, \dots, y_n]$ in q, also gilt $q \in \mathcal{V}(I \cap k[y_1, \dots, y_n])$. Ist umgekehrt $r \notin \overline{\pi(W)}$, dann gibt es also $f \in k[y_1, \dots, y_n]$ mit $f(\pi(p, q)) = 0$ für alle $(p, q) \in W$, aber $f(r) \neq 0$. Nach dem Nullstellensatz gibt es $l \geqslant 1$ mit $f^l \in I$. Also gilt $f^l(r) \neq 0$ und $f^l \in I \cap k[y_1, \dots, y_n]$ und damit $r \notin \mathcal{V}(I \cap k[y_1, \dots, y_n])$. ∎

Ist $\varphi\colon V \to \mathbb{A}^n$ ein Morphismus, so heißt

$$\Gamma_\varphi = \big\{(p, q) \in V \times \mathbb{A}^n \colon q = \varphi(p)\big\}$$

der **Graph von** φ. Der Graph ist selbst eine affine k-Varietät in $\mathbb{A}^m \times \mathbb{A}^n$, die explizit folgendermaßen beschrieben ist. Gegeben ein Ideal $I \subset k[x_1, \dots, x_m]$ mit $V = \mathcal{V}(I)$ und Polynome $f_1, \dots, f_n \in k[x_1, \dots, x_m]$ mit $\varphi = (f_1, \dots, f_n)\colon V \to \mathbb{A}^n$, setze

$$J_\varphi = \langle y_1 - f_1, \dots, y_n - f_n\rangle + \langle I\rangle \subset k[x_1, \dots, x_m, y_1, \dots, y_n].$$

Dann gilt $\mathcal{V}(J_\varphi) = \Gamma_\varphi$, was man einfach an der Definition von J_φ ablesen kann.

Korollar 1.43. *Sei $I \subset k[x_1, \dots, x_m]$ ein Ideal und $V = \mathcal{V}(I)$. Seien $f_1, \dots, f_n \in k[x_1, \dots, x_m]$, $\varphi = (f_1, \dots, f_n) \colon V \to \mathbb{A}^n$ und $J_\varphi \subset k[x_1, \dots, x_m, y_1, \dots, y_n]$ wie oben. Dann gilt*

$$\overline{\varphi(V)} = \mathcal{V}\big(J_\varphi \cap k[y_1, \dots, y_n]\big).$$

Beweis. Es sei $\pi \colon \mathbb{A}^m \times \mathbb{A}^n \to \mathbb{A}^n, (x, y) \mapsto y$ die Projektion auf den zweiten Faktor. Dann gilt $\varphi(V) = \pi(\Gamma_\varphi)$ und die Aussage folgt aus dem Satz. ∎

Übungen

Übung 1.24. Sei K/k eine Körpererweiterung, $I \subset k[x_1, \dots, x_n]$ ein Ideal und J das von I in $K[x_1, \dots, x_n]$ erzeugte Ideal. Zeigen Sie, dass $J \cap k[x_1, \dots, x_n] = I$ gilt. (*Vorschlag:* Koeffizientenvergleich)

Übung 1.25. Zeigen Sie, dass das Radikal eines Ideals wieder ein Ideal ist.

Übung 1.26. Es sei $V \subset \mathbb{A}^3$ die Vereinigung der drei Koordinatenebenen und $W \subset \mathbb{A}^3$ die Vereinigung der drei Koordinatenachsen. Zeigen Sie

$$\mathcal{I}(V) = \langle xyz \rangle \qquad \text{und} \qquad \mathcal{I}(W) = \langle xy, yz, xz \rangle.$$

(*Hinweis:* Für $f \in \mathcal{I}(W)$, betrachten Sie $f(x, y, z) - f(0, y, z) - f(x, 0, z) - f(x, y, 0)$.)

Übung 1.27. Seien $f, g \in k[x_1, \dots, x_n]$. Zeigen Sie:
(a) Genau dann ist f reduziert, wenn $\langle f \rangle$ ein Radikalideal ist.
(b) Genau dann gilt $\mathcal{V}(f) \subset \mathcal{V}(g)$, wenn g eine Potenz von f teilt.

Übung 1.28. Sei R ein Ring und seien I und J Ideale in R. Zeigen Sie:
(a) $\sqrt{\sqrt{I}} = \sqrt{I}$; (b) $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$; (c) $\sqrt{IJ} = \sqrt{I \cap J}$; (d) $\sqrt{I} = \langle 1 \rangle \Leftrightarrow I = \langle 1 \rangle$.
Gilt auch $\sqrt{IJ} = \sqrt{I}\sqrt{J}$?

Übung 1.29. Bestimmen Sie alle maximalen Ideale des Polynomrings $\mathbb{R}[x]$ in einer Variablen.

Übung 1.30. Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass jedes Radikalideal von $K[x_1, \dots, x_n]$ ein Durchschnitt von maximalen Idealen ist.

Übung 1.31. Sei M ein maximales Ideal in $k[x_1, \dots, x_n]$. Zeigen Sie, dass M von höchstens n Elementen erzeugt wird, also dass es Polynome $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ mit $M = \langle f_1, \dots, f_n \rangle$ gibt.
Hinweise. Führen Sie Induktion nach n. Betrachten Sie $M' = k[x_1, \dots, x_{n-1}]$, $L = k[x_1, \dots, x_n]/M$ und $L' = k[x_1, \dots, x_{n-1}]/M'$. Verwenden Sie das Minimalpolynom des Erzeugers der Körpererweiterung L/L'.

Übung 1.32. Den Nullstellensatz kann man stärker formalisiert folgendermaßen betrachten.

Es seien $\mathcal{X}$ und $\mathcal{Y}$ zwei partiell geordnete Mengen und seien $\mathcal{I} \colon \mathcal{X} \to \mathcal{Y}$ und $\mathcal{V} \colon \mathcal{Y} \to \mathcal{X}$ zwei Abbildungen mit den folgenden beiden Eigenschaften:

(i) $\mathcal{I}$ und $\mathcal{V}$ sind ordnungsumkehrend, d.h.

$$x_1 \leqslant x_2 \implies \mathcal{I}(x_1) \geqslant \mathcal{I}(x_2) \qquad \text{und} \qquad y_1 \leqslant y_2 \implies \mathcal{V}(y_1) \geqslant \mathcal{V}(y_2).$$

(ii) Die Kompositionen $\mathcal{I} \circ \mathcal{V}$ und $\mathcal{V} \circ \mathcal{I}$ sind monoton, d.h. es gelten $\mathcal{V}(\mathcal{I}(x)) \geqslant x$ für alle $x \in \mathcal{X}$ und $\mathcal{I}(\mathcal{V}(y)) \geqslant y$ für alle $y \in \mathcal{Y}$.

(a) Zeigen Sie, dass $\mathcal{I}$ und $\mathcal{V}$ Bijektionen zwischen den Mengen $\mathcal{I}(\mathcal{X}) \subset \mathcal{Y}$ und $\mathcal{V}(\mathcal{Y}) \subset \mathcal{X}$ definieren.

(b) Sei k ein Körper. Ein Ideal $I \subset k[x_1, \ldots, x_n]$ heiße **formal radikal**, wenn es eine Teilmenge $M \subset k^n$ mit $I = \mathcal{I}(M)$ gibt. Benutzen Sie (a) um zu zeigen, dass die Abbildungen $\mathcal{I}$ und $\mathcal{V}_k$ eine Bijektion zwischen den Nullstellenmengen in k^n und den formal radikalen Idealen von $k[x_1, \ldots, x_n]$ etablieren.

Bemerkung. Die Verstärkung im Hilbertschen Nullstellensatz steckt in der Aussage, dass das formale Radikal genau das übliche Radikal ist, wenn k algebraisch abgeschlossen ist. Über Körpern, die nicht algebraisch abgeschlossen sind, ist es schwieriger die formal radikalen Ideale zu charakterisieren. Möglich ist das zum Beispiel für $k = \mathbb{R}$, was auf die *reellen Radikalideale* und den *reellen Nullstellensatz* führt.

1.7. Koordinatenringe und die algebro-geometrische Korrespondenz

Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät mit Verschwindungsideal $\mathcal{I}(V) \subset k[x_1, \ldots, x_n]$. Aus der Algebra ist bekannt, dass man in dieser Situation den **Restklassenring**

$$k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V)$$

von $k[x_1, \ldots, x_n]$ *modulo dem Ideal* $\mathcal{I}(V)$ bilden kann. Dieser wird als **Koordinatenring** der affinen k-Varietät V bezeichnet.

Die Elemente von $k[V]$ sind per Definition Restklassen von Polynomen. Wir schreiben meistens einfach $\overline{g}$ für die Restklasse $g + \mathcal{I}(V)$ eines Polynoms $g \in k[x_1, \ldots, x_n]$ in $k[V]$. Konkret bedeutet das in dieser Situation folgendes: Ein Polynom $f \in k[x_1, \ldots, x_n]$ bestimmt eine Polynomfunktion

$$f\colon \mathbb{A}^n \to K,\ p \mapsto f(p).$$

Die Einschränkung dieser Funktion auf die affine k-Varietät V ist also eine Funktion $f|_V\colon V \to K$. Zwei Polynome f und g bestimmen genau dann dieselbe Funktion $V \to K$, wenn $f - g$ auf V verschwindet, also wenn $f - g \in \mathcal{I}(V)$. Per Definition ist dies äquivalent dazu, dass f und g in derselben Restklasse modulo des Ideals $\mathcal{I}(V)$ liegen, also $\overline{f} = \overline{g}$. Wir sehen also:

> Der Koordinatenring $k[V]$ ist der Ring aller Funktionen $V \to K$, die durch Polynome mit Koeffizienten in k definiert sind.

Neben den Ringen $\mathbb{Z}/n\mathbb{Z}$, die die Arithmetik in $\mathbb{Z}$ modulo einer Zahl n beschreiben, und der Konstruktion von Körpererweiterungen durch Adjunktion von Nullstellen, gehören die Koordinatenringe zu den wichtigsten Beispielen für den Begriff des Restklassenrings aus der Algebra.

Beispiel 1.44. Betrachte die Neilsche Parabel $C = \mathcal{V}(y^2 - x^3)$ in der affinen Ebene. Da $y^2 - x^3$ irreduzibel ist, ist $\langle y^2 - x^3 \rangle$ ein Radikalideal und damit gilt $\mathcal{I}(C) = \langle y^2 - x^3 \rangle$, also

$$k[C] \ = \ k[x, y]/\langle y^2 - x^3 \rangle.$$

Im Koordinatenring $k[C]$ gilt deswegen die Gleichheit $\overline{y^2} = \overline{x^3}$ und damit auch $\overline{y}^{2m} = \overline{x}^{3m}$ für alle $m \geqslant 0$. Ist $f \in k[x, y]$, $f = \sum_{i,j} a_{i,j} x^i y^j$ ein beliebiges Polynom, so gilt

$$\begin{aligned} \overline{f} &= \overline{\sum_{i,j} a_{i,2j} x^i y^{2j}} + \overline{\sum_{i,j} a_{i,2j+1} x^i y^{2j+1}} \\ &= \sum_{i,j} a_{i,2j} \overline{x}^{i+3j} + \sum_{i,j} a_{i,2j+1} \overline{x}^{i+3j} \overline{y} \end{aligned}$$

und jedes Element von $k[C]$ hat eine eindeutige solche Darstellung.

Einige Begriffe aus der Algebra: Eine k-**Algebra** ist ein Ring A, der k als Teilring enthält. Der Polynomring über k (in beliebig vielen Variablen) ist eine k-Algebra. Ist A eine k-Algebra und ist $G = \sum a_i x_1^{i_1} \cdots x_n^{i_n} \in k[x_1, \ldots, x_n]$ ein Polynom in n Variablen, dann kann man beliebige Elemente $f_1, \ldots, f_n \in A$ in G einsetzen und erhält ein Element

$$(*) \qquad G(f_1, \ldots, f_n) = \sum a_i f_1^{i_1} \cdots f_n^{i_n} \in A.$$

Ist A eine k-Algebra und T eine Teilmenge von A, dann ist der Durchschnitt aller k-Teilalgebren von A, die T enthalten, wieder eine k-Algebra, die **von** T **erzeugte** k-**Algebra**. Eine k-Algebra heißt **endlich erzeugt**, wenn sie von einer endlichen Teilmenge erzeugt wird.

Lemma 1.45. *Die von T erzeugte k-Teilalgebra von A besteht genau aus allen Elementen der Form $(*)$ mit $f_1, \ldots, f_n \in T$ (wobei n und G beliebig sind).*

Beweis. Sei B irgendeine k-Teilalgebra von A, die T enthält. Da B unter Addition und Multiplikation abgeschlossen ist, muss B dann alle Elemente der Form $(*)$ mit $f_1, \ldots, f_n \in T$ enthalten. Andererseits ist die Menge aller solcher Ausdrücke abgeschlossen unter Addition und Multiplikation und damit selbst eine k-Teilalgebra. Das beweist die Behauptung. ∎

Ein **Homomorphismus von** k-**Algebren** zwischen zwei k-Algebren A und B ist ein Ringhomomorphismus $\varphi\colon B \to A$, der außerdem k-linear ist, also mit

$$\varphi(af) = a\varphi(f) \text{ für alle } f \in B, a \in k.$$

Die Umkehrabbildung eines bijektiven Homomorphismus von k-Algebren ist wieder ein Homomomorphismus. Wie üblich heißt ein bijektiver Homomorphismus deshalb ein **Isomorphismus**. Zwei k-Algebren A und B heißen **isomorph**, wenn es zwischen ihnen einen Isomorphismus gibt, in Zeichen $A \cong B$ (oder zur Verdeutlichung $A \cong_k B$).

Korollar 1.46. *Sei A eine k-Algebra.*

(1) Genau dann ist A endlich erzeugt, wenn es eine Zahl $n \in \mathbb{N}$ und einen surjektiven Homomorphismus

$$\varphi\colon k[x_1, \ldots, x_n] \to A$$

von k-Algebren gibt.

(2) Genau dann ist A endlich erzeugt, wenn es eine Zahl $n \in \mathbb{N}$ und ein Ideal $I \subset k[x_1, \ldots, x_n]$ gibt mit

$$A \cong k[x_1, \ldots, x_n]/I.$$

Beweis. (1) Wird A von der endlichen Teilmenge $\{f_1, \ldots, f_n\}$ erzeugt, dann ist

$$\varphi \begin{cases} k[x_1, \ldots, x_n] & \to & A \\ G & \mapsto & G(f_1, \ldots, f_n) \end{cases}$$

ein Homomorphismus von k-Algebren. Nach dem vorangehenden Lemma ist φ surjektiv.

(2) Nach dem Homomorphiesatz für Ringe ist das einfach eine Umformulierung von (1). ∎

Eine Beschreibung einer endlich erzeugten k-Algebra als Restklassenring eines Polynomrings wie in Kor. 1.46(2) nennt man auch eine Beschreibung **durch Erzeuger und Relationen**.

Die Erzeuger sind die Restklassen der Variablen $x_1, \ldots, x_n$. Die Relationen sind die Elemente des Ideals I, die ausdrücken, welche Identitäten die Erzeuger erfüllen.

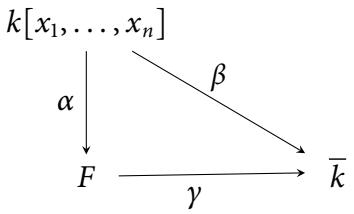
Der schwache Nullstellensatz lässt sich in dieser Sprache rein algebraisch formulieren.

Satz 1.47 (Nullstellensatz, algebraische Form)**.** *Es sei F/k eine Körpererweiterung. Wenn F als k-Algebra endlich erzeugt ist, dann ist F/k endlich algebraisch (d.h. es gilt $\dim_k(F) < \infty$).*

Beweis. Dass F als k-Algebra endlich erzeugt ist, bedeutet nach Kor. 1.46, dass es eine natürliche Zahl n und einen surjektiven Homomorphismus

$$\alpha\colon k[x_1, \ldots, x_n] \to F$$

von k-Algebren gibt; setze $I = \ker(\alpha)$. Sei $\overline{k}$ der algebraische Abschluss von k. Nach dem schwachen Nullstellensatz gilt $\mathcal{V}(I) \neq 0$, es gibt also einen Punkt $p \in \mathcal{V}(I) \subset \mathbb{A}^n_{\overline{k}}$. Sei $\beta\colon k[x_1, \ldots, x_n] \to \overline{k}$, $p \mapsto f(p)$ die Auswertung im Punkt p. Wegen $p \in \mathcal{V}(I)$ gilt dann $I \subset \ker(\beta)$. Nach dem Homomorphiesatz gibt es einen Homomorphismus $\gamma\colon F \to \overline{k}$ mit $\beta = \gamma \circ \alpha$, d.h. wir erhalten ein kommutierendes Diagramm



Also ist F ein Teilkörper von $\overline{k}$ und damit algebraisch über k. Damit ist F auch endlich, denn es wird von den Elementen $\overline{x_1}, \ldots, \overline{x_n}$ erzeugt. ∎

Man kann diese Aussage auch ausschließlich mit Ringtheorie beweisen und den schwachen Nullstellensatz relativ leicht daraus zurückgewinnen (siehe Übung 1.42).

Sei R ein Ring. Ein Element $f \in R$ heißt **nilpotent**, wenn es eine Zahl $m \geqslant 1$ gibt mit $f^m = 0$. Ein Ring R heißt **reduziert**, wenn er keine nilpotenten Elemente ungleich 0 enthält. In einem reduzierten Ring gilt also

$$f^m = 0 \implies f = 0.$$

Der Begriff hängt eng mit dem des Radikalideals zusammen. Ist $I \subset k[x_1, \ldots, x_n]$ ein Ideal im Polynomring, dann ist die k-Algebra

$$k[x_1, \ldots, x_n]/I$$

genau dann reduziert, wenn I ein Radikalideal ist.

Nach diesen Allgemeinheiten über k-Algebren kehren wir nun zu den Koordinatenringen von affinen k-Varietäten zurück.

Korollar 1.48 (zum Nullstellensatz)**.** *Der Koordinatenring einer affinen k-Varietät ist eine endlich erzeugte, reduzierte k-Algebra. Umgekehrt ist jede endlich erzeugte, reduzierte k-Algebra zum Koordinatenring einer affinen k-Varietät isomorph.*

Beweis. Ist $V \subset \mathbb{A}^m$ eine affine k-Varietät mit Verschwindungsideal $\mathcal{I}(V)$, so ist nach Definition $k[V] = k[x_1, \ldots, x_m]/\mathcal{I}(V)$ und damit eine endlich erzeugte, reduzierte k-Algebra, da $\mathcal{I}(V)$ ein Radikalideal ist. Ist umgekehrt A eine endlich erzeugte reduzierte k-Algebra, dann gibt es $n \in \mathbb{N}$ und ein Radikalideal $I \subset k[x_1, \ldots, x_m]$ mit $A \cong k[x_1, \ldots, x_m]/I$. Ist V die affine k-Varietät $\mathcal{V}(I)$, so gilt $\mathcal{I}(V) = \sqrt{I} = I$ nach dem starken Nullstellensatz (Satz 1.34), also $k[V] \cong A$. ∎

Erinnerung an die Algebra. Sei R ein Ring, I ein Ideal in R und $\alpha\colon R \to R/I$ der Restklassenhomomorphismus $f \mapsto \overline{f}$. Ist J ein Ideal von R mit $I \subset J$, dann ist $\alpha(J)$ ein Ideal von R/I; umgekehrt existiert zu jedem Ideal J' von R/I ein Ideal J von R mit $I \subset J$ und $\alpha(J) = J'$, nämlich $J = \alpha^{-1}(J')$. (Insbesondere gilt $\alpha^{-1}(\langle 0 \rangle) = I$ per Definition.) Es gibt also eine Bijektion

$$\big\{\text{Ideale } J \text{ von } R \text{ mit } I \subset J\big\} \longleftrightarrow \big\{\text{Ideale von } R/I\big\}.$$

Diese Bijektion respektiert Durchschnitte, Summen, Produkte und Radikale von Idealen.

Sind nun $V, W \subset \mathbb{A}^n$ zwei affine k-Varietäten, so gilt $W \subset V$ genau dann, wenn $\mathcal{I}(V) \subset \mathcal{I}(W)$. In diesem Fall ist also $\overline{\mathcal{I}(W)}$ ein Ideal von $k[V]$. Die Korrespondenz zwischen affinen k-Varietäten in $\mathbb{A}^n$ und Radikalidealen in $k[x_1, \ldots, x_n]$ lässt sich deshalb genauso für abgeschlossene Untervarietäten einer Varietät V und Radikalideale von $k[V]$ formulieren.

Korollar 1.49 (zum starken Nullstellensatz)**.** *Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät mit Koordinatenring $k[V]$ und sei $\alpha\colon k[x_1, \ldots, x_n] \to k[V]$ der Restklassenhomomorphismus. Die Zuordnungen $W \mapsto \alpha(\mathcal{I}(W))$ und $I \mapsto \mathcal{V}(\alpha^{-1}(I))$ sind zwischen den Mengen*

$$\big\{\textit{abgeschlossene Untervarietäten von } V\big\} \leftrightarrow \big\{\textit{Radikalideale in } k[V]\big\}$$
$$\big\{\textit{irreduzible abgeschlossene Untervarietäten von } V\big\} \leftrightarrow \big\{\textit{Primideale in } k[V]\big\}$$

zueinander invers und definieren jeweils eine Bijektion. Falls $k = K$ algebraisch abgeschlossen ist, dann induzieren dieselben Zuordnungen auch eine Bijektion

$$\big\{\textit{Punkte in } V\big\} \leftrightarrow \big\{\textit{Maximale Ideale in } k[V]\big\}.$$

Beweis. Das folgt aus Kor. 1.41 und der beschriebenen Korrespondenz zwischen Idealen von $k[x_1, \ldots, x_n]$, die $\mathcal{I}(V)$ enthalten, und Idealen von $k[V]$. ∎

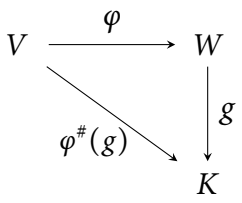
Die Korrespondenz zwischen affinen k-Varietäten und endlich erzeugten, reduzierten k-Algebren erstreckt sich auch auf Morphismen. Es seien $V \subset \mathbb{A}^m$ und $W \subset \mathbb{A}^n$ affine k-Varietäten und $\varphi = (f_1, \ldots, f_n)\colon V \to W$ ein Morphismus, gegeben durch $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$. Da wir uns nur für die Werte von $f_1, \ldots, f_n$ auf V interessieren, können wir auch ebenso gut $f_1, \ldots, f_n \in k[V]$ nehmen. Für jedes $g \in k[W]$ ist dann

$$g \circ \varphi = g(f_1, \ldots, f_n)$$

ein Element von $k[V]$. Dies definiert einen Homomorphismus von k-Algebren

$$\varphi^{\#}: \begin{cases} k[W] & \to & k[V] \\ g & \mapsto & g \circ \varphi \end{cases}$$

zwischen den Koordinatenringen in umgekehrter Richtung. Die Funktion $\varphi^{\#}(g) \in k[V]$ entsteht also 'durch Zurückziehen' von V nach W mittels φ.



Beispiel 1.50. Kommen wir zurück auf die Neilsche Parabel. Betrachte die Abbildung

$$\varphi: \begin{cases} \mathbb{A}^1 & \to & \mathbb{A}^2 \\ t & \mapsto & (t^2, t^3) \end{cases},$$

mit Bild $C = \varphi(\mathbb{A}^1) = \mathcal{V}(x^3 - y^2)$. Dazu gehört der Homomorphismus von k-Algebren $\varphi^{\#}: k[C] \to k[t]$. Da $\varphi^{\#}$ k-linear und multiplikativ ist, ist $\varphi^{\#}$ eindeutig bestimmt durch die Bilder der beiden Erzeuger $\overline{x}$ und $\overline{y}$. Dabei gilt

$$\varphi^{\#}(\overline{x})(t) = (\overline{x} \circ \varphi)(t) = \overline{x}(t^2, t^3) = t^2 \qquad \text{und} \qquad \varphi^{\#}(\overline{y})(t) = (\overline{y} \circ \varphi)(t) = \overline{y}(t^2, t^3) = t^3.$$

Proposition 1.51. *Es seien $\varphi: V \to W$ und $\psi: W \to X$ Morphismen von affinen k-Varietäten.*

(1) Die Abbildungen $\varphi^{\#}, \psi^{\#}$ sind Homomorphismen von k-Algebren und es gilt

$$(\psi \circ \varphi)^{\#} = \varphi^{\#} \circ \psi^{\#}.$$

(2) Für $\rho: V \to V$ gilt $\rho^{\#} = \mathrm{id}_{k[V]}$ genau dann, wenn $\rho = \mathrm{id}_V$.

(3) Zu jedem Homomorphismus $\alpha: k[W] \to k[V]$ existiert ein Morphismus $\varphi: V \to W$ von k-Varietäten mit $\alpha = \varphi^{\#}$.

Beweis. (1), (2): Übung. (3) Es sei $\alpha: k[W] \to k[V]$ ein Homomorphismus. Es gelte $W \subset \mathbb{A}^n$, dann ist $k[W] = k[y_1, \ldots, y_n]/\mathcal{I}(W)$. Schreibe $\overline{y_i}$ für die Restklasse von y_i in $k[W]$ und setze

$$f_i = \alpha(\overline{y_i}) \qquad \text{für } i = 1, \ldots, n.$$

Dann ist $\varphi = (f_1, \ldots, f_n): V \to \mathbb{A}^n$ ein Morphismus und es gilt $\varphi(V) \subset W$. Denn ist $p \in V$ und $g \in \mathcal{I}(W)$, so gilt

$$g(\varphi(p)) = g\big(\alpha(\overline{y_1})(p), \ldots, \alpha(\overline{y_n})(p)\big) = \alpha(g(\overline{y_1}, \ldots, \overline{y_n}))(p) = \alpha(g)(p) = 0.$$

Dabei gilt die erste Gleichheit nach Definition, die zweite weil α ein Homomorphismus ist und die letzte wegen $g \in \mathcal{I}(W)$ und damit $\overline{g} = 0$. Also folgt $\varphi(p) \in \mathcal{V}(\mathcal{I}(W)) = W$. Nach Konstruktion von φ gilt außerdem

$$\varphi^{\#}(g) = g \circ \varphi = g\big(\alpha(\overline{y_1}), \ldots, \alpha(\overline{y_n})\big) = \alpha(g)$$

für alle $g \in k[W]$, also $\varphi^{\#} = \alpha$. ∎

Ein Morphismus $\varphi\colon V \to W$ von k-Varietäten heißt ein **Isomorphismus**, wenn es einen Morphismus $\psi\colon W \to V$ gibt mit $\psi \circ \varphi = \mathrm{id}_V$ und $\varphi \circ \psi = \mathrm{id}_W$. In diesem Fall schreibt man φ^{-1} für ψ. Wenn ein Isomorphismus zwischen V und W existiert, dann heißen V und W **isomorph**.

Korollar 1.52. *Genau dann ist $\varphi\colon V \to W$ ein Isomorphismus, wenn $\varphi^{\#}\colon k[W] \to k[V]$ ein Isomorphismus von k-Algebren ist. Genau dann sind V und W isomorphe affine k-Varietäten, wenn ihre Koordinatenringe $k[V]$ und $k[W]$ isomorphe k-Algebren sind.*

Beweis. Dies folgt aus Prop. 1.51(1)&(2), denn damit gilt $\varphi^{\#} \circ \psi^{\#} = \mathrm{id}_{k[V]}$ genau dann, wenn $\psi \circ \varphi = \mathrm{id}_V$; Entsprechendes gilt für $\psi^{\#} \circ \varphi^{\#}$. ∎

Beispiel 1.53. Schließlich diskutieren wir die Neilsche Parabel zu Ende. Sei $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^2$ die Parametrisierung wie oben. Der Homomorphismus

$$\varphi^{\#}\colon \begin{cases} k[C] = k[x,y]/\langle y^2 - x^3\rangle & \to & k[t] \\ \overline{x} & \mapsto & t^2 \\ \overline{y} & \mapsto & t^3 \end{cases}$$

ist injektiv aber nicht surjektiv und damit *kein* Isomorphismus. Die Injektivität kann man leicht nachrechnen, indem man den Kern der Abbildung $k[x,y] \to k[t], x \mapsto t^2, y \mapsto t^3$ bestimmt. Dass $\varphi^{\#}$ nicht surjektiv ist, liegt daran, dass das Polynom t offensichtlich nicht im Bild liegt. Tatsächlich gilt $\mathrm{im}(\varphi^{\#}) = k[t^2, t^3, \dots] \subset k[t]$.

Damit ist φ auch kein Isomorphismus. Es gibt also keinen Morphismus $C \to \mathbb{A}^1$, der zu φ invers wäre. Geometrisch entspricht das der Tatsache, dass man die Singularität im Nullpunkt, die 'Spitze' der Neilschen Parabel, nicht einfach wieder ausbügeln kann. Das werden wir später systematischer betrachten.

Die Hauptaussage des ganzen Abschnitts kann man folgendermaßen zusammenfassen.

Zwischen affinen k-Varietäten und endlich erzeugten reduzierten k-Algebren gibt es eine ein-eindeutige Korrespondenz. Alle Information über Untervarietäten und Morphismen von k-Varietäten steckt auch in den Koordinatenringen. Diese vollkommene Entsprechung zwischen Geometrie und Algebra wird die *algebro-geometrische Korrespondenz* genannt.

Natürlich kann man auch in Macaulay2 mit Ringhomomorphismen rechnen. Wir betrachten dazu nochmal Beispiel 1.50.

```
i1 : R = QQ[t];
i2 : S = QQ[x,y];
i3 : phi = map(R,S,{x=>t^2,y=>t^3})
                2   3
o3 = map(R,S,{t , t })
o3 : RingMap R <--- S
```

Die Abbildung $\varphi\colon S \to R$ entspricht der Parametrisierung der Neilschen Parabel. Man beachte, dass beim Befehl `map` das Ziel zuerst angegeben wird.

```
i4 : kernel(phi)
             3    2
o4 = ideal(x  - y )
o4 : Ideal of S
```

Der Kern von φ ist genau das Verschwindungsideal der Neilschen Parabel. Wir können φ auch direkt auf dem Koordinatenring definieren:

```
i5 : T = S/ideal(y^2-x^3);
i6 : phi = map(R,T,{x=>t^2,y=>t^3})
                2   3
o6 = map(R,T,{t , t })
o6 : RingMap R <--- T
i7 : kernel(phi)
o7 = ideal ()
o7 : Ideal of T
```

Dabei ist zu beachten, dass Macaulay2 zunächst nicht überprüft, ob die Abbildung überhaupt wohldefiniert ist. Darum muss man erst bitten:

```
i8 : isWellDefined(phi)
o8 = true
```

Eine Abbildung, bei der die Bilder von x und y nicht mit der Relation $y^2 = x^3$ in T verträglich sind, ist dagegen natürlich nicht wohldefiniert.

```
i9 : psi = map(R,T,{x=>t,y=>t^3})
                   3
o9 = map(R,T,{t, t })
o9 : RingMap R <--- T
i10 : isWellDefined(psi)
o10 = false
```

Der Umgang mit Ringhomomorphismen in Macaulay2 ist etwas gewöhnungsbedürftig. So weit ich sehen kann, gibt es zum Beispiel keinen einfachen Befehl, um festzustellen, ob so ein Homomorphismus ein Isomorphismus ist.

Macaulay2 kann auch die zu den Koordinatenringen gehörenden Varietäten erfassen.

```
i11 : C = Spec(T)
o11 = C
o11 : AffineVariety
```

Der Befehl `Spec` steht dabei für *Spectrum* und bezieht sich auf die Menge aller Primideale des Koordinatenrings T. Dahinter steht im Wesentlichen Kor. 1.49, Macaulay2 erfasst also die affine Varietät über die Ideale des Koordinatenrings. Man kann Macaulay2 jetzt nach geometrischen Eigenschaften der Varietät fragen, zum Beispiel nach der Dimension (die wir noch nicht definiert haben).

```
i12 : dim C
o12 = 1
```

Übungen

Übung 1.33. Beweisen Sie die folgenden Aussagen aus der Algebra: Sei R ein Ring und I ein Ideal in R.
(a) Genau dann ist R/I ein reduzierter Ring, wenn I ein Radikalideal ist.
(b) Genau dann ist R/I nullteilerfrei (also ein Integritätsring), wenn I ein Primideal ist.
(c) Genau dann ist R/I ein Körper, wenn I ein maximales Ideal ist.

Übung 1.34. Beweisen Sie, dass jedes Primideal $\neq \langle 0 \rangle$ in $k[x]$ ein maximales Ideal ist.

Übung 1.35. Es seien $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_r \rangle$ und $V = \mathcal{V}(I)$. Zeigen Sie:
(a) Falls $\mathcal{V}(I)$ nur aus endlich vielen Punkten besteht, so ist $k[V]$ ein endlich-dimensionaler k-Vektorraum. (*Hinweis:* Die Elemente von $k[V]$ sind Funktionen $V \to K$.)
(b)* Falls $\mathcal{V}(I)$ nur aus endlich vielen Punkten besteht, so ist der Restklassenring $k[x_1, \ldots, x_n]/I$ ein endlich-dimensionaler k-Vektorraum. (*Hinweis:* Verwenden Sie den starken Nullstellensatz.)

Übung 1.36. Sei $\varphi\colon R \to S$ ein Ringhomomorphismus, I ein Ideal in R und J ein Ideal in S. Zeigen Sie:
(a) $\varphi^{-1}(J)$ ist ein Ideal in R.
(b) Falls φ surjektiv ist, so ist $\varphi(I)$ ein Ideal von R.
(c) Zeigen Sie durch ein Beispiel, dass $\varphi(I)$ im allgemeinen kein Ideal von R zu sein braucht.

Übung 1.37. Es sei $f = x^3 + y^3 + z^3 + 3xyz \in k[x, y, z]$. Sei $I = \langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \frac{\partial f}{\partial z} \rangle$ und $R = k[x, y, z]/I$. Verwenden Sie Macaulay2, um die folgenden Fragen zu beantworten.
(a) Ist xyz für $k = \mathbb{Q}$ ein Nullteiler in R? Für $k = \mathbb{F}_3$?
(b) Finden sie die kleinste Zahl $m \geqslant 1$ mit $\overline{(x + y + z)}^m = 0$ in R für $k = \mathbb{Q}$ und $k = \mathbb{F}_3$.

Übung 1.38. (a) Es C_1 die Parabel $\mathcal{V}(y - x^2)$. Zeigen Sie, dass $k[C_1]$ zum Polynomring in einer Variablen isomorph ist und damit C_1 zur affinen Geraden.
(b) Sei C_2 die Hyperbel $\mathcal{V}(1 - xy)$. Zeigen Sie, dass $k[C_2]$ nicht zum Polynomring in einer Variablen isomorph ist.
(c) Sei $k = K$ algebraisch abgeschlossen und sei $f \in k[x, y]$ ein irreduzibles quadratisches Polynom. Zeigen Sie, dass $C = \mathcal{V}(f)$ zu C_1 oder C_2 isomorph ist.

Übung 1.39. Es sei $C \subset \mathbb{A}^3$ das Bild der Abbildung

$$\varphi\colon \mathbb{A}^1 \to \mathbb{A}^3, t \mapsto (t, t^2, t^3),$$

die verdrehte Kubik aus Beispiel 1.21(2). Zeigen Sie, dass φ ein Isomorphismus ist.

Übung 1.40. Es sei $I \subset k[x_1, \ldots, x_n]$ ein Ideal und $V = \mathcal{V}(I)$. Zeigen Sie:
(a) Genau dann ist ein Element $f \in k[V]$ eine Einheit, wenn $f(p) \neq 0$ für alle $p \in V$ gilt.
(b) Ist $f \in \mathcal{I}(V)$, so ist $1 + f$ eine Einheit in $k[x_1, \ldots, x_n]/I$.

Übung 1.41. Es sei $\varphi\colon V \to W$ ein Morphismus von affinen k-Varietäten. Zeigen Sie
(a) Genau dann ist $\varphi(V)$ Zariski-dicht in W, wenn $\varphi^{\#}\colon k[W] \to k[V]$ injektiv ist.
(b) Allgemeiner gilt $\overline{\varphi(V)} = \mathcal{V}(\ker(\varphi^{\#}))$. (*Hinweis:* Benutzen Sie Kor. 1.43.)

Übung 1.42. Folgern Sie den schwachen Nullstellensatz (1.28) aus der algebraischen Form (1.47).

Daniel Plaumann
Technische Universität Dortmund
Sommersemester 2016
Fassung vom 17. Juli 2016

2. GRÖBNERBASEN

In diesem Kapitel beschäftigen wir uns mit der Frage, wie man mit Polynomen in mehreren Veränderlichen und den von ihnen erzeugten Idealen, die im ersten Kapitel eine große Rolle gespielt haben, am besten konkret rechnen kann.

Sei k ein Körper. Gegeben zwei Polynome $f, g \in k[x]$ in einer Variablen, dann können wir f mit Hilfe des euklidischen Algorithmus durch g teilen, d.h. es gibt $h, r \in k[x]$ mit

$$f = hg + r,$$

wobei der Rest r von kleinerem Grad als g ist. Diese Tatsache verallgemeinert nicht nur die Division mit Rest in den ganzen Zahlen, sie ist für das Rechnen im Polynomring in einer Variablen fundamental. Zum Beispiel können wir völlig problemlos entscheiden, ob $f \in \langle g \rangle$ gilt, denn das ist genau dann der Fall, wenn der Rest von f bei Division durch g gleich 0 ist.

Der Polynomring $k[x_1, \ldots, x_n]$ in mehreren Variablen ist zwar immerhin noch faktoriell, d.h. jedes Polynom kann eindeutig in irreduzible Faktoren zerlegt werden. Im Gegensatz zum Fall $n = 1$ ist er für $n \geqslant 2$ aber nicht mehr euklidisch, bekanntlich noch nicht einmal ein Hauptidealring. Um also zum Beispiel zu entscheiden, ob ein Polynom f im Ideal $\langle g_1, \ldots, g_r \rangle$ liegt, müssen wir im Stande sein, durch mehrere Polynome auf einmal 'mit Rest zu teilen'. Wir brauchen als erstes etwas Vorbereitung, um sagen zu können, was das überhaupt heißen soll.

2.1. Monomiale Ideale

Sei k ein Körper. Jedes Polynom $f \in k[x_1, \ldots, x_n]$ ist eine Linearkombination

$$f = \sum_{\alpha \in \mathbb{Z}_+^n} c_\alpha x^\alpha$$

von **Monomen** $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, wobei die Koeffizienten $c_\alpha \in k$ nur für endlich viele $\alpha \in \mathbb{Z}_+^n$ ungleich 0 sind. Ein Produkt $c_\alpha x^\alpha$ aus einem Monom und einem Koeffizienten heißt ein **Term**. Wir sagen, das Monom x^α **kommt in** f **vor**, wenn $c_\alpha \neq 0$ gilt. Außerdem schreiben wir

$$|\alpha| = \alpha_1 + \cdots + \alpha_n.$$

Die Monome mit der Multiplikation $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$ bilden ein Monoid mit Eins $x^0 = 1$, das offensichtlich einfach zum additiven Monoid $\mathbb{Z}_+^n$ isomorph ist.

Definition 2.1. Ein **monomiales Ideal** in $k[x_1, \ldots, x_n]$ ist ein von Monomen erzeugtes Ideal.

Ein monomiales Ideal ist also von der Form $\langle x^\alpha : \alpha \in T \rangle$ für eine Teilmenge $T \subset \mathbb{Z}_+^n$.

Definition 2.2. Die **natürliche Ordnung** auf $\mathbb{Z}_+^n$ ist die partielle Ordnung

$$\alpha \preceq \beta \quad \Longleftrightarrow \quad \alpha_i \leqslant \beta_i \text{ für alle } i = 1, \dots, n.$$

Lemma 2.3. *Die Elemente des monomialen Ideals $\langle x^\alpha : \alpha \in T \rangle$ sind genau die Linearkombinationen der Monome x^β mit $\beta \succeq \alpha$ für ein $\alpha \in T$.*

Beweis. Sei $I = \langle x^\alpha : \alpha \in T \rangle$. Ist $\alpha \in T$ und $\beta \succeq \alpha$, dann ist $x^\beta = x^{\beta-\alpha} x^\beta \in I$. Ist umgekehrt $f \in I$, dann gibt es $\alpha_1, \dots, \alpha_r \in T$ und Polynome $q_1, \dots, q_r$ mit $f = \sum_{i=1}^r q_i x^{\alpha_i}$. Jedes in f vorkommende Monom ist also von der Form $x^{\alpha_i+\gamma}$, wobei γ ein in q_i vorkommendes Monom ist. ∎

Ein monomiales Ideal besitzt also eine lineare Basis aus Monomen. Dagegen braucht ein allgemeines Ideal nicht ein einziges Monom zu enthalten, zum Beispiel das Ideal $\langle x + 1 \rangle \subset k[x]$.

Frage 2.4. Wie sieht man der Varietät $\mathcal{V}(I)$ an, ob $\sqrt{I}$ ein Monom enthält?

Satz 2.5 (Lemma von Gordan[1]/Dicksons[2] Lemma)**.** *Es sei T eine Teilmenge von $\mathbb{Z}_+^n$. Dann gibt es eine endliche Teilmenge S von T derart, dass für jedes $t \in T$ ein $s \in S$ mit $s \preceq t$ existiert.*

Beweis. Nach dem Hilbertschen Basissatz wird das monomiale Ideal $\langle x^\alpha : \alpha \in T \rangle$ bereits von einer endlichen Teilmenge von $\{x^\alpha : \alpha \in T\}$ erzeugt. Diese ist notwendig von der Form $\{x^\alpha : \alpha \in S\}$ für eine endliche Teilmenge $S \subset T$, und S hat offenbar die behauptete Eigenschaft. Das Lemma von Gordan ist also ein Spezialfall des Hilbertschen Basissatzes.

Wir geben auch noch einen direkten Beweis, der ohne den Basissatz auskommt. Es bezeichne $T_{\min}$ die Menge der minimalen Elemente von T. Da es in $\mathbb{Z}_+^n$ unter der natürlichen Ordnung keine unendlich absteigenden Ketten gibt, ist $T_{\min}$ offenbar genau die kleinste Teilmenge von T mit der gewünschten Eigenschaft. Die Aussage ist also gerade, dass $T_{\min}$ endlich ist.

Wir führen Induktion nach n. Für $n = 1$ ist die Aussage klar, denn jede nichtleere Teilmenge von $\mathbb{Z}_+$ enthält ein eindeutiges Element, also $|T_{\min}| = 1$. Sei $n \geqslant 2$ und die Aussage gelte für kleinere n. Für $k \geqslant 0$ setze

$$U_k = \{t' \in \mathbb{Z}_+^{n-1} : (t', k) \in T\} \qquad \text{und} \qquad U = \bigcup_{k \geqslant 0} U_k$$

Nach Induktionsvoraussetzung sind die Mengen $U_{\min}$ und $(U_k)_{\min}$ alle endlich. Insbesondere gibt es ein $m \geqslant 0$ mit $U_{\min} \subset U_0 \cup \dots \cup U_m$. Setze

$$S = \bigcup_{k=0}^{m} \big((U_k)_{\min} \times \{k\} \big).$$

Dann ist S eine endliche Teilmenge von T und wir behaupten, dass sie die gewünschte Eigenschaft hat. Sei dazu $t \in T$, etwa $t = (t', k)$, mit $t' \in \mathbb{Z}_+^{n-1}$ und $k \geqslant 0$. Ist $k \leqslant m$, so gibt es $u \in (U_k)_{\min}$ mit $u \preceq t'$ und es folgt $(u, k) \in S$ und $(u, k) \preceq (t', k) = t$. Ist $k > m$, so gibt es nach Wahl von m ein $l \leqslant m$ und ein $u \in (U_l)_{\min}$ mit $u \preceq t'$. Es folgt $(u, l) \in S$ und $(u, l) \preceq (t', k) = t$. ∎

Korollar 2.6. *Jedes monomiale Ideal wird von endlich vielen Monomen erzeugt.* ∎

Natürlich wussten wir das schon aus dem Basissatz, haben aber jetzt einen unhängigen Beweis.

[1] Paul Gordan (1837–1912), deutscher Mathematiker
[2] L. E. Dickson (1874–1954), US-amerikanischer Mathematiker

Übungen

Übung 2.1. Zeigen Sie: Die Anzahl der Monome vom Grad d in n Variablen $x_1, \dots, x_n$ ist $\binom{n+d-1}{d}$.

Übung 2.2. Es seien I ein monomiales Ideal und f ein Polynom in $k[x_1, \dots, x_n]$. Zeigen Sie, dass folgende Aussagen äquivalent sind:
(a) Es gilt $f \in I$.
(b) Jeder Term von f liegt in I.
(c) Das Polynom f ist eine Linearkombination von Monomen aus I.

2.2. Monomordnungen und Division mit Rest

Definition 2.7. Eine **(globale) Monomordnung** ist eine totale Ordnung $\leqslant$ auf $\mathbb{Z}_+^n$ mit den folgenden beiden Eigenschaften:

(1) Sind $\alpha, \beta \in \mathbb{Z}_+^n$ mit $\alpha \leqslant \beta$, so folgt $\alpha + \gamma \leqslant \beta + \gamma$ für alle $\gamma \in \mathbb{Z}_+^n$.
(2) $\alpha \geqslant 0$ für alle $\alpha \in \mathbb{Z}_+^n$.

Unter einer Monomordnung sind natürlich wie der Name schon sagt auch die Monome geordnet, und die Eigenschaften (1) und (2) übersetzen sich zu

(1) $x^\alpha \leqslant x^\beta \;\Rightarrow\; x^{\alpha+\gamma} \leqslant x^{\beta+\gamma}$.
(2) $x^\alpha \geqslant 1$.

für alle $\alpha, \beta, \gamma \in \mathbb{Z}_+^n$.

Neben den globalen Monomordnungen gibt es auch *lokale* Monomordnungen, in denen (1) gilt, statt (2) jedoch $x^\alpha < 1$ für alle $\alpha \in \mathbb{Z}_+^n$; ferner *gemischte* Monomordnungen, die weder global noch lokal sind. Wir werden uns aber auf globale Monomordnungen beschränken und lassen den Zusatz 'global' auch häufig weg.

Für $n = 1$ gibt es nur eine einzige Monomordnung, nämlich $1 < x < x^2 < \cdots$. Für $n \geqslant 2$ gibt es dagegen viele Monomordnungen. Jede globale Monomordnung $\leqslant$ auf $\mathbb{Z}_+^n$ ist feiner als die natürliche partielle Ordnung, d.h. $\alpha \preceq \beta$ impliziert $\alpha \leqslant \beta$. Denn $\alpha \preceq \beta$ bedeutet gerade $\beta - \alpha \in \mathbb{Z}_+^n$ und damit $\beta - \alpha \geqslant 0$ nach (2), also $\beta \geqslant \alpha$ nach (1).

Die am häufigsten benutzten globalen Monomordnungen sind die folgenden:

(1) Die **lexikographische Ordnung** lex: Es gilt $\alpha \leqslant \beta$, wenn $\alpha_i \leqslant \beta_i$ gilt für den ersten Index i, in dem sich α und β unterscheiden, das heißt:

$$\alpha >_{\mathsf{lex}} \beta \qquad \Longleftrightarrow \qquad \alpha_1 = \beta_1, \dots, \alpha_i = \beta_i, \alpha_{i+1} > \beta_{i+1} \text{ für ein } i \in \{1, \dots, n\}.$$

Also für $n = 2$ z.B. $(1,3) < (2,1)$, $(1,3) < (1,5)$ usw.

(2) Für jede Permutation der Koordinaten die entsprechende permutierte lexikographische Ordnung; insbesondere die **invers-lexikographische Ordnung** invlex, in der die letzte verschiedene Komponente entscheidet.

(3) Die **grad-lexikographische Ordnung** glex; in dieser gilt:

$$\alpha \leqslant_{\mathsf{glex}} \beta \qquad \Longleftrightarrow \qquad \begin{array}{l} |\alpha| < |\beta| \text{ oder} \\ |\alpha| = |\beta| \text{ und } \alpha \leqslant_{\mathsf{lex}} \beta \end{array}.$$

(4) Die **grad-revers-lexikographische Ordnung** grevlex, die folgendermaßen definiert ist:

$$\alpha <_{\text{grevlex}} \beta \iff \begin{array}{l} |\alpha| < |\beta| \text{ oder} \\ |\alpha| = |\beta| \text{ und } \alpha_{i+1} = \beta_{i+1}, \dots, \alpha_n = \beta_n, \alpha_i > \beta_i \\ \qquad \text{für ein } i \in \{1, \dots, n\} \end{array} .$$

Dabei entscheidet bei gleichem Grad also der letzte verschiedene Eintrag, aber in umgedrehter Richtung (deshalb 'revers'). Das sieht ein bißchen gekünstelt aus. Es hat sich aber erwiesen, dass diese Monomordnung in vielen Anwendungen besonders effizient ist (warum auch immer; siehe [Eisenbud], §15.7). Deshalb wird sie auch in den meisten Computer-Algebra-Systemen als Standard verwendet (z.B. Macaulay2 und Singular).

Natürlich muss man sich überzeugen, dass die angegebenen Monomordnungen auch tatsächlich welche sind (siehe Übung 2.3).

Lemma 2.8. *Es sei $\leqslant$ eine totale Ordnung auf $\mathbb{Z}_+^n$, welche die Eigenschaft (1) aus Def. 2.7 erfüllt. Dann sind äquivalent:*

(i) $\leqslant$ ist eine globale Monomordnung, also $\alpha \geqslant 0$ für alle $\alpha \in \mathbb{Z}_+^n$;

(ii) $\leqslant$ ist eine Wohlordnung, d.h. jede nicht-leere Teilmenge von $\mathbb{Z}_+^n$ hat ein kleinstes Element;

(iii) jede absteigende Folge $\alpha_1 \geqslant \alpha_2 \geqslant \alpha_3$ in $\mathbb{Z}_+^n$ wird stationär.

Beweis. (i)⇒(ii). Sei $\leqslant$ eine Monomordnung und sei $T \subset \mathbb{Z}_+^n$ eine nicht-leere Teilmenge. Nach dem Lemma von Gordan 2.5 gibt es eine endliche Teilmenge $S \subset T$ mit

$$\forall t \in T \; \exists s \in S\colon \; s \leq t.$$

Ist s_0 das bezüglich $\leqslant$ kleinste Element in S, so ist also $s_0 \leqslant t$ für alle $t \in T$, denn wie oben bemerkt ist $\leqslant$ feiner als die natürliche Ordnung.

(ii)⇒(iii) ist klar. (iii)⇒(i). Wäre $\alpha < 0$, dann wäre $0 > \alpha > 2\alpha > 3\alpha > \cdots$ eine unendlich absteigende Folge. ∎

Im folgenden *fixieren wir eine Monomordnung* $\leqslant$ auf $\mathbb{Z}_+^n$. Sei außerdem

$$f = \sum_{\alpha \in \mathbb{Z}_+^n} c_\alpha x^\alpha$$

ein Polynom, $f \neq 0$, und sei $\delta(f) = \max\{\alpha\colon c_\alpha \neq 0\}$ (das Maximum bezüglich der fixierten Monomordnung), der **Multigrad von f bezüglich** $\leqslant$. (Zur klaren Unterscheidung heißt die Zahl $\deg(f) = \max\{|\alpha|\colon c_\alpha \neq 0\}$ der **Totalgrad** von f). Also ist $x^{\delta(f)}$ das größte in f vorkommende Monom. Wie üblich setzen wir $\delta(0) = -\infty$. Weiter schreiben wir

$$\mathrm{LM}(f) = x^{\delta(f)}, \quad \mathrm{LC}(f) = c_{\delta(f)}, \quad \mathrm{LT}(f) = c_{\delta(f)} x^{\delta(f)}$$

und nennen $\mathrm{LM}(f)$ das **Leitmonom**, $\mathrm{LC}(f)$ den **Leitkoeffizienten** und $\mathrm{LT}(f)$ den **Leitterm** von f. Das Polynom f heißt **normiert**, wenn $\mathrm{LC}(f) = 1$ gilt.

Lemma 2.9. *Für $f, g \in k[x_1, \dots, x_n]$ gelten:*

(1) $\delta(fg) = \delta(f) + \delta(g)$;

(2) $\delta(f+g) \leqslant \max\{\delta(f), \delta(g)\}$, mit Gleichheit falls $\delta(f) \neq \delta(g)$ ist.

Beweis. trivial. ∎

Satz 2.10 (Division mit Rest). *Es sei eine Monomordnung $\leqslant$ fixiert und seien $g_1, \dots, g_s \in k[x_1, \dots, x_n]$, alle ungleich 0. Für jedes $f \in k[x_1, \dots, x_n]$ gibt es Polynome $q_1, \dots, q_s, r \in k[x_1, \dots, x_n]$ mit*

$$f = \sum_{i=1}^{s} q_i g_i + r$$

und mit den folgenden beiden Eigenschaften:

(1) Keines der im Polynom r vorkommenden Monome ist durch eines der Leitmonome $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$ teilbar;

(2) Es gilt $\delta(q_i g_i) \leqslant \delta(f)$ für $i = 1, \dots, s$.

Beachte: Aus (2) folgt insbesondere auch $\delta(r) \leqslant \delta(f)$, aber (2) ist im allgemeinen stärker.

Beweis. Der Beweis besteht aus einem Algorithmus, der die gesuchten Polynome produziert. Es sei $f \in k[x_1, \dots, x_n]$, ohne Einschränkung $f \neq 0$. Zunächst unterscheiden wir zwei Fälle:

(i) Das Leitmonom $\mathrm{LM}(f)$ ist durch eines der Monome $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$ teilbar. Ist j der kleinste Index mit $\mathrm{LM}(g_j) | \mathrm{LM}(f)$, etwa $\mathrm{LT}(f) = t \cdot \mathrm{LT}(g_j)$ für einen Term t, so setze $\widetilde{f} = f - t g_j$. Dann ist $\delta(\widetilde{f}) < \delta(f)$.

(ii) Das Leitmonom $\mathrm{LM}(f)$ ist durch keines der $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$ teilbar. Dann setzen wir $\widetilde{f} = f - \mathrm{LT}(f)$ und es gilt wieder $\delta(\widetilde{f}) < \delta(f)$.

Ist die Aussage für $\widetilde{f}$ richtig, dann haben wir also eine Darstellung

$$\widetilde{f} = \sum_{i=1}^{s} \widetilde{q}_i g_i + \widetilde{r}$$

mit Polynomen $\widetilde{q}_i, \widetilde{r}$ derart, dass die Eigenschaften (1) und (2) erfüllt sind. Daraus erhalten wir nun die Aussage für f: Falls wir im ersten Fall (i) sind, dann setzen wir $q_j = t + \widetilde{q}_j$, $q_i = \widetilde{q}_i$ für $i \neq j$ und $r = \widetilde{r}$. Aussage (2) bleibt richtig wegen $\delta(\widetilde{f}) < \delta(f)$ und

$$\delta(q_j g_j) = \delta(t g_j + \widetilde{q}_j g_j) \leqslant \max\{\delta(t g_j), \delta(\widetilde{q}_j g_j)\} = \delta(f)$$

(denn es ist $\delta(t g_j) = \delta(f)$ und $\delta(\widetilde{q}_j g_j) < \delta(\widetilde{f}) < \delta(f)$).

Im zweiten Fall (ii) setzen wir $r = \mathrm{LT}(f) + \widetilde{r}$ und $q_i = \widetilde{q}_i$ für $i = 1, \dots, s$. Dann bleibt (2) richtig und (1) ebenso nach der Voraussetzung in Fall (ii).

Dieses Verfahren endet nach endlich vielen Schritten, da der Multigrad in jedem Schritt kleiner wird und es keine unendlich absteigenden Folgen bezüglich der Monomordnung gibt. ∎

Definition 2.11. Das Polynom r in Satz 2.10 nennt man einen **Standardrest** von f bezüglich $g_1, \dots, g_s$ und der fixierten Monomordnung.

Im Fall $n = 1$ und $s = 1$ ist Satz 2.10 einfach die übliche Division mit Rest für Polynome in einer Variablen. Bekanntlich ist die Darstellung $f = q_1 g_1 + r$ in diesem Fall eindeutig. Im allgemeinen ist diese Eindeutigkeit aber nicht mehr gegeben, noch nicht einmal für $n = 1$: Sei $g_1 = x$ und $g_2 = x - 1$ in $k[x]$, dann hat $f = x$ die beiden Darstellungen

$$f = 1 \cdot x + 0(x - 1) + 0 = 0 \cdot x + 1(x - 1) + 1,$$

die beide die Eigenschaften (1) und (2) erfüllen. Nicht nur die Darstellungen, auch die beiden Standardreste sind verschieden.

Ein weiteres Beispiel mit $n = 2$ und $s = 2$: Sei $g_1 = xy + 1$ und $g_2 = y^2 - 1$ und

$$\begin{aligned} f = xy^2 - x &= y(xy+1) + 0 \cdot (y^2-1) - (x+y) \\ &= 0 \cdot (xy+1) + x(y^2-1) + 0. \end{aligned}$$

Wieder erfüllen beide Darstellungen (1) und (2) bezüglich jeder Monomordnung.

Die Division mit Rest ist für Polynome in mehreren Variablen also möglich, hat aber im allgemeinen keine guten Eigenschaften.

Idealerweise hätten wir gern,

(a) dass der Standardrest von f bezüglich $g_1, \ldots, g_s$ wenigstens bei fixierter Monomordnung wohldefiniert ist.

(b) dass dieser Standardrest genau dann 0 ist, wenn f im Ideal $\langle g_1, \ldots, g_s \rangle$ enthalten ist.

Wir werden zeigen, dass jedes Ideal ein Erzeugendensystem $g_1, \ldots, g_s$ besitzt derart, dass die Division mit Rest in gewünschter Weise funktioniert, nämlich eine sogenannte Gröbnerbasis.

In Macaulay2 kann man verschiedene Monomordnungen zusammen mit dem Ring spezifizieren. Zum Beispiel definiert `R = QQ[x,y,z,MonomialOrder=>GLex]` den Polynomring $\mathbb{Q}[x, y, z]$ mit der grad-lexikographischen Monomordnung. Die oben aufgeführten Monomordnungen heißen in Macaulay2 entsprechend `Lex`, `GLex` und `GRevLex` (die Voreinstellung).

Der Befehl `f % L` berechnet den Standardrest r eines Polynoms f bezüglich einer Matrix L von Polynomen. Der Befehl `f // L` produziert dagegen die Darstellung von $f - r$ im Ideal $\langle L \rangle$. Schauen wir uns das Beispiel von oben an.

```
i1 : R = QQ[x,y];
i2 : g1=x*y+1; g2=y^2-1; f = x*y^2-x;
i5 : L = matrix({{g1,g2}});

i6 : f % L
o6 = 0
o6 : R

i7 : f // L
o7 = {2} | y3-y     |
     {2} | -xy2+x-y |
               2       1
o7 : Matrix R  <--- R
```

Der Standardrest `f % L` ist 0, es gilt also $f \in \langle g_1, g_2 \rangle$. Der Output von `f//L` besteht aus den beiden Polynomen h_1, h_2 mit $f = h_1 g_1 + h_2 g_2$, die aus dem Divisionsalgorithmus entstehen.

Wenn man mit einem Ideal I arbeitet, dann liefert `gens I` die Liste von Erzeugern, die man im Divisionsalgorithmus verwenden kann.

```
i8 : I = ideal(g1,g2);
o8 : Ideal of R

i9 : f % (gens I)
o9 = 0
```

Übungen

Übung 2.3. Verifizieren Sie, dass lex, glex und grevlex tatsächlich Monomordnungen sind.

Übung 2.4. Ordnen Sie die Terme der folgenden Polynome bezüglich lex, glex und grevlex:

$$f = 2x + 3y + z + x^2 - z^2 + x^3, \qquad g = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4.$$

Übung 2.5. Betrachten Sie die totale Ordnung auf $\mathbb{Z}_+^n$, die durch

$$\alpha < \beta \qquad \Longleftrightarrow \qquad \alpha_{i+1} = \beta_{i+1}, \ldots, \alpha_n = \beta_n, \alpha_i > \beta_i \text{ für ein } i \in \{1, \ldots, n\}$$

gegeben ist. Entscheiden Sie, ob es sich um eine Monomordnung handelt.

Übung 2.6. Gegeben seien die folgenden drei Polynome in $k[x, y, z]$:

$$f = x^3 - x^2y - x^2z, \quad g_1 = x^2 - z, \quad g_2 = xy - 1.$$

(a) Verwenden Sie den Divisionsalgorithmus bezüglich glex, um die folgenden Reste zu berechnen: (1) den Rest r_1 von f bei Division durch (g_1, g_2); (2) den Rest r_2 von f bei Division durch (g_2, g_1).

(b) Seien r_1 und r_2 die Reste aus (a) und setze $r = r_1 - r_2$. Berechnen Sie den Rest von r bei Division durch (g_1, g_2). Ist das Ergebnis in irgendeiner Weise bemerkenswert?

Übung 2.7. Gegeben seien die Polynome

$$g_1 = 2xy^2 - x, \quad g_2 = 3x^2y - y - 1$$

in $\mathbb{Q}[x, y]$. Finden Sie ein Polynom $f \in \langle g_1, g_2 \rangle$, dessen Rest bei Division durch (g_1, g_2) gleich f selbst ist.

Übung 2.8*. Diese Aufgabe erklärt, wie man jede Monomordnung aus der lexikographischen erhält.

(a) Es sei $\leqslant$ eine Monomordnung auf $\mathbb{Z}_+^n$. Zeigen Sie, dass sich $\leqslant$ zu einer Anordnung der Gruppe $(\mathbb{Q}^n, +)$ fortsetzen lässt. (Das bedeutet: Es gibt eine totale Ordnung $\leqslant$ auf $\mathbb{Q}^n$, die auf $\mathbb{Z}_+^n$ mit der gegebenen Monomordnung übereinstimmt und die $\alpha \leqslant \beta \Rightarrow \alpha + \gamma \leqslant \beta + \gamma$ für alle $\alpha, \beta, \gamma \in \mathbb{Q}^n$ erfüllt.)

(b) Sei $V \subset \mathbb{Q}^n$ ein Unterraum der Dimension $r > 0$ und $V_{\mathbb{R}}$ der von V in $\mathbb{R}^n$ erzeugte Unterraum. Setze

$$V_0 = \left\{ x \in V_{\mathbb{R}} \colon \forall \varepsilon > 0 \exists z_+, z_i \in B_\varepsilon(x) \cap V \colon z_+ > 0, z_- < 0 \right\},$$

wobei $B_\varepsilon(x) = \{y \in V_{\mathbb{R}} \colon \|x - y\| < \varepsilon\}$. Zeigen Sie, dass V_0 ein $\mathbb{R}$-linearer Unterraum der Dimension $r-1$ ist. (*Hinweis:* Zeigen Sie für die Dimensionsaussage (1) $V_0 \cap V \neq V$; (2) Für je zwei Punkte $\alpha, \beta \in V$ mit $\alpha > 0$ und $\beta < 0$ hat die Verbindungsgerade $\{\lambda\alpha + (1-\lambda)\beta \colon \lambda \in \mathbb{R}\}$ einen Schnittpunkt mit V_0.)

(c) Zeigen Sie, dass es eine Matrix $A \in \mathrm{GL}_n(\mathbb{R})$ gibt derart, dass

$$\alpha \geqslant 0 \qquad \Longleftrightarrow \qquad A \cdot \alpha \geqslant_{\mathsf{lex}} 0$$

gilt, wobei lex die lexikographische Ordnung auf $\mathbb{R}^n$ bezeichnet. (*Hinweis.* Zur Veranschaulichung betrachten Sie den Fall der lexikographischen Ordnung auf $V = \mathbb{Q}^n$. Was ist dann V_0 in (b)?)

2.3. Gröbnerbasen und der Buchberger-Algorithmus

Wir arbeiten in diesem Abschnitt immer mit einer fixierten Monomordnung $\leqslant$.

Definition 2.12. Sei I ein Ideal in $k[x_1, \ldots, x_n]$. Das monomiale Ideal

$$L(I) = \big\langle \mathrm{LM}(f) \colon f \in I \setminus \{0\} \big\rangle,$$

das von den Leitmonomen aus I erzeugt wird, heißt das **Leitideal** von I.

Wenn wir Erzeuger von I wählen, etwa $I = \langle g_1, \ldots, g_s \rangle$, dann gilt $\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s) \rangle \subset L(I)$. Im allgemeinen gilt aber keine Gleichheit: Betrachte zum Beispiel wieder $g_1 = xy + 1$, $g_2 = y^2 - 1$ und $I = \langle g_1, g_2 \rangle$. Dann ist $\mathrm{LM}(g_1) = xy$ und $\mathrm{LM}(g_2) = y^2$ (bezüglich jeder Monomordnung), aber es gilt

$$yg_1 - xg_2 = (xy^2 + y) - (xy^2 - x) = x + y.$$

Also liegt, je nach Monomordnung, auch x oder y in $L(I)$, aber nicht in $\langle \mathrm{LM}(g_1), \mathrm{LM}(g_2) \rangle$. Es zeigt sich, dass darin im Zusammenhang mit der Division mit Rest genau das entscheidende Problem liegt.

Definition 2.13. Sei I ein Ideal in $k[x_1, \ldots, x_n]$. Eine endliche Teilmenge G von I mit $0 \notin G$ heißt eine **Gröbnerbasis**[3] von I, wenn gilt

$$L(I) = \big\langle \mathrm{LM}(g) \colon g \in G \big\rangle,$$

wenn also das Leitideal von den Leitmonomen der Basiselemente erzeugt wird.

Satz 2.14. *Jedes Ideal in $k[x_1, \ldots, x_n]$ hat eine Gröbnerbasis. Jede Gröbnerbasis eines Ideals I ist ein Erzeugendensystem von I.*

Beweis. Sei I ein Ideal. Falls $I = \langle 0 \rangle$, dann ist die leere Menge eine Gröbnerbasis von I. Sei also $I \neq \langle 0 \rangle$. Nach Definition gilt $L(I) = \langle \mathrm{LM}(g) \colon g \in I \rangle$. Nach dem Lemma von Gordan wird das monomiale Ideal $L(I)$ schon von endlich vielen der Monome $\mathrm{LM}(g)$ erzeugt. Es gibt also eine endliche Teilmenge $G = \{g_1, \ldots, g_s\}$ von $I \setminus \{0\}$ mit $L(I) = (\mathrm{LM}(g_1), \ldots, LM(g_s))$. Damit ist G eine Gröbnerbasis von I.

Sei nun G irgendeine Gröbnerbasis von I. Das von G erzeugte Ideal $J = \langle G \rangle$ ist dann in I enthalten. Umgekehrt sei $f \in I \setminus \{0\}$. Division mit Rest bezüglich $g_1, \ldots, g_r$ liefert einen Standardrest r, dessen Monome durch keines der $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$ teilbar sind. Aus $f \in I$ folgt außerdem $r \in I$. Wäre $r \neq 0$, so wäre also $\mathrm{LM}(r) \in L(I)$ und damit durch eines der Monome $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$ teilbar (Lemma 2.3), ein Widerspruch. Also ist $r = 0$ und damit $f \in J$. ∎

Da Gröbnerbasen nach Definition endlich sind, haben wir damit nebenbei auch den Hilbertschen Basissatz neu bewiesen.

Korollar 2.15. *Jedes Ideal in $k[x_1, \ldots, x_n]$ ist endlich erzeugt.* ∎

Wir zeigen nun, dass die Division mit Rest für Gröbnerbasen gute Eigenschaften hat.

[3] Wolfgang Gröbner (1899–1980), österreichischer Mathematiker

Satz 2.16. *Es sei I ein Ideal in $k[x_1, \ldots, x_n]$. Der Standardrest eines Polynoms f bezüglich einer Gröbnerbasis von I ist eindeutig bestimmt und hängt sogar nur von f, I und der gewählten Monomordnung ab.*

Beweis. Es seien $G = \{g_1, \ldots, g_s\}$ und $G' = \{g'_1, \ldots, g'_{s'}\}$ zwei Gröbnerbasen von I. Seien r bzw. r' Standardreste von f bezüglich G bzw. G'. Per Definition ist keines der in r vorkommenden Monome durch $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$ teilbar. Da G eine Gröbnerbasis ist, liegt also keines der Monome von r in $L(I)$. Ebenso liegt keines der Monome von r' in $L(I)$. Dann gilt dasselbe auch für $r - r'$. Andererseits gilt $r - r' \in I$. Wäre $r - r' \neq 0$, so also $\mathrm{LM}(r - r') \in L(I)$, Widerspruch. ∎

Der Standardrest r eines Polynoms f bezüglich einer Gröbnerbasis G wird auch als **Reduktion** von f modulo I bezeichnet und man sagt, dass f modulo I zu r **reduziert**.

Korollar 2.17. *Genau dann liegt ein Polynom f in einem Ideal I, wenn es modulo I zu 0 reduziert.*

Beweis. Sei G eine Gröbnerbasis. Wenn f modulo I zu 0 reduziert, dann gilt $f \in I$. Gilt umgekehrt $f \in I$, so ist $G \cup \{f\}$ eine Gröbnerbasis von I die für f offenbar den Standardrest 0 liefert. ∎

Da die Division mit Rest konstruktiv ist, können wir damit die Frage, ob ein Polynom in einem gegebenem Ideal liegt, durch einen Algorithmus beantworten, vorausgesetzt, wir kennen eine Gröbnerbasis des Ideals. Als grundlegendes Rechenproblem bleibt damit nur die Frage, wie man eine Gröbnerbasis findet.

Es ist zunächst aus der Definition nicht klar, wie man praktisch überprüfen kann, dass ein gegebenes Erzeugendensystem eines Ideals I eine Gröbnerbasis ist. Denn wie findet man Erzeuger des Leitideals $L(I)$? Das **Buchberger-Kriterium**[4] stellt einen praktikablen Test dar, der auch den Schlüssel zur Konstruktion von Gröbnerbasen enthält.

Wie zuvor fixieren wir eine Monomordnung $\leqslant$. Für $\alpha, \beta \in \mathbb{Z}_+^n$ setzen wir

$$\alpha \wedge \beta = \big(\min\{\alpha_1, \beta_1\}, \ldots, \min\{\alpha_n, \beta_n\}\big)$$

(gelesen: α *meet* β) und

$$\alpha \vee \beta = \big(\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}\big).$$

(gelesen: α *join* β). Damit ist

$$\mathrm{ggT}(x^\alpha, x^\beta) = x^{\alpha \wedge \beta} \quad \text{und} \quad \mathrm{kgV}(x^\alpha, x^\beta) = x^{\alpha \vee \beta}.$$

Frage 2.18. Überprüfen Sie die Gleichheit $\alpha \vee \beta = \alpha + \beta - \alpha \wedge \beta$.

Definition 2.19. Für je zwei Polynome $f, g \neq 0$ ist das **S-Polynom von f und g** definiert durch

$$S(f,g) = \frac{\mathrm{LT}(g)f - \mathrm{LT}(f)g}{\mathrm{ggT}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big)} = \frac{\mathrm{LT}(g)f - \mathrm{LT}(f)g}{x^{\delta(f) \wedge \delta(g)}}.$$

Es ist klar, dass $S(f,g)$ ein Polynom ist, weil der Nenner beide Summanden im Zähler teilt. Nach Konstruktion kürzen sich außerdem im Zähler die Leitterme. Damit gilt

$$\delta\big(S(f,g)\big) < \delta(f) + \delta(g) - (\delta(f) \wedge \delta(g)) = \delta(f) \vee \delta(g).$$

[4] Bruno Buchberger (geb. 1942) österreichischer Mathematiker; entwickelte Gröbnerbasen in seiner Dissertation bei Gröbner.

Wir bemerken außerdem, dass man Skalare herausziehen kann, d.h. es gilt

$$S(af, bg) = abS(f, g)$$

für alle Polynome $f, g \neq 0$ und alle $a, b \in k^\times$.

Lemma 2.20. *Es seien $g_1, \ldots, g_r \neq 0$ Polynome vom Multigrad α und seien $a_1, \ldots, a_r \in k$. Falls*

$$\delta\Big(\sum_{i=1}^r a_i g_i\Big) < \alpha$$

dann ist $\sum_{i=1}^r a_i g_i$ eine Linearkombination der S-Polynome $S(g_i, g_{i+1})$ ($i = 1, \ldots, r-1$).

Wie wir gerade bemerkt haben, gilt $\delta(S(g_i, g_j)) < \alpha$ für alle i, j. Deshalb ist das Kriterium im Lemma auch notwendig.

Beweis. Setze $b_i = \mathrm{LC}(g_i)$ und $p_i = \frac{1}{b_i} g_i$ für $i = 1, \ldots, r$. Setze außerdem $p_{r+1} = 0$. Die Voraussetzung $\delta(\sum_{i=1}^r a_i g_i) < \alpha$ bedeutet gerade $\sum_{i=1}^r a_i b_i = 0$. Es folgt

$$\begin{aligned}\sum_{i=1}^r a_i g_i = \sum_{i=1}^r a_i b_i p_i &= \sum_{i=1}^r \Bigg(\sum_{j=1}^i a_j b_j\Bigg)(p_i - p_{i+1}) \\ &= \sum_{i=1}^{r-1} \Bigg(\sum_{j=1}^i a_j b_j\Bigg)(p_i - p_{i+1}).\end{aligned}$$

Die letzte Gleichheit benutzt dabei $\sum_{i=1}^r a_i b_i = 0$. Die S-Polynome sind gerade

$$S(g_i, g_j) = \frac{b_j x^\alpha g_i - b_i x^\alpha g_j}{x^\alpha} = b_j g_i - b_i g_j = b_i b_j (p_i - p_j),$$

womit das Lemma bewiesen ist. ∎

Satz 2.21 (Buchberger-Kriterium)**.** *Es sei $(g_1, \ldots, g_s)$ eine Folge von Polynomen $\neq 0$. Für jedes Paar (i, j) von Indizes sei h_{ij} ein Standardrest von $S(g_i, g_j)$ bezüglich $g_1, \ldots, g_s$. Genau dann ist $\{g_1, \ldots, g_s\}$ eine Gröbnerbasis von $\langle g_1, \ldots, g_s\rangle$, wenn $h_{ij} = 0$ für alle $i < j$ gilt.*

Beweis. Sei $G = \{g_1, \ldots, g_s\}$ und $I = \langle G\rangle$. Falls G eine Gröbnerbasis von I ist, dann sind wegen $S(g_i, g_j) \in I$ die Standardreste $h_{ij} = 0$ für alle i, j, nach Korollar 2.17.

Umgekehrt seien die Voraussetzungen des Buchberger-Kriteriums erfüllt. Sei $f \in I$, $f \neq 0$. Wir müssen zeigen, dass das Leitmonom $\mathrm{LM}(f)$ von einem der Leitmonome $\mathrm{LM}(g_i)$, $i = 1, \ldots, s$ geteilt wird. Nach Voraussetzung gibt es eine Darstellung

$$f = \sum_{i=1}^s q_i g_i \qquad (*)$$

für geeignete Polynome $q_1, \ldots, q_s$, und wir setzen

$$\vartheta = \max_{i=1,\ldots,s} \delta(q_i g_i).$$

Offenbar gilt $\delta(f) \leqslant \vartheta$. Falls Gleichheit gilt, dann sind wir fertig. Denn dann folgt

$$\mathrm{LM}(f) = x^{\delta(f)} = \mathrm{LM}(q_i g_i) = \mathrm{LM}(q_i)\,\mathrm{LM}(g_i)$$

für ein i und die Behauptung ist bewiesen.

Falls $\vartheta > \delta(f)$, dann produzieren wir eine neue Darstellung der Form $(*)$, in der alle Multigrade $\delta(q_i g_i)$ strikt kleiner als ϑ sind. Nach endlich vielen Schritten erhalten wir so eine Darstellung mit $\delta(f) = \vartheta$, wie gewünscht.

Setze $\vartheta_i = \delta(q_i g_i)$ für $i = 1, \dots, s$. Nach Umnummerieren können wir annehmen, dass $\vartheta_i = \vartheta$ für $i = 1, \dots, t$ und $\vartheta_i < \vartheta$ für $i = t+1, \dots, s$ gilt, mit $1 \leqslant t \leqslant s$. Zerlege die Summe $(*)$ wie folgt:

$$f = \sum_{i=1}^{t} \mathrm{LT}(q_i) g_i + \sum_{i=1}^{t} \big(q_i - \mathrm{LT}(q_i)\big) g_i + \sum_{i=t+1}^{s} q_i g_i.$$

Setze zur Abkürzung $A = \sum_{i=1}^{t} \mathrm{LT}(q_i) g_i$. Da die Terme in der zweiten und der dritten Summe alle kleineren Multigrad als ϑ haben und f ebenso, folgt auch $\delta(A) < \vartheta$. Es genügt, A in der Form $A = \sum_{i=1}^{s} \widetilde{q}_i g_i$ mit geeigneten $\widetilde{q}_i$ so darzustellen, dass $\delta(\widetilde{q}_i g_i) < \vartheta$ für alle $i = 1, \dots, s$ gilt.

Wir wenden Lemma 2.20 auf A und die Polynome $\mathrm{LM}(q_i) g_i$ für $i = 1, \dots, t$ an und schließen, dass A eine Linearkombination der S-Polynome

$$s_{ij} = S\big(\mathrm{LM}(q_i) g_i, \mathrm{LM}(q_j) g_j\big)$$

für $1 \leqslant i, j \leqslant t$ ist. Um die Polynome s_{ij} durch $S(g_i, g_j)$ auszudrücken, schreiben wir $\alpha_i = \delta(g_i)$. Dann ist $\mathrm{LM}(q_i) g_i = x^{\vartheta - \alpha_i} g_i$ für $i = 1, \dots, t$, also $\alpha_i \preceq \vartheta$ und

$$\begin{aligned} s_{ij} &= x^{-\vartheta} \Big(x^{\vartheta - \alpha_j} \mathrm{LT}(g_j) x^{\vartheta - \alpha_i} g_i - x^{\vartheta - \alpha} \mathrm{LT}(g_i) x^{\vartheta - \alpha_j} g_j \Big) \\ &= x^{\vartheta - (\alpha_i + \alpha_j)} \big(\mathrm{LT}(g_j) g_i - \mathrm{LT}(g_i) g_j \big) \\ &= x^{\beta_{ij}} S(g_i, g_j), \end{aligned}$$

wobei

$$\beta_{ij} = \vartheta - (\alpha_i + \alpha_j) + (\alpha_i \wedge \alpha_j) = \vartheta - (\alpha_i \vee \alpha_j) \geqslant 0$$

für $i, j = 1, \dots, t$. Nach Voraussetzung haben wir $h_{ij} = 0$ und damit Darstellungen

$$S(g_i, g_j) = \sum_{k=1}^{s} p_{ijk} g_k$$

mit Polynomen p_{ijk} derart, dass

$$\delta(p_{ijk} g_k) \leqslant \delta\big(S(g_i, g_j)\big) < \alpha_i \vee \alpha_j$$

für alle i, j, k gilt. Für $i, j = 1, \dots, t$ ist also $s_{ij} = \sum_k \widetilde{p}_{ijk} g_k$ mit $\widetilde{p}_{ijk} = x^{\beta_{ij}} p_{ijk}$, und dabei ist

$$\delta(\widetilde{p}_{ijk} g_k) = \beta_{ij} + \delta(p_{ijk} g_k) < \vartheta$$

für alle k. Damit haben wir die gesuchte Darstellung von A gefunden. ∎

Aus dem Buchberger-Kriterium erhalten wir nun leicht einen Algorithmus zur Berechnung einer Gröbner-Basis für ein beliebiges Ideal.

Satz 2.22. *Seien $g_1, \dots, g_s \neq 0$ Polynome und $I = \langle g_1, \dots, g_s \rangle$. Der folgende Algorithmus produziert eine Gröbner-Basis von I:*
Berechne alle Standardreste h_{ij} der S-Polynome $S(g_i, g_j)$ bezüglich $g_1, \dots, g_s$ für $i < j$. Sind

alle $h_{ij} = 0$, so ist $\{g_1, \ldots, g_s\}$ eine Gröbnerbasis von I. Ist erstmals $h_{ij} \neq 0$ für ein Paar $i < j$, so füge h_{ij} zu $g_1, \ldots, g_s$ hinzu und starte erneut mit der verlängerten Folge.

Beweis. Nach dem Buchberger-Kriterium müssen wir nur noch beweisen, dass der Algorithmus terminiert, also irgendwann alle h_{ij} tatsächlich 0 sind. Ist $h_{ij} \neq 0$, so ist die Inklusion

$$\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s) \rangle \subsetneq \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s), \mathrm{LM}(h_{ij}) \rangle$$

von monomialen Idealen strikt. Denn nach Definition des Standardrests wird $\mathrm{LM}(h_{ij})$ von keinem der $\mathrm{LM}(g_k)$ für $k = 1, \ldots, s$ geteilt. Nach Korollar 2.3 können die beiden obigen Ideale nicht gleich sein. Andererseits wird jede aufsteigende Folge von monomialen Idealen stationär, nach Kor. 2.6. Wenn das geschieht, bricht der Algorithmus also ab. ∎

Das ist die einfachste Form des Buchberger-Algorithmus. Sie produziert häufig sehr große, redundante Gröbnerbasen und in tatsächlichen Implementierungen werden viele Verfeinerungen vorgenommen, um die Leistung zu verbessern.[5]

In Macaulay2 kann man eine Gröbnerbasis eines Ideals I mit dem Befehl `gb I` berechnen. Da viele Berechnungen in Macaulay2 eine Gröbnerbasis eines Ideals (oder eines daraus abgeleiteten Hilfsideals) voraussetzen, berechnet Macaulay2 Gröbnerbasen aber auch häufig automatisch im Hintergrund, so dass man den expliziten Befehl tatsächlich eher selten braucht.

```
i1 : R = QQ[x,y];
i2 : g1=x*y+1; g2=y^2-1; f = x*y^2-x;

i3 : gb I
o3 = GroebnerBasis[status: done; S-pairs encountered up to degree 3]
o3 : GroebnerBasis
```

Der Output zeigt die Elemente der Gröbnerbasis nicht an. Dazu dient wieder der Befehl `gens`.

```
i4 : gens gb I

o4 = | x+y y2-1 |
               1       2
o4 : Matrix R  <--- R
```

Übungen

Übung 2.9. Es sei $G = \{x^2 - y, x^3 - z\} \subset k[x, y, z]$. Entscheiden Sie, ob G eine Gröbnerbasis von $\langle G \rangle$ ist, (a) bezüglich grlex; (b) bezüglich invlex.

Übung 2.10. Es sei $G = \{x + z, y - z\} \subset k[x, y, z]$.

(a) Zeigen Sie, dass G eine Gröbnerbasis von $\langle G \rangle$ bezüglich lex ist.

(b) Teilen Sie xy durch $(x + z, y - z)$ und durch $(y - z, x + z)$. Was fällt dabei auf?

[5] Außerdem ist der Buchberger-Algorithmus auch mit Verfeinerungen inzwischen nicht mehr das letzte Wort. Der im allgemeinen beste Algorithmus stammt von Jean-Charles Faugère aus dem Jahr 2002 und wird als $F5$-Algorithmus bezeichnet. Er ist in `Singular` inzwischen implementiert, nicht jedoch in Macaulay2.

Übung 2.11. Es sei I ein Hauptideal im Polynomring $k[x_1, \ldots, x_n]$. Zeigen Sie, dass jede endliche Teilmenge von I, die einen Erzeuger von I enthält, eine Gröbnerbasis ist.

Übung 2.12. Beweisen Sie folgende Umkehrung von Kor. 2.17. Sei $G \subset k[x_1, \ldots, x_n]$ eine endliche Teilmenge, $I = \langle G \rangle$. Falls jedes Element von I modulo G zu 0 reduziert, so ist G eine Gröbnerbasis von I.

Übung 2.13. Verwenden Sie das Buchberger-Kriterium, um zu entscheiden, ob die folgenden Mengen von Polynomen in $k[x, y, z]$ Gröbnerbasen sind.
(a) $G = \{x^2 - y, x^3 - z\}$ bezüglich grlex;
(b) $G = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$ bezüglich lex.

Übung 2.14. Verwenden Sie den Buchberger-Algorithmus, um eine Gröbnerbasis für die folgenden Ideale in $k[x, y, z]$ zu finden.
(a) $I = \langle x^2y - 1, xy^2 - x \rangle$ bezüglich lex und grlex;
(b) $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3 \rangle$ bezüglich grlex.

2.4. Minimale und reduzierte Gröbnerbasen

Fügt man einer Gröbnerbasis eines Ideals I beliebig endlich viele Elemente aus $I \setminus \{0\}$ hinzu, erhält man nach Definition wieder eine Gröbnerbasis. Der Buchberger-Algorithmus tendiert dazu, Gröbnerbasen zu produzieren, die in diesem Sinn viel zu groß, also redundant sind. Es stellt sich die Frage, wie man überflüssige Erzeuger systematisch loswerden kann.

Lemma 2.23. *Es sei G eine Gröbnerbasis des Ideals I. Wird das Leitmonom eines Elements $g \in G$ vom Leitmonom eines Elements $h \in G \setminus \{g\}$ geteilt, so ist auch $G \setminus \{g\}$ eine Gröbnerbasis von I.*

Beweis. Sei $J = \langle G \setminus \{g\} \rangle$. Dann ist $J \subset I$ und nach Voraussetzung gilt

$$L(J) \subset L(I) = \langle \mathrm{LM}(G) \rangle = \langle \mathrm{LM}(G \setminus \{g\}) \rangle \subset L(J)$$

Also ist $L(I) = \langle \mathrm{LM}(G \setminus \{g\}) \rangle$ und somit auch $G \setminus \{g\}$ eine Gröbnerbasis von I. ∎

Definition 2.24. Eine Gröbnerbasis G heißt **minimal**, falls $\mathrm{LM}(h) \nmid \mathrm{LM}(g)$ für alle $g \neq h$ in G.

Nach dem obigen Lemma können wir eine Gröbnerbasis, die wir etwa mit dem Buchberger-Algorithmus erzeugt haben, sehr leicht so lange ausdünnen, bis sie minimal ist.

Lemma 2.25. *Für jede minimale Gröbnerbasis G eines Ideals I ist $\mathrm{LM}(G)$ die Menge der bezüglich $\leqslant$ minimalen Monome in $L(I)$. Insbesondere haben alle minimalen Gröbnerbasen von I (bezüglich derselben Monomordnung) dieselbe Länge.*

Beweis. Die minimalen Monome von $\mathrm{LM}(I)$ müssen für jede Gröbnerbasis G offenbar in $\mathrm{LM}(G)$ enthalten sein. Die Umkehrung folgt aus der Minimalität von G. ∎

Korollar 2.26. *Für eine Gröbnerbasis G eines Ideals I sind äquivalent:*
(i) G ist minimal gemäß Def. 2.24.
(ii) G ist minimal unter allen Gröbnerbasen bezüglich Inklusion.
(iii) G hat unter allen Gröbnerbasen die minimale Mächtigkeit. ∎

Für manche Anwendungen problematisch ist die Tatsache, dass ein Ideal im allgemeinen immer noch viele verschiedene minimale Gröbnerbasen besitzt. Dieses Problem lässt sich eliminieren, indem man eine weitere Minimalitätsforderung hinzufügt.

Definition 2.27. Eine Gröbnerbasis G heißt **reduziert**, wenn jedes Element von G normiert ist und für jedes $g \in G$ gilt: Für $h \in G \setminus \{g\}$ ist keines der Monome in g durch $\mathrm{LM}(h)$ teilbar.

Nach Definition ist jede reduzierte Gröbnerbasis auch minimal. Der wesentliche Unterschied liegt in der folgenden Aussage.

Satz 2.28. *Bei fixierter Monomordnung besitzt jedes Ideal eine eindeutige reduzierte Gröbnerbasis.*

Beweis. Wir zeigen zunächst die Existenz einer reduzierten Gröbnerbasis. Sei dazu $G \neq \varnothing$ eine minimale Gröbnerbasis von $I = \langle G \rangle$. Wir nennen ein Element $g \in G$ reduziert bezüglich G, wenn es die gewünschte Eigenschaft besitzt, wenn also kein in g vorkommendes Monom durch irgendein Leitmonom $\mathrm{LM}(h)$ für $h \neq g$ aus G teilbar ist.

Sei $g \in G$ und sei g' ein Standardrest von g bezüglich $G \setminus \{g\}$. Ersetze nun g durch g', d.h. setze $G' = (G \setminus \{g\}) \cup \{g'\}$. Aufgrund der Minimalität von G ist $\mathrm{LM}(g)$ durch keines der $\mathrm{LM}(h)$ für $h \in G \setminus \{g\}$ teilbar. Deshalb ist $\mathrm{LM}(g') = \mathrm{LM}(g)$. Wegen $g' \in I$ ist also auch G' eine minimale Gröbnerbasis von I. Nach Konstruktion ist dabei nun g' reduziert bezüglich G'.

Indem wir mit allen Elementen von G so verfahren, erhalten wir nach endlich vielen Schritten eine Gröbnerbasis $\widetilde{G}$, deren Elemente alle reduziert bezüglich $\widetilde{G}$ sind. Nach Normieren aller Elemente, durch Multiplikation von $g \in \widetilde{G}$ mit $\frac{1}{\mathrm{LC}(g)}$, haben wir eine reduzierte Gröbnerbasis.

Um die Eindeutigkeit zu beweisen, seien G und G' zwei reduzierte Gröbnerbasen von I. Dann ist insbesondere $\mathrm{LM}(G) = \mathrm{LM}(G')$ nach Lemma 2.25. Sei $g \in G$ und sei $g' \in G$ das (eindeutige) Element mit $\mathrm{LM}(g') = \mathrm{LM}(g)$. Wegen $g - g' \in I$ und $\delta(g - g') < \delta(g)$ muss $g - g' = 0$ sein, denn sonst wäre $\mathrm{LM}(g - g')$ teilbar durch $\mathrm{LM}(h)$ für ein $h \in G$. Also gilt $G \subset G'$ und aus Symmetriegründen auch $G = G'$. ∎

Wieder ist der Beweis konstruktiv, so dass wir einen Algorithmus zur Berechnung der reduzierten Gröbnerbasis eines Ideals mit vorgebenenen Erzeugern haben.

Der Befehl `gens gb I` in Macaulay2 produziert automatisch eine reduzierte Gröbnerbasis.

Übungen

Übung 2.15. Der Buchberger-Algorithmus verallgemeinert gleichzeitig das gaußsche Eliminationsverfahren aus der linearen Algebra und den euklidischen Algorithmus für Polynome in einer Variablen.

(a) Seien $f_1, \ldots, f_r$ Linearformen in $k[x_1, \ldots, x_n]$, etwa

$$f_i = \sum_{j=1}^{n} a_{ij} x_j.$$

Zeigen Sie: Die reduzierte Gröbnerbasis des Ideals $I = \langle f_1, \ldots, f_r \rangle$ bezüglich lex entspricht genau der reduzierten Zeilenstufenform der Matrix $A = (a_{ij})$ (also mit Pivotelement 1 in jeder

Zeile und Nullen an allen anderen Stellen der Pivotspalten). Soll heißen: Sei $B = (b_{ij})$ die besagte reduzierte Zeilenstufenform und $g_1, \dots, g_s$ die zu den von Null verschiedenen Zeilen von B gehörenden Linearformen. Dann ist $\{g_1, \dots, g_s\}$ die reduzierte Gröbnerbasis von I.

(b) Sei $n = 1$ und seien $f, g \in k[x]$ Polynome ungleich 0. Zeigen Sie: Die reduzierte Gröbnerbasis von $\langle f, g\rangle$ bezüglich lex besteht aus dem normierten ggT von f und g.

2.5. Anwendungen

Mit Hilfe von Gröbnerbasen kann man eine ganze Reihe von algorithmischen Problemen lösen, die in der algebraischen Geometrie von Bedeutung sind. Die beiden wichtigsten sind zunächst der Inklusionstest und die Berechnung von Eliminationsidealen. Viele weitere Anwendungen ergeben sich aus diesen beiden Grundbausteinen.

2.5.1. Inklusionstest. Gegeben Polynome $f_1, \dots, f_r$ und f. Entscheide, ob $f \in \langle f_1, \dots, f_r\rangle$ gilt.

Konstruiere dazu eine Gröbnerbasis $G = \{g_1, \dots, g_s\}$ von $I = \langle f_1, \dots, f_r\rangle$ und bestimme den Standardrest von f bezüglich G durch Division mit Rest. Nach Kor. 2.17 gilt $f \in I$ genau dann, wenn dieser Standardrest 0 ist.

Allgemeiner kann man damit auch die Frage nach der Inklusion oder Gleichheit von zwei Idealen im Polynomring entscheiden. Denn sind I und J Ideale in $k[x_1, \dots, x_n]$, dann gilt $I \subset J$ genau dann, wenn J eine Menge von Erzeugern von I enthält.

> In Macaulay2 kann man den Standardrest eines Polynoms f bezüglich eines Ideals I mit dem Befehl `f % I` berechnen lassen. Nach Satz 2.16 hängt der Standardrest außer von f und I nur noch von der gewählten Monomordnung ab, die in Macaulay2 in den Ring integriert ist.
>
> Die Inklusion $J \subset I$ testet der Befehl `isSubset(J,I)`. Für beides berechnet Macaulay2 eine Gröbnerbasis von I, auch ohne explizite Anweisung.

2.5.2. Lösbarkeit von Gleichungssystemen. Die erste direkte Anwendung des Inklusionstests ist der schwache Nullstellensatz: Sind $f_1, \dots, f_r \in k[x_1, \dots, x_n]$, so gilt $\mathcal{V}(f_1, \dots, f_r) = \varnothing$ genau dann, wenn $1 \in \langle f_1, \dots, f_r\rangle$ gilt (Satz 1.28). Ob das der Fall ist, können wir durch einen Inklusionstest nachprüfen. Damit haben wir einen Algorithmus, der direkt entscheidet, ob ein Gleichungssystem lösbar oder unlösbar ist.

2.5.3. Eliminationsideale. Sei I ein Ideal in $k[x_1, \dots, x_n]$. Für $j = 1, \dots, n$ heißt

$$I_j = I \cap k[x_{j+1}, \dots, x_n]$$

das j-**te Eliminationsideal von** I. Dies ist ein Ideal im Polynomring $k[x_{j+1}, \dots, x_n]$ und hat, wie wir wissen, folgende geometrische Interpretation: Sei $V = \mathcal{V}(I) \subset \mathbb{A}^n$, $W_j = \mathcal{V}(I_j) \subset \mathbb{A}^{n-j}$ und

$$\pi_j \colon \mathbb{A}^n \to \mathbb{A}^{n-j},\ (x_1, \dots, x_n) \mapsto (x_{j+1}, \dots, x_n).$$

Dann ist W_j der Zariski-Abschluss der Projektion $\pi_j(V)$ (Satz 1.42). Das Eliminationsideal I_j lässt sich mit Hilfe von Gröbnerbasen folgendermaßen berechnen.

Definition 2.29. Eine Monomordnung $\leqslant$ auf $\mathbb{Z}_+^n$ heißt **Eliminationsordnung** für $x_1, \dots, x_j$, falls

$$x_{j+1}^{\alpha_{j+1}} \cdots x_n^{\alpha_n} < x_i \quad \text{für alle } i = 1, \dots, j \text{ und alle } \alpha_{j+1}, \dots, \alpha_n \geqslant 0$$

gilt, falls also die Variablen $x_1, \dots, x_j$ größer sind als alle Monome in den übrigen Variablen.

Offenbar ist die lexikographische Ordnung eine Eliminationsordnung für jedes $j = 1, \dots, n$.

Satz 2.30. *Sei I ein Ideal in $k[x_1, \dots, x_n]$ und sei G eine Gröbnerbasis von I bezüglich einer Eliminationsordnung für $x_1, \dots, x_j$ ($1 \leqslant j \leqslant n$). Dann ist*

$$G_j = G \cap k[x_{j+1}, \dots, x_n]$$

eine Gröbnerbasis des j-ten Eliminationsideals (bezüglich der auf $k[x_{j+1}, \dots, x_n] \subset k[x_1, \dots, x_n]$ induzierten Monomordnung).

Beweis. Sei $f \in I_j$, $f \neq 0$. Dann wird das Leitmonom $\mathrm{LM}(f)$ von einem der Leitmonome $\mathrm{LM}(g)$, $g \in G$ geteilt. Es folgt $\mathrm{LM}(g) \in k[x_{j+1}, \dots, x_n]$ und, da wir eine Eliminationsordnung verwenden, daraus auch $g \in k[x_{j+1}, \dots, x_n]$. Also ist $g \in G_j$ und die Behauptung bewiesen. ∎

Eliminationsideale berechnet man in Macaulay2 mit dem Befehl `eliminate`.

```
i1 : R = QQ[x,y,z];
i2 : I = ideal(y-x^2,z-x^3);
o2 : Ideal of R

i3 : eliminate(I,{x})
             3    2
o3 = ideal(y  - z )
o3 : Ideal of R
```

(siehe Beispiel 1.23). Dazu berechnet Macaulay2 im Hintergrund eine Gröbnerbasis für I bezüglich einer geeigneten Eliminationsordnung. Es ist nicht nötig (aber möglich durch Wechsel des Rings), eine Eliminationsordnung explizit anzugeben.

2.5.4. Gleichungssysteme mit endlich vielen Lösungen. Es sei $I = \langle f_1, \dots, f_r \rangle$ ein Ideal in $k[x_1, \dots, x_n]$. Wir wollen wissen, ob die Varietät $\mathcal{V}(I)$ endlich ist und, falls ja, wollen wir diese endlich vielen Punkte ausrechnen. Im Prinzip kann man das durch Elimination erreichen. Fixiere die lexikographische Ordnung. Diese ist eine Eliminationsordnung für $x_1, \dots, x_j$, für jedes $j = 1, \dots, n$. Sei G eine Gröbnerbasis von I. Wie wir gesehen haben, gilt dann

$$I \cap k[x_j, \dots, x_n] = \langle G \cap k[x_j, \dots, x_n] \rangle \quad \text{für } j = 1, \dots, n.$$

Wenn $\mathcal{V}(I)$ endlich ist, dann auch die Projektion auf die letzten $n - j + 1$ Koordinaten. Deshalb muss G in diesem Fall für jedes $j = 1, \dots, n$ ein Polynom enthalten, in dem nur die Variablen $x_j, \dots, x_n$ vorkommen. (Und keine Variable darf ganz fehlen.) Insbesondere besteht G aus mindestens n Elementen. Genauer gilt: Ist $G = \{g_1, \dots, g_r\}$, dann können wir die Elemente von G so

umsortieren und skalieren, dass

$$g_j \in k[x_j, \ldots, x_n] \text{ und } \mathrm{LM}(g_j) = x_j^{m_j}$$

für $j = 1, \ldots, n$ und gewisse $m_1, \ldots, m_n \geqslant 1$ gilt. (Für die Behauptung über die Leitmonome muss man noch ein wenig arbeiten; siehe Übung 2.19). Mit anderen Worten, die Variablen sind in den ersten n Gleichungen 'dreiecksförmig' verteilt:

$$\begin{aligned} g_1(x_1, \ldots, x_j, x_{j+1}, \ldots, x_n) &= 0 \\ &\vdots \\ g_j(x_j, x_{j+1}, \ldots, x_n) &= 0 \\ &\vdots \\ g_n(x_n) &= 0. \end{aligned}$$

Im Prinzip können wir das Gleichungssystem damit durch Rückeinsetzung lösen, genauso wie in der linearen Algebra: Als erstes lösen wir die letzte Gleichung, in der nur die Variable x_n vorkommt. Danach setzen wir die endlich vielen Lösungen in die nächste Gleichung ein, in der dann nur noch x_{n-1} vorkommt, und so weiter. Am Schluss müssen wir noch alle so erhaltenen Lösungen darauf überprüfen, ob die verbleibenden Polynome $g_{n+1}, \ldots, g_r$ in ihnen verschwinden.

Dieser Algorithmus ist wieder nur eine Skizze und kann für die Praxis erheblich verbessert werden. Er bringt aber in jedem Fall gewisse Schwierigkeiten mit sich: Erstens ist es schon mit dem Lösen von Gleichungen in einer Variablen nicht so einfach, wie wir aus der Algebra wissen; solche Lösungen lassen sich eben nicht immer durch Wurzelziehen hinschreiben. Trotzdem kann man mit ihnen im Prinzip exakt rechnen (Stichwort: Algebraische Zahlen). Zweitens wächst die Zahl der Gleichungen in einer Variablen, die man durch Einsetzungen aller vorigen Lösungen erhält, im allgemeinen rasant (exponentiell), so dass es bei wachsender Zahl von Gleichungen und Variablen schnell unmöglich wird, das Verfahren praktisch durchzuführen.

Trotz dieser Einschränkungen haben wir damit in gewisser Weise die beste Annäherung an das Gaußsche Eliminationsverfahren für lineare Gleichungssysteme erreicht, die für nichtlineare Gleichungssysteme möglich ist. Ein einfaches Beispiel diskutieren wir in Übung 2.18.

Frage 2.31. Wie kann man entscheiden, ob $\mathcal{V}(I)$ endlich ist, ohne die Lösungen auszurechnen?

2.5.5. Implizitisierung. Gegeben $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$, betrachte den Morphismus

$$\varphi\colon \mathbb{A}^m \to \mathbb{A}^n, p \mapsto \big(f_1(p), \ldots, f_n(p)\big).$$

Der Zariski-Abschluss $Z = \overline{\varphi(\mathbb{A}^m)}$ des Bildes ist eine irreduzible k-Varietät in $\mathbb{A}^n$. Nach Kor. 1.43 wird Z durch das Ideal

$$\langle y_1 - f_1, \ldots, y_n - f_n \rangle \cap k[y_1, \ldots, y_n],$$

beschrieben, wobei der Durchschnitt im Polynomring $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$ gebildet wird. Durch Elimination können wir also Gleichungen für die parametrisierte Varietät Z berechnen.

2.5.6. Durchschnitt von Idealen. Seien $I = \langle f_1, \ldots, f_r \rangle$ und $J = \langle g_1, \ldots, g_s \rangle$ Ideale in $k[x_1, \ldots, x_n]$. Für die Ideale $I + J$ und IJ kann man sofort Erzeuger hinschreiben, aber für $I \cap J$ ist das deutlich schwieriger. Mit Hilfe von Gröbnerbasen kann man wie folgt vorgehen:

Satz 2.32. *Seien I und J Ideale wie oben und seien $\widetilde{I}$ bzw. $\widetilde{J}$ die von I bzw. J erzeugten Ideale im Polynomring $k[t, x_1, \dots, x_n]$ mit einer zusätzlichen Variablen t. Dann ist*

$$I \cap J = \left(t\widetilde{I} + (1-t)\widetilde{J}\right) \cap k[x_1, \dots, x_n].$$

Beweis. Für $f \in I \cap J$ liegt $f = tf + (1-t)f$ im Ideal auf der rechten Seite. Umgekehrt sei f im rechten Ideal gelegen. Es gibt also Polynome $p_i, q_j \in k[t, x_1, \dots, x_n]$ ($i = 1, \dots, r$, $j = 1, \dots, s$) mit

$$f(x) = t \sum_{i=1}^{r} p_i(t,x) f_i(x) + (1-t) \sum_{j=1}^{s} q_j(t,x) g_j(x).$$

Substitution von $t = 1$ bzw. $t = 0$ zeigt $f \in I$ bzw. $f \in J$. ∎

Das Problem der Berechnung von $I \cap J$ ist damit auf das Eliminationsproblem zurückgeführt, das wir schon gelöst haben. Explizit ist

$$t\widetilde{I} + (1-t)\widetilde{J} = \langle tf_1, \dots, tf_r, (1-t)g_1, \dots, (1-t)g_s \rangle$$

Man bekommt also eine Gröbnerbasis des Durchschnitts $I \cap J$, indem man eine Gröbnerbasis des Ideals $t\widetilde{I} + (1-t)\widetilde{J}$ bezüglich einer Eliminationsordnung für t bestimmt und alle Polynome daraus weglässt, in denen die Variable t vorkommt.

In Macaulay2 gibt es natürlich einen Befehl, der den Durchschnitt $I \cap J$ direkt berechnet, nämlich `intersect(I,J)`. Es können auch mehr als zwei Ideale angegeben werden.

2.5.7. Radikale. Im Hinblick auf den starken Nullstellensatz und seine Anwendungen wäre es ausgesprochen nützlich, wenn wir das Radikal eines Ideals mit Hilfe von Gröbnerbasen berechnen könnten. Tatsächlich gibt es entsprechende Algorithmen, aber ganz einfach ist die Sache nicht und wir werden hier nicht darauf eingehen (siehe zum Beispiel [Greuel-Pfister, Kap. 4]).

Sehr viel einfacher ist es allerdings zu testen, ob ein einzelnes Polynom f im Radikal eines gegebenen Ideals enthalten ist. Sei $I \subset k[x_1, \dots, x_n]$ ein Ideal und $f \in k[x_1, \dots, x_n]$. Genau dann ist f in $\sqrt{I}$ enthalten, wenn

$$1 \in \langle I \rangle + \langle 1 - fy \rangle \subset k[x_1, \dots, x_n, y]$$

gilt. Das ist im wesentlichen der 'Trick von Rabinowitsch' im Beweis des starken Nullstellensatzes; siehe Übung 2.16. Das Problem ist damit auf einen Inklusionstest zurückgeführt.

Das Radikal eines Ideals I wird in Macaulay2 mit dem Befehl `radical(I)` berechnet. Bei komplexeren Problemen kann das allerdings ziemlich lange dauern oder auch gar nicht in akzeptabler Zeit terminieren. Wenn man nur wissen will, ob ein bestimmtes Polynom im Radikal liegt, kann es sich daher lohnen, den gerade beschriebenen Trick anzuwenden.

2.5.8. Urbild eines Ideals. Es sei

$$\alpha\colon k[y_1, \dots, y_n] \to k[x_1, \dots, x_m]$$

ein Homomorphismus zwischen zwei Polynomringen und sei I ein Ideal in $k[x_1,\dots,x_m]$. Wir wollen das Urbildideal $\alpha^{-1}(I)$ berechnen.

Der Homomorphismus α ist durch die Bilder der Variablen $y_1,\dots,y_n$ eindeutig festgelegt. Es gibt also Polynome $f_1,\dots,f_n \in k[x_1,\dots,x_m]$ mit $\alpha(y_j) = f_j$ für $j = 1,\dots,n$.

Lemma 2.33. *Es sei* $J = \langle y_1 - f_1,\dots,y_n - f_n\rangle \subset k[x_1,\dots,x_m,y_1,\dots,y_n]$. *Dann gilt*

$$\alpha^{-1}(I) = (\langle I\rangle + J) \cap k[y_1,\dots,y_n],$$

wobei $\langle I\rangle$ *das von* I *in* $k[x_1,\dots,x_m,y_1,\dots,y_n]$ *erzeugte Ideal bezeichnet.*

Beweis. Wir schreiben kurz $x = (x_1,\dots,x_m)$ und $y = (y_1,\dots,y_n)$. Betrachte den Homomorphismus von k-Algebren

$$\beta\colon k[x,y] \to k[x],\ \beta(x_i) = x_i, \beta(y_j) = f_j.$$

Die Behauptung ergibt sich aus den folgenden drei Aussagen:

(i) Es gilt $\alpha^{-1}(I) = \beta^{-1}(I) \cap k[y]$, denn α ist die Einschränkung von β auf $k[y]$.
(ii) Es gilt $\beta^{-1}(I) = \langle I\rangle + \langle\ker(\beta)\rangle$, denn die Einschränkung von β auf $k[x]$ ist die Identität.
(iii) Es gilt $\ker(\beta) = J$ (siehe Übung 2.17). ∎

Das Lemma reduziert die Berechnung des Urbildideals damit auf ein Eliminationsproblem. Das Ideal $\langle I\rangle + J$ kennen wir übrigens schon: Es definiert gerade den Graph des Morphismus $\varphi = (f_1,\dots,f_n)\colon \mathcal{V}(I) \to \mathbb{A}^n$, was wir in Kor. 1.43 benutzt haben.

2.5.9. Kern eines Homomorphismus. Ein allgemeineres Problem als das vorige ist die Berechnung des Kerns einen beliebigen Homomorphismus $\rho\colon B \to A$ von endlich erzeugten k-Algebren.

Dazu müssen die Algebren A und B durch Erzeuger und Relationen gegeben sein. Das heißt, wir fixieren Erzeuger $a_1,\dots,a_m$ von A und $b_1,\dots,b_n$ von B und betrachten die Epimorphismen

$$\alpha\colon \begin{cases} k[x_1,\dots,x_m] & \to & A \\ x_i & \mapsto & a_i \end{cases} \quad\text{und}\quad \beta\colon \begin{cases} k[y_1,\dots,y_n] & \to & B \\ y_i & \mapsto & b_i \end{cases}.$$

Setze $I = \ker(\alpha)$ und $J = \ker(\beta)$. Der Homomorphismus $\rho\colon B \to A$ ist durch die Bilder von $b_1,\dots,b_m$ eindeutig bestimmt. Es gibt also Polynome $f_j \in k[x_1,\dots,x_m]$ mit $\rho(b_j) = \alpha(f_j)$ für $j = 1,\dots,n$. Für alle $g \in J$ muss dabei $g(f_1,\dots,f_n)$ in I liegen (Homomorphiesatz). Definiere

$$\widetilde{\rho}\colon \begin{cases} k[y_1,\dots,y_n] & \to & k[x_1,\dots,x_m] \\ y_j & \mapsto & f_j \end{cases}.$$

Nach Konstruktion haben wir dann ein kommutierendes Diagramm

$$\begin{array}{ccc} k[y_1,\dots,y_n] & \xrightarrow{\widetilde{\rho}} & k[x_1,\dots,x_m] \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\alpha} \\ B & \xrightarrow{\rho} & A. \end{array}$$

Das gesuchte Ideal ist also $\rho^{-1}(0) = \beta(\widetilde{\rho}^{-1}(I))$. Das Ideal $\widetilde{\rho}^{-1}(I)$ können wir dabei wie oben berechnen. Wegen $\beta(\widetilde{\rho}^{-1}(I)) = \widetilde{\rho}^{-1}(I)/J$ müssen wir dann nur noch die Erzeuger dieses Ideals modulo J reduzieren und erhalten das gesuchte Ideal.

Ist $\varphi\colon V \to W$ ein Morphismus von affinen k-Varietäten und $\varphi^{\#}\colon k[W] \to k[V]$ der zugehörige Homomorphismus zwischen den Koordinatenringen, dann definiert $\ker\varphi^{\#}$ genau den Zariski-Abschluss des Bildes $\varphi(V)$ (siehe Übung 1.41).

Übungen

Übung 2.16. Sei $I \subset k[x_1, \ldots, x_n]$ ein Ideal und $f \in k[x_1, \ldots, x_n]$. Zeigen Sie:

$$f \in \sqrt{I} \qquad \Longleftrightarrow \qquad 1 \in \langle I \rangle + \langle 1 - fy \rangle \subset k[x_1, \ldots, x_n, y].$$

Übung 2.17. Die folgende Aussage wurde im Text benutzt. Es sei R ein Ring, seien $a_1, \ldots, a_n \in R$ und

$$\alpha\colon R[x_1, \ldots, x_n],\ \alpha(x_i) = a_i \text{ für } i = 1, \ldots, n$$

der *Auswertungshomomorphismus*. Dann gilt

$$\ker(\alpha) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

(*Vorschlag:* Reduzieren Sie auf den Fall $a_1 = \cdots = a_n = 0$.)

Übung 2.18. Gegeben seien die drei Polynome

$$f_1 = x^2 + y^2 + z^2 - 1, \quad f_2 = x^2 - y + z^2, \quad f_3 = x - z$$

in $\mathbb{Q}[x, y, z]$. Zeigen Sie, dass $\mathcal{V}(f_1, f_2, f_3)$ endlich ist und bestimmen Sie alle komplexen Punkte dieser Varietät mit dem Verfahren aus Abschnitt 2.5.4.

Übung 2.19. Die folgende Aussage haben wir in Abschnitt 2.5.4 benutzt: Es sei I ein Ideal in $k[x_1, \ldots, x_n]$ und die Varietät $\mathcal{V}(I)$ sei eine endliche Menge von Punkten. Sei G eine Gröbnerbasis von I bezüglich lex. Zeigen Sie, dass G für jedes $j = 1, \ldots, n$ ein Element g_j mit $\mathrm{LM}(g_j) = x^{m_j}$ für ein $m_j \geqslant 1$ enthält. (*Vorschlag:* Benutzen Sie Übung 1.35).

Übung 2.20. Es seien $f, g \in k[x, y]$, $I = \langle f, g \rangle$ und G eine Gröbnerbasis von I bezüglich lex. Sei $r \in k[y]$ die Resultante von f und g bezüglich y. Zeigen Sie, dass jeder Faktor von r ein Element von G teilt.

Übung 2.21. Gegeben ganze Zahlen a, b, c mit

$$a + b + c = 3, \quad a^2 + b^2 + c^2 = 5, \quad a^3 + b^3 + c^3 = 7.$$

(a) Zeigen Sie $a^4 + b^4 + c^4 = 9$ und $a^5 + b^5 + c^5 \neq 11$.
(b) Bestimmen Sie $a^5 + b^5 + c^5$ und $a^6 + b^6 + c^6$.

Daniel Plaumann
Technische Universität Dortmund
Sommersemester 2016
Fassung vom 17. Juli 2016

3. PROJEKTIVE GEOMETRIE

In der projektiven Geometrie wird der affine Raum durch Hinzufügen von Punkten, die man sich als unendlich ferne Schnittpunkte paralleler Geraden vorstellen kann, zum projektiven Raum erweitert. Viele geometrische Aussagen werden dadurch einfacher, weil es weniger Ausnahmefälle gibt. In der Algebra entspricht das dem Übergang von beliebigen Polynomgleichungen zu homogenen Gleichungen. Auch das macht für die algebraische Theorie vieles einfacher. Zunächst führen wir projektive Räume ein und versuchen, ein geometrisches Bild von ihnen zu entwerfen. Danach entwickeln wir die Theorie der homogenen Polynomgleichungen.

3.1. Projektive Räume

Es sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Der **projektive Raum über** V ist die Menge aller 1-dimensionalen Unterräume von V und wird mit $\mathbb{P}V$ bezeichnet. Die Elemente von $\mathbb{P}V$ heißen die **Punkte** von $\mathbb{P}V$. Die Punkte des projektiven Raums sind also die Ursprungsgeraden des Vektorraums. Die **(projektive) Dimension** von $\mathbb{P}V$ ist definiert als

$$\dim \mathbb{P}V = \dim(V) - 1.$$

Der projektive Raum $\mathbb{P}K^{n+1}$ hat also die Dimension n und wird kurz mit $\mathbb{P}^n_K$ bezeichnet oder, bei fixiertem K, nur mit $\mathbb{P}^n$. Man nennt $\mathbb{P}^n$ auch einfach *den* n**-dimensionalen projektiven Raum über** K. Wie erwartet heißt $\mathbb{P}^1$ die projektive Gerade, $\mathbb{P}^2$ die projektive Ebene über K. Der 0-dimensionale projektive Raum $\mathbb{P}^0$ besteht nur aus einem einzigen Element und wird daher als Punkt aufgefasst. Per Definition ist außerdem $\mathbb{P}\{0\} = \varnothing$ und $\dim \mathbb{P}\{0\} = -1$.

Diese Definition projektiver Räume ist technisch einfach aber vollkommen unanschaulich. Von unendlich fernen Punkten ist nichts zu sehen. Wir müssen also die Geometrie erst noch entwickeln. Zunächt noch etwas lineare Algebra: Ist V ein Vektorraum und $U \subset V$ ein Unterraum, so ist $\mathbb{P}U \subset \mathbb{P}V$ ein **projektiver Unterrraum** von $\mathbb{P}V$. Projektive Unterräume der Dimension 1 heißen **Geraden**, der Dimension 2 **Ebenen**, der Dimension $\dim \mathbb{P}V - 1$ **Hyperebenen**.

Sind U_1 und U_2 zwei Unterräume von V und ist $L_1 = \mathbb{P}U_1$, $L_2 = \mathbb{P}U_2$, so definiere

$$\overline{L_1 L_2} = \mathbb{P}(U_1 + U_2),$$

der **Verbindungsraum** von L_1 und L_2. Außerdem gilt offenbar

$$L_1 \cap L_2 = \mathbb{P}(U_1 \cap U_2).$$

Aus der Definition der projektiven Dimension und der Dimensionsformel für lineare Unterräume erhält man sofort die **projektive Dimensionsformel**

$$\dim \overline{L_1 L_2} = \dim L_1 + \dim L_2 - \dim(L_1 \cap L_2).$$

Beispiel 3.1. Zwei verschiedene Geraden in $\mathbb{P}^2$ schneiden sich in genau einem Punkt (Übung!). Es gibt also keine 'parallelen' Geraden in $\mathbb{P}^2$. Zwei Geraden L_1 und L_2 in $\mathbb{P}^3$ heißen **windschief**, falls $L_1 \cap L_2 = \varnothing$. Der Verbindungsraum hat dann die Dimension $\dim \overline{L_1 L_2} = 1+1-(-1) = 3$ (denn $\dim \varnothing = -1$!). Also spannen L_1 und L_2 den ganzen Raum auf. Wenn L_1 und L_2 einen Schnittpunkt haben, dann liegen sie in einer gemeinsamen Ebene und es gilt $\dim \overline{L_1 L_2} = 1 + 1 - 0 = 2$.

Ein Punkt von $\mathbb{P}V$, also ein 1-dimensionaler Unterraum von V, wird von einem Vektor $v \neq 0$ aufgespannt. Wir schreiben kurz $[v] = K \cdot v$. Natürlich gilt dann

$$[v] = [\lambda v] \text{ für alle } \lambda \in K^\times.$$

In $\mathbb{P}^n_K$ schreiben wir $[a_0, \ldots, a_n]$ für den Punkt $K \cdot (a_0, \ldots, a_n)$. Es gilt dann

$$[\lambda a_0, \ldots, \lambda a_n] = [a_0, \ldots, a_n] \text{ für alle } \lambda \in K^\times.$$

Ist $p = [a_0, \ldots, a_n]$, so heißen die Zahlen $a_0, \ldots, a_n$, die nur bis auf Skalierung durch p bestimmt sind, die **homogenen Koordinaten** von p. Die homogenen Koordinaten ändern sich also durch Skalierung, aber ob eine Koordinate Null ist oder nicht, ändert sich dabei natürlich nicht. Weil für jeden Punkt in $\mathbb{P}^n$ mindestens eine homogene Koordinate ungleich 0 ist, ist jeder Punkt in einer der Mengen

$$D_i = \left\{ [a_0, \ldots, a_n] \in \mathbb{P}^n : a_i \neq 0 \right\} \qquad (i = 1, \ldots, n)$$

enthalten. In D_i können wir die Koordinate $a_i \neq 0$ durch Division zu 1 machen, d.h. es gilt

$$[a_0, \ldots, a_n] = \left[\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i} \right], \quad \text{falls } a_i \neq 0.$$

Zu jedem $p \in D_i$ existiert also ein eindeutiger Vektor $(a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in K^n$ mit

$$p = [a_0, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n].$$

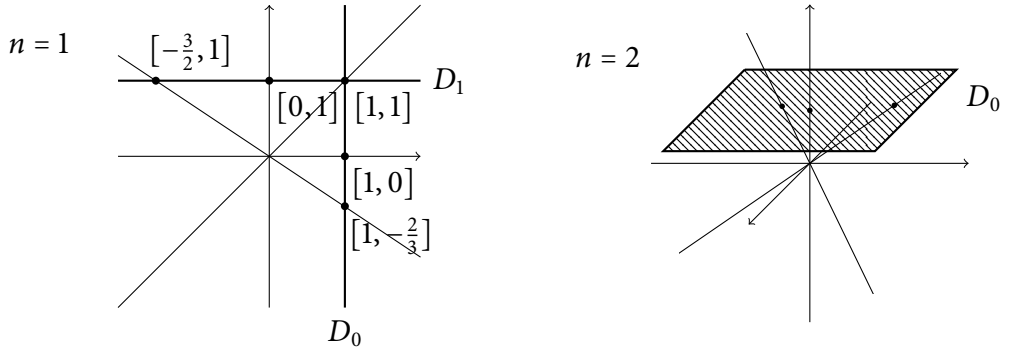
Da der i-te Eintrag dann also immer 1 ist, ist die Abbildung

$$\rho_i : \begin{cases} \mathbb{A}^n & \to & D_i \\ (a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) & \mapsto & [a_0, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n] \end{cases}$$

eine Bijektion zwischen dem affinen Raum $\mathbb{A}^n$ und der Teilmenge D_i. Wir halten fest:

> Der projektive Raum $\mathbb{P}^n$ wird von $n+1$ Kopien des affinen Raums $\mathbb{A}^n$ überdeckt.

Diese Überdeckung kann man sich in den Fällen $n = 1, 2$ folgendermaßen veranschaulichen:



Die Ursprungsgeraden in K^2 werden mit ihren Schnittpunkten mit der affinen Geraden $x_0 = 1$ bzw. $x_1 = 1$ identifiziert. Entsprechend für $n = 2$, wo die Ursprungsgeraden mit ihren Schnittpunkten mit einer affinen Ebene identifiziert werden. Für $n = 1$ gilt

$$D_1 = \{[x,1]: x \in K\} \cong \mathbb{A}^1.$$

Das Komplement $\mathbb{P}^1 \setminus D_1$ besteht nur aus einem einzigen Punkt, nämlich $[1,0]$. Im Allgemeinen ist das Komplement von D_i eine Hyperebene in $\mathbb{P}^n$, und zwar

$$H_i = \mathbb{P}^n \setminus D_i = \{[a_0,\dots,a_{i-1},0,a_{i+1},\dots,a_n] \in \mathbb{P}^n\} = \mathbb{P}\{a \in K^{n+1}: a_i = 0\} \cong \mathbb{P}K^n = \mathbb{P}^{n-1}.$$

Im Bezug auf den affinen Raum $D_i \cong \mathbb{A}^n$ heißt H_i die **Hyperebene im Unendlichen**. Im Bild oben entspricht H_0 also der Menge aller Ursprungsgeraden, die die Ebene $\{x_0 = 1\}$ in K^3 nicht schneiden, weil sie in der parallelen Ebene $\{x_0 = 0\}$ liegen. Geraden in der Ebene D_0 entstehen als Schnitt von D_0 mit 2-dimensionalen Unterräumen von K^3. Genau dann sind die beiden Geraden parallel, wenn sich die beiden 2-dimensionalen Unterräume in einem 1-dimensionalen Unterraum in der Ebene $\{x_0 = 0\}$ schneiden. Der Schnittpunkt der beiden parallelen Geraden liegt nicht in D_0, sondern 'im Unendlichen', auf der projektiven Geraden H_0.

Warnung. Diese Bilder sind zur Veranschaulichung hilfreich, sie können aber auch verwirren. Die Terminologie ist nicht zufällig gewählt: Einen Punkt im projektiven Raum soll man sich auch als Punkt vorstellen, nicht als Gerade in einem affinen Raum. Die projektive Gerade ist eine Gerade, die Ebene eine Ebene, der Raum ein Raum. So wie die geometrischen Bilder immer reelle (und nicht komplexe) Bilder sind, so sind sie auch immer affin, nicht projektiv. In unserer Vorstellung ist also z.B. $\mathbb{P}^2_{\mathbb{C}}$ eine Ebene, nur mit gewissen idealisierten Eigenschaften.

Es sei V ein K-Vektorraum der Dimension $n+1$. Eine Menge $\{p_0,\dots,p_r\}$ von Punkten in $\mathbb{P}V$ mit $r \leqslant n$ heißt **projektiv unabhängig**, wenn

$$\dim(\overline{p_0,\dots,p_r}) = r$$

gilt. Wenn wir Vektoren $v_0,\dots,v_r \in V$ wählen mit $p_i = [v_i]$, dann sind $p_0,\dots,p_r$ offenbar genau dann projektiv unabhängig, wenn $v_0,\dots,v_r$ linear unabhängig sind. Das ist also nichts Neues. Ein System von $n+1$ projektiv unabhängigen Punkten in $\mathbb{P}V$ heißt ein **homogenes Koordinatensystem**. Allgemeiner sagt man, die Punkte $p_0,\dots,p_r$ (mit r nicht unbedingt kleiner oder gleich n) seien **(linear) in allgemeiner Lage**, wenn jede Wahl von höchstens $n+1$ Punkten aus $\{p_0,\dots,p_r\}$ projektiv unabhängig ist.

Schließlich überlegen wir uns noch, wie es mit linearen Abbildungen im Projektiven aussieht. Es seien V und W zwei K-Vektorräume und $\Phi: V \to W$ eine lineare Abbildung. Ist $v \in V$ mit $\Phi(v) \neq 0$, dann können wir dem Punkt $[v] \in \mathbb{P}V$ den Bildpunkt $[\Phi(v)] \in \mathbb{P}W$ zuordnen. Ist dagegen $\Phi(v) = 0$, dann können wir damit nichts anfangen, denn $\Phi(v)$ erzeugt dann ja keinen 1-dimensionalen Unterraum von W. Wir erhalten also eine Abbildung

$$[\Phi]: \begin{cases} \mathbb{P}V \setminus (\mathbb{P}\ker\Phi) & \to & \mathbb{P}W \\ [v] & \mapsto & [\Phi(v)] \end{cases}.$$

Zwei Typen von solchen Abbildungen sind besonders wichtig, nämlich Projektivitäten und Projektionen, die wir nun nach einander diskutieren.

Wenn $\Phi\colon V \to V$ ein Isomorphismus (=lineare Bijektion) ist, also $\Phi \in \mathrm{GL}(V)$, dann ist $[\Phi]\colon \mathbb{P}V \to \mathbb{P}V$ ebenfalls bijektiv und heißt die durch Φ bestimmte **Projektivität** von $\mathbb{P}V$ auf sich. Die Projektivitäten bilden unter Komposition eine Gruppe, die **projektive lineare Gruppe**, die wir mit $\mathrm{PGL}(V)$ bezeichnen. Wir können ziemlich leicht sagen, wie diese Gruppe aussieht: Per Definition haben wir einen surjektiven Gruppenhomomorphismus

$$\mathrm{GL}(V) \to \mathrm{PGL}(V), \Phi \mapsto [\Phi].$$

Da $[\lambda\Phi(v)] = [\Phi(v)]$ für alle $\lambda \in K^\times$ und alle $[v] \in \mathbb{P}V$ gilt, können wir Φ durch $\lambda\Phi$ ersetzen, ohne dass sich die Projektivität ändert. Mit anderen Worten, der Kern des obigen Gruppenhomomophismus ist der Normalteiler $K^\times \mathrm{id}_V = \{\lambda \cdot \mathrm{id}_V \colon \lambda \in K^\times\}$, bestehend aus den Vielfachen der Identität. Nach dem Isomorphiesatz gilt also

$$\mathrm{PGL}(V) \cong \mathrm{GL}(V)/(K^\times \mathrm{id}_V).$$

In homogenen Koordinaten sieht das so aus: Ist $V = K^{n+1}$, dann induziert jeder Koordinatenwechsel, gegeben durch eine invertierbare Matrix $P \in \mathrm{GL}_{n+1}(K)$, $v \mapsto Pv$ eine Projektivität (einen projektiven Koordinatenwechsel)

$$\mathbb{P}^n \to \mathbb{P}^n, [v] \mapsto [Pv].$$

Dabei ergeben P und λP für $\lambda \in K^\times$ denselben projektiven Koordinatenwechsel. Die Gruppe $\mathrm{PGL}(K^{n+1})$ wird mit $\mathrm{PGL}_{n+1}(K)$ bezeichnet[1]. Es gilt

$$\mathrm{PGL}_{n+1}(K) \cong \mathrm{GL}_{n+1}(K)/(K^\times I_{n+1}).$$

Die Projektivitäten von $\mathbb{P}^n$ auf sich sind also durch Matrizen beschrieben, die aber, wie die homogenenen Koordinaten der Punkte, nur bis auf Skalierung wohlbestimmt sind.

Satz 3.2. *Es seien $(p_0, \dots, p_{n+1})$ und $(q_0, \dots, q_{n+1})$ zwei Tupel von $n+2$ Punkten in allgemeiner Lage in $\mathbb{P}^n$. Dann gibt es genau eine Projektivität $[P]$ von $\mathbb{P}^n$ mit*

$$[P]p_i = q_i \text{ für } i = 0, \dots, n+1.$$

Dass man je zwei Tupel von $n+1$ projektiv unabhängigen Punkten in $\mathbb{P}^n$ durch eine Projektivität aufeinander abbilden kann, ist klar, weil es einfach einem Basiswechsel in K^{n+1} entspricht. Die Aussage des Satzes ist gerade, dass man im Projektiven einen Freiheitsgrad gewinnt.

Beweis. Es seien $v_i \in K^{n+1}$ Vektoren mit $p_i = [v_i]$ für $i = 0, \dots, n+1$. Da $p_0, \dots, p_n$ in allgemeiner Lage sind, sind $v_0, \dots, v_n$ linear unabhängig, also eine Basis. Es gibt also $a_0, \dots, a_n \in K$ mit

$$v_{n+1} = a_0 v_0 + \cdots + a_n v_n.$$

Dabei sind die Skalare $a_0, \dots, a_n$ alle ungleich 0, da nach Voraussetzung jede echte Teilmenge von $\{v_0, \dots, v_{n+1}\}$ linear unabhängig ist. Wir können deshalb v_i durch $a_i v_i$ ersetzen, für $i = 0, \dots, n$. Dann gilt immer noch $p_i = [v_i]$ und außerdem

$$v_{n+1} = v_0 + \cdots + v_n.$$

[1]Da dies die Gruppe der Projektivitäten von $\mathbb{P}^n$ auf sich ist, wäre es konsequenter, sie mit $\mathrm{PGL}_n(K)$ zu bezeichnen, aber dies wäre entgegen der allgemein üblichen Konvention.

Sei nun $P_1 \in \mathrm{GL}_{n+1}(K)$ die Matrix mit Spalten $v_0, \dots, v_n$. Dann gilt

$$[P_1 e_i] = [v_i] = p_i \quad \text{für } i = 0, \dots, n \quad \text{und} \quad [P_1(e_0 + \cdots + e_n)] = [v_0 + \cdots + v_n] = p_{n+1}.$$

Genauso gibt es $P_2 \in \mathrm{GL}_{n+1}(K)$ mit

$$[P_2 e_i] = q_i \quad \text{für } i = 0, \dots, n \quad \text{und} \quad [P_2(e_0 + \cdots + e_n)] = q_{n+1}.$$

Also ist $P = P_2 P_1^{-1}$ die gesuchte Matrix. Die Konstruktion zeigt außerdem, dass P_1 und P_2 bis auf Skalierung eindeutig sind, somit $[P]$ eindeutig ist als Element von $\mathrm{PGL}_{n+1}(K)$. ∎

Auf dem ganzen projektiven Raum betrachtet sind Projektivitäten ziemlich einfach, weil sie linearen Abbildungen entsprechen. Was aber geschieht auf den affinen Teilmengen? Es sei

$$D_0 = \{[1, x_1, \dots, x_n] \colon (x_1, \dots, x_n) \in \mathbb{A}^n\} \cong \mathbb{A}^n$$

wie oben. Sei $[A] \in \mathrm{PGL}_{n+1}(K)$ eine invertierbare Matrix mit Zeilenvektoren $a_0, \dots, a_n$ und sei $[p] = [1, x_1, \dots, x_n] \in D_0$. Dann gilt also

$$[Ap] = [a_0 \cdot p, a_1 \cdot p, \dots, a_n \cdot p],$$

wobei wir p jetzt als Spaltenvektor auffassen. Wenn wir A durch ein Vielfaches λA, $\lambda \neq 0$, ersetzen, dann ändert sich $[Ap]$ nicht, der Ausdruck ist also wohldefiniert. Wenn $a_0 \cdot p \neq 0$ ist, dann können wir durch diesen Eintrag teilen und landen wieder in D_0, also

$$[Ap] = \left[1, \frac{a_1 \cdot p}{a_0 \cdot p}, \dots, \frac{a_n \cdot p}{a_0 \cdot p}\right].$$

Jeder Ausdruck $a_i \cdot p$ ist dabei ein Polynom ℓ_i vom Grad 1 in $x = (x_1, \dots, x_n)$, nämlich

$$\ell_i(x) = a_i \cdot (1, x) = a_{i,0} + \sum_{j=1}^{n} a_{i,j} x_j.$$

Die Einschränkung von $[A]$ auf D_0 können wir also als Funktion

$$\varphi \colon \mathbb{A}^n \to \mathbb{A}^n, \ (x_1, \dots, x_n) \mapsto \left(\frac{\ell_1(x)}{\ell_0(x)}, \dots, \frac{\ell_n(x)}{\ell_0(x)}\right)$$

auffassen, eine sogenannte **gebrochen-lineare Transformation**. Wie bei rationalen Funktionen üblich, ist sie nicht auf ganz $\mathbb{A}^n$ definiert, sondern nur in den Punkten $x \in \mathbb{A}^n$, wo der Nenner $\ell_0(x)$ ungleich 0 ist. Da A invertierbar ist, ist ℓ_0 nicht die Nullfunktion und φ ist definiert auf dem Komplement der affinen Hyperebene $\{x \in \mathbb{A}^n \colon \ell_0(x) = 0\}$. Dieser Wechsel zwischen projektiver und affiner Sichtweise kommt in der projektiven Geometrie immer wieder vor.

Wir diskutieren den Fall $n = 1$ noch etwas ausführlicher. Es sei $\mathbb{P}^1 \setminus D_1 = \{\infty\}$ mit $\infty = [1, 0]$ wie oben und sei

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}_2(K).$$

In homogenen Koordinaten definiert A die Abbildung

$$[A] \colon \mathbb{P}^1 \to \mathbb{P}^1, [x_0, x_1] \mapsto [ax_0 + bx_1, cx_0 + dx_1].$$

Die Einschränkung von $[A]$ auf D_1 ist die gebrochen-lineare Transformation

$$\varphi\colon \mathbb{A}^1 \to \mathbb{A}^1, x \mapsto \frac{ax+b}{cx+d},$$

die entsteht, indem wir $x_1 = 1$ setzen und durch den zweiten Eintrag teilen. Solche gebrochen-linearen Transformationen in einer Variablen werden (vor allem in der komplexen Analysis) auch **Möbius-Transformationen**[2] genannt. Obwohl wir auf D_1 eingeschränkt haben, sehen wir immer noch, was die Funktion φ auf der ganzen projektiven Geraden tut: Denn φ ist undefiniert, wo der Nenner $cx + d$ verschwindet. Wenn $c \neq 0$ ist, dann ist das der Punkt $x = -d/c$. Dieser wird dann von $[A]$ gerade auf $\infty = [1, 0]$ abgebildet, denn es gilt

$$A[-d/c, 1] = A[-d, c] = [-ad + bc, 0] = [1, 0] = \infty.$$

Ist $c = 0$, so ist φ die Polynomfunktion $\varphi(x) = (a/d)x + (b/d)$ und bildet ∞ auf ∞ ab. Die Aussage von Satz 3.2 wird zu:

Korollar 3.3. *Es seien p, q, r drei verschiedene Punkte in $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. Dann gibt es genau eine Möbius-Transformation $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ mit*

$$\varphi(0) = p, \quad \varphi(1) = q, \quad \varphi(\infty) = r. \qquad \blacksquare$$

Der andere ganz wichtige Typ von linearen Abbildungen in der projektiven Geometrie, neben den Projektivitäten, sind die Projektionen. Es sei

$$\pi\colon \begin{cases} K^{n+1} & \to & K^n \\ (a_0, a_1, \ldots, a_n) & \mapsto & (a_1, \ldots, a_n) \end{cases}$$

die lineare Projektion auf die letzten n Koordinaten. Der Kern von π ist die Gerade $K \cdot e_0$, die dem Punkt $p = [1, 0, \ldots, 0] \in \mathbb{P}^n$ entspricht. Wie oben im allgemeinen beschrieben, induziert π also eine Abbildung

$$\pi_p\colon \mathbb{P}^n \setminus \{p\} \to \mathbb{P}^{n-1},\ [a_0, a_1, \ldots, a_n] \mapsto [a_1, \ldots, a_n],$$

genannt die **Projektion mit Zentrum** p. Damit ist die folgende geometrische Sichtweise verbunden: Wir können $\mathbb{P}^{n-1}$ als Teilraum von $\mathbb{P}^n$ auffassen, indem wir $\mathbb{P}^{n-1}$ mit der Hyperebene

$$H = \{[0, a_1, \ldots, a_n]\colon [a_1, \ldots, a_n] \in \mathbb{P}^{n-1}\} \subset \mathbb{P}^n$$

identifizieren. Dann entspricht π_p der Abbildung

$$\pi_p\colon \mathbb{P}^n \setminus \{p\} \to H, [a_0, a_1, \ldots, a_n] \mapsto [0, a_1, \ldots, a_n],$$

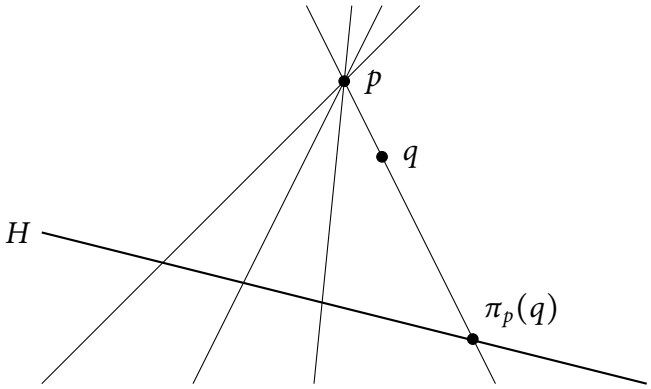
die die erste Koordinate durch 0 ersetzt.[3] Diese Projektion können wir geometrisch folgendermaßen verstehen: Sei $q \in \mathbb{P}^n$, $q \neq p$. Dann gilt

$$\pi_p(q) = \overline{pq} \cap H.$$

In Worten: Man projiziert q vom Zentrum p auf die Hyperebene H, indem man die Verbindungsgerade von p und q mit H schneidet.

[2] August Ferdinand Möbius (1790–1868), deutscher Mathematiker und Astronom

[3] Streng genommen handelt es sich natürlich nicht um dieselbe Abbildung, da das Ziel einmal $\mathbb{P}^{n-1}$ und einmal $H \subset \mathbb{P}^n$ ist. Je nach Kontext wird aber beides als Projektion mit Zentrum p bezeichnet.



Um das einzusehen, schreibe $p = [1, 0, \ldots, 0]$ wie gehabt und $q = [a_0, \ldots, a_n]$, dann gilt

$$\overline{pq} = \{[\lambda p + \mu q] = [\lambda + \mu a_0, \mu a_1, \ldots, \mu a_n] : \lambda, \mu \in K \text{ nicht beide } 0\}$$

Der Schnittpunkt $\overline{pq} \cap H$ entspricht also $[\lambda, \mu] \in \mathbb{P}^1$ mit $\lambda + \mu a_0 = 0$. Falls $a_0 = 0$, dann also $q \in H$ und $\lambda = 0$, also $\overline{pq} \cap H = \{[0, \mu a_1, \ldots, \mu a_n]\} = \{q\}$, so dass $\pi_p(q) = q$. Falls $a_0 \neq 0$, dann folgt $\mu = -\lambda/a_0$, so dass $\overline{pq} \cap H$ der Punkt $[0, (-\lambda/a_0)a_1, \ldots, (-\lambda/a_0)a_n] = [0, a_1, \ldots, a_n] = q$ ist.

Diese Sichtweise erklärt anschaulich, warum die Projektion in ihrem Zentrum p nicht definiert sein kann, denn p selbst bestimmt keine Verbindungsgerade mit p.

Wenn $p \in \mathbb{P}^n$ beliebig ist, dann bezeichnet π_p immer die Projektion mit Zentrum p auf das orthogonale Komplement, also auf die Hyperebene $H = \{q \in \mathbb{P}^n : \langle p, q \rangle = 0\}$, wobei $\langle -, - \rangle$ das Standardskalarprodukt auf K^{n+1} bezeichnet. Durch einen orthogonalen Koordinatenwechsel kann man immer $p = [1, 0 \ldots, 0]$ und H wie oben erreichen.

Übungen

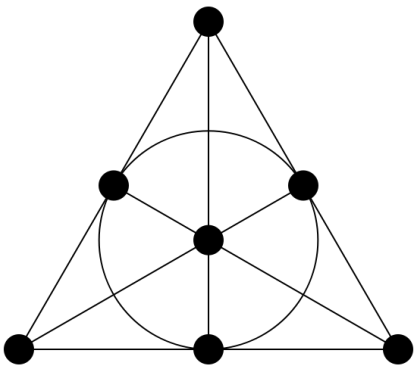
Übung 3.1. Es sei V ein K-Vektorraum der Dimension $n+1$. Zeigen Sie, dass jeder m-dimensionale projektive Unterraum von $\mathbb{P}V$ ein Durchschnitt von $n - m$ projektiven Hyperebenen ist.

Übung 3.2. Es sei $\mathbb{F}_q$ der Körper mit q Elementen ($q = p^r$, p prim). Zeigen Sie:

(a) Jede Gerade in $\mathbb{P}^n_{\mathbb{F}_q}$ enthält genau $q + 1$ Punkte.

(b) Die projektive Ebene $\mathbb{P}^2_{\mathbb{F}_q}$ hat $q^2 + q + 1$ Punkte und genauso viele Geraden.

(c) Interpretieren Sie den Graph im Bild als Darstellung der projektiven Ebene $\mathbb{P}^2_{\mathbb{F}_2}$. (Auch die Kreislinie ist eine Gerade). Diese projektive Ebene mit sieben Punkten und Geraden wird **Fano-Ebene** genannt.



Übung 3.3. Es sei V ein endlich-dimensionaler K-Vektorraum und $M \subset \mathbb{P}V$ eine Teilmenge. Sei $W = \mathbb{P}(\operatorname{span}(M))$ der von M aufgespannte projektive Unterraum und betrachte die Menge der *Sekanten*

$$\operatorname{Sek}^1(M) = \{\overline{pq} : p, q \in M\}$$

zwischen Punkten in M. Definiere induktiv $\operatorname{Sek}^m(M) = \operatorname{Sek}^1\big(\operatorname{Sek}^{m-1}(M)\big)$ für $m \geqslant 2$. Zeigen Sie:

(a) $W = \bigcup_{m \geqslant 1} \operatorname{Sek}^m(M)$;

(b) Falls $\dim(M) \leqslant n$, dann gilt $W = \operatorname{Sek}^n(M)$.

Übung 3.4. Sei $K = \mathbb{C}$. Bestimmen Sie alle Möbius-Transformationen auf $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, die die folgenden Teilmengen in sich abbilden:

(a) (i) $\mathbb{R} = \{x + iy : y = 0\}$; (ii) $\mathbb{H} = \{x + iy : y > 0\}$; (iii) $\overline{\mathbb{H}} = \{x + iy : y \geqslant 0\}$; (iv) $\mathbb{D} = \{x + iy : x^2 + y^2 < 1\}$; (v) $\overline{\mathbb{D}} = \{x + iy : x^2 + y^2 \leqslant 1\}$.

(b) Sei $\varphi(t) = \frac{t-i}{t+i}$. Zeigen Sie, dass $\varphi(\mathbb{H}) = \mathbb{D}$ gilt.

3.2. Kurze Geschichte der Geometrie

Die Geometrie wurde mehr als zweitausend Jahre lang, von der Antike bis in die Neuzeit, vor allem durch die berühmten *Elemente* des Euklid[4] bestimmt. Sie wird dort als eine *axiomatische Theorie* präsentiert, d.h. sie geht von wenigen einfachen Grundtatsachen aus, den Axiomen, die als plausibel angesehen und nicht weiter begründet werden, und alles Übrige wird durch logisches Schließen aus den Axiomen hergeleitet[5]. Diese Herangehensweise hat natürlich die ganze Mathematik geprägt, obwohl sie lange fast völlig auf die Geometrie beschränkt war.

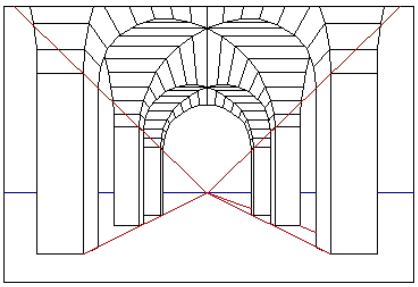
Lateinische Übersetzung der *Elemente* des Euklid — Druck von Erhard Ratdolt (1482)

Bildquelle: Wikimedia Commons

[4] Euklid von Alexandria (vermutlich 3. Jahrhundert v. Chr.), griechischer Mathematiker, der berühmteste Geometer der Geschichte; über sein Leben ist jedoch fast nichts bekannt.

[5] Jedenfalls nach moderner Interpretation. Euklid argumentiert dazwischen durchaus auch anschaulich.

Die Entwicklung der projektiven Geometrie nahm in der Renaissance ihren Anfang. Sie ist eine der ersten neuzeitlichen Theorien, die sich klar von der antiken Geometrie abheben und entstand als eine Erweiterung der euklidischen Geometrie zunächst aus der Überzeugung, dass parallele Geraden, die in den Aussagen der euklidischen Geometrie häufig zu Ausnahmen führen, sich „im Unendlichen schneiden". Die Grundlagen der projektiven Geometrie wurden unter anderem durch Kepler[6] und Desargues[7] gelegt. Eine wichtige Rolle hat auch die Entwicklung der perspektivischen Malerei gespielt. Dort schneiden sich parallele Geraden im Raum, wenn sie durch Zentralprojektion auf einer Leinwand dargestellt werden, im sogenannten Fluchtpunkt, der ebenfalls einen unendlich-fernen Punkt repräsentiert.



Zentralperspektive mit Fluchpunkt
Bildquelle: Wikimedia Commons (W. Gothe)

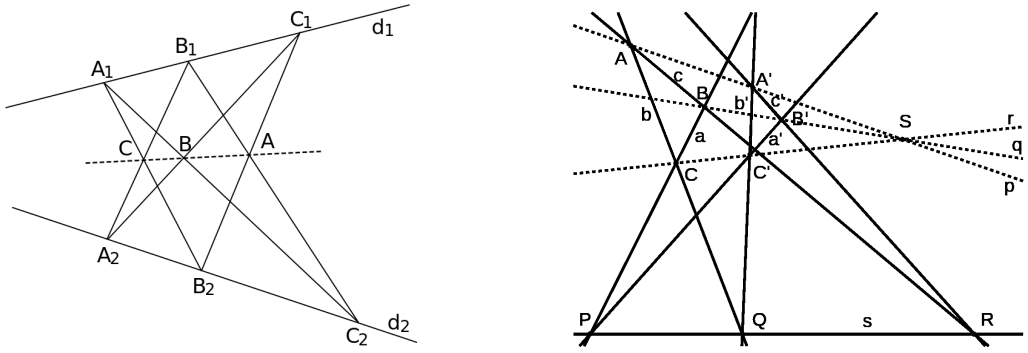
Raffael: *Die Schule von Athen* (Fresko, Stanza della Segnatura, Vatikan, 1510) *Bildquelle:* Wikimedia Commons

Trotz dieser Analogie über die Schnittpunkte paralleler Geraden, sind die Geometrie der perspektivischen Darstellung (sogenannte darstellende Geometrie) und die projektive Geometrie nicht genau dasselbe. Diese schönen Bilder sollte man also nicht mit den dreidimensionalen Bildern verwechseln, die wir zur Illustration der projektiven Ebene verwendet haben.

Außer der projektiven Geometrie nahm aber in der frühen Neuzeit eine noch weiterreichende Entwicklung ihren Anfang: Das Rechnen in Koordinaten, die *kartesische Geometrie*[8]. Dadurch ließ sich alle Geometrie vollständig in Algebra übersetzen. Für den axiomatischen Zugang wie bei Euklid setzte sich später die Bezeichnung *synthetische Geometrie* durch, für die kartesische Geometrie dagegen die Bezeichnung *analytische Geometrie*[9].

Zunächst spielten kartesische Koordinaten aber eher in der Mechanik und in der Analysis eine Rolle. Die synthetische Geometrie war bis weit ins 19. Jahrhundert bestimmend dafür, was als Geometrie galt und war fester Bestandteil jeder mathematischen Ausbildung. Ihre klaren, logischen Ableitungen galten als Inbegriff mathematischer Schönheit und Präzision. Die synthetische Geometrie (in der Form der projektiven aber auch der sogenannten nicht-euklidischen Geometrie) erreichte im späten 19. Jahrhundert ihren Höhepunkt.

[6]Johannes Kepler (1571–1630), deutscher Astronom, Mathematiker und Universalgelehrter
[7]Girard Desargues (1591–1661), französischer Mathematiker und Ingenieur
[8]nach René Descartes (1596–1650), französischer Philosoph, Mathematiker und Naturwissenschaftler
[9]Auch die algebraische Geometrie ist demnach analytisch. Der Gegensatz 'analytisch/synthetisch' in dem hier beschriebenen Sinn hat nicht direkt mit dem Gegensatz 'analytisch/algebraisch' bei der modernen Einteilung der Mathematik in ihre Teilgebiete zu tun.



Schließungssätze von Pappos[10] und Desargues; der Satz von Pappos impliziert — durch rein synthetische Argumente — den von Desargues (Satz von Hessenberg, 1905); *Bildquelle:* Wikimedia Commons

Gleichzeitig entwickelte sich ab dem frühen 19. Jahrhundert die analytische Geometrie. Die Geometrie profitierte dabei von neuen Methoden der Algebra und der Analysis und es entstanden die Gebiete, die heute *algebraische Geometrie* und *Differentialgeometrie* heißen, mit Konsequenzen, die meilenweit über das antike Verständnis hinausgehen.

Der analytische Zugang zur projektiven Geometrie durch homogene Koordinaten entstand im frühen 19. Jahrhundert, vor allem durch Arbeiten von Möbius (1827) und Plücker[11] (1830). Nach und nach gewann die analytische Geometrie an Reichweite und Bedeutung und hat sich im 20. Jahrhundert immer mehr durchgesetzt. Die synthetische Geometrie hat dagegen an Gewicht verloren (zunächst in der Forschung, dann auch in der Lehre). Gegenwärtig ist sie vor allem für die Kombinatorik von Bedeutung.

Übungen

Die folgenden Aufgaben enthalten einige Konzepte der klassischen projektiven Geometrie. Sie haben mit der algebraischen Geometrie nur am Rand zu tun, stellen aber die Verbindung zu einigen Konstruktionen der synthetischen Geometrie her.

Übung 3.5. Es seien $p_1, \dots, p_4$ vier verschiedene Punkte in $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. Nach Kor. 3.3 gibt es genau eine Projektivität $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ mit

$$\varphi(p_2) = 1,\ \varphi(p_3) = 0,\ \varphi(p_4) = \infty.$$

Die Zahl $[p_1, p_2; p_3, p_4] = \varphi(p_1) \in K \setminus \{0,1\}$ heißt das **Doppelverhältnis** des geordneten Viertupels (p_1, p_2, p_3, p_4). Zeigen Sie:

(a) Seien $(p_1, \dots, p_4)$, $(q_1, \dots, q_4)$ zwei geordnete Viertupel von Punkten in $\mathbb{P}^1$. Genau dann gibt es eine Projektivität Ψ auf $\mathbb{P}^1$ mit $\Psi(p_i) = q_i$ (für $i = 1, \dots, 4$), wenn $[p_1, p_2; p_3, p_4] = [q_1, q_2; q_3, q_4]$ gilt. Insbesondere erhalten Projektivitäten das Doppelverhältnis.

(b) Es gilt

$$[p_1, p_2, p_3, p_4] = \frac{p_1 - p_3}{p_2 - p_3} : \frac{p_1 - p_4}{p_2 - p_4}.$$

[10] Pappos von Alexandria (ca. 290–350)

[11] Julius Plücker (1801–1868), deutscher Mathematiker und Physiker

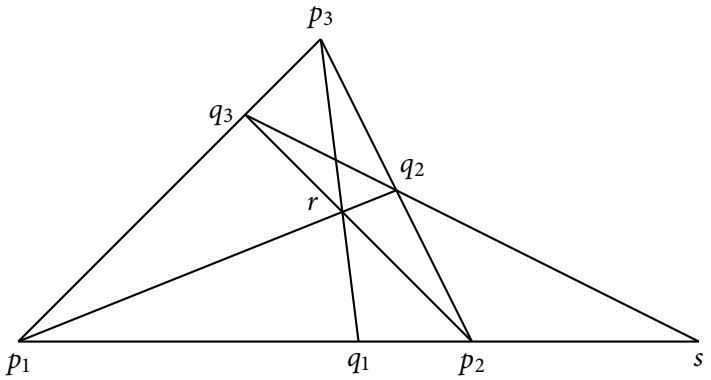
(c) In homogenen Koordinaten berechnet sich das Doppelverhältnis folgendermaßen. Es sei $p_i = [x_i, y_i]$, $i = 1, \dots, 4$. Dann gilt

$$[p_1, p_2; p_3, p_4] = \frac{x_1 y_3 - x_3 y_1}{x_2 y_3 - x_3 y_2} : \frac{x_1 y_4 - x_4 y_1}{x_2 y_4 - x_4 y_2}.$$

Übung 3.6. Es sei K ein Körper der Charakteristik $\neq 2$. Ein Viertupel (p_1, p_2, p_3, p_4) von Punkten heißt **harmonisch**, wenn $[p_1, p_2; p_3, p_4] = -1$ gilt. Zeigen Sie: Genau dann ist $(p_1, \dots, p_4)$ harmonisch, wenn es eine Projektivität gibt, die p_1 und p_2 vertauscht und p_3 und p_4 fixiert.

Übung 3.7. Es K ein Körper der Charakteristik $\neq 2$ und seien p_1, p_2, p_3 drei Punkte, nicht auf einer Geraden. Wähle Punkte $q_2 \in \overline{p_2 p_3}$, $q_3 \in \overline{p_1 p_3}$ mit $q_i \neq p_i$ für alle i, j. Es seien

$$r = \overline{p_1 q_2} \cap \overline{p_2 q_3}, \quad q_1 = \overline{p_1 p_2} \cap \overline{p_3 r}, \quad s = \overline{p_1 p_2} \cap \overline{q_2 q_3}.$$



Beweisen Sie, dass (p_1, p_2, q_1, s) harmonisch ist. (*Vorschlag:* Wählen Sie homogene Koordinaten derart, dass $p_1 = [0, 0, 1]$, $p_2 = [2, 0, 1]$, $p_3 = [0, 1, 0]$ und $s = [1, 0, 0]$. Zeigen Sie, dass dann $q_1 = [1, 0, 1]$ gilt.)

Übung 3.8. Es sei V ein Vektorraum der Dimension $n + 1$. Die durch einen Isomorphismus $\Phi\colon V \to V$ gegebene Projektivität $[\Phi]\colon \mathbb{P}V \to \mathbb{P}V$ heißt eine **Perspektivität** von $\mathbb{P}V$, wenn es eine Hyperebene H in $\mathbb{P}V$ gibt mit $[\Phi]q = q$ für alle $q \in H$.

(a) Beweisen Sie, dass die folgenden Aussagen äquivalent sind:
  (i) $[\Phi]$ ist eine Perspektivität.
  (ii) Es gibt eine Zahl $\lambda \in K$ mit $\operatorname{Rang}(\Phi - \lambda \mathrm{I}_{n+1}) \leqslant 1$.
  (iii) Es gibt $p \in \mathbb{P}V$ mit $[\Phi] \in \overline{pq}$ für alle $q \in \mathbb{P}V \setminus \{p\}$.
  (iv) Es gibt ein homogenes Koordinatensystem $p_0, \dots, p_n \in \mathbb{P}V$ mit

$$[\Phi]p_0 = p_0 \qquad \text{und} \qquad [\Phi]p_i \in \overline{p_0 p_i} \text{ für } i = 1, \dots, n.$$

(b) Es sei $[\Phi]$ eine Perspektivität, $[\Phi] \neq \mathrm{id}_{\mathbb{P}V}$. Zeigen Sie, dass der Punkt p mit der Eigenschaft (3) eindeutig bestimmt ist. Der Punkt p_0 heißt das **Zentrum** der Perspektivität.

(c) Veranschaulichen Sie mit einer Skizze, wie eine Perspektivität in $\mathbb{P}^2$ geometrisch aussieht.

Übung 3.9. Es sei V ein Vektorraum der Dimension $n+1$ und $\varphi\colon \mathbb{P}V \to \mathbb{P}V$ eine Projektivität. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) Es gibt einen Unterraum $H \subset \mathbb{P}V$ der Dimension $n - r$ mit $\varphi(p) = p$ für jedes $p \in H$.
(ii) Es gibt einen Unterraum $L \subset \mathbb{P}V$ der Dimension $r - 1$ mit $\varphi(q) \in \overline{qL}$ für jedes $q \in \mathbb{P}V$.
(iii) Es gibt Perspektivitäten $\varphi_1, \dots, \varphi_r$ von $\mathbb{P}V$ mit $\varphi = \varphi_1 \circ \cdots \circ \varphi_r$.

3.3. Projektive Varietäten

Wir untersuchen nun Lösungen von polynomialen Gleichungen im projektiven Raum, wie vorher im affinen Raum. Dazu fixieren wir wieder eine Körpererweiterung K/k mit K algebraisch abgeschlossen. Gegeben ein Polynom $f \in k[x_0, \dots, x_n]$ und einen Punkt $p = [a_0, \dots, a_n] \in \mathbb{P}^n = \mathbb{P}^n_K$, dann stoßen wir auf das Problem, dass die Auswertung $f(p)$ nicht ohne weiteres definiert ist; denn der Vektor $(a_0, \dots, a_n) \in K^{n+1}$ ist durch p nur bis auf Skalierung bestimmt und der Wert $f(a_0, \dots, a_n)$ kann sich durch diese Skalierung natürlich ändern.

Ein Polynom f heißt **homogen vom Grad** d oder eine **Form vom Grad** d, wenn alle Terme von f den Totalgrad d haben. Ein allgemeines Polynom, das homogen sein kann oder auch nicht, nennen wir zur Unterscheidung **inhomogen**. Ist f nun homogen vom Grad d, dann gilt

$$f(\lambda v) = \lambda^d f(v)$$

für alle $\lambda \in K$ und $v \in K^{n+1}$. Denn diese Gleichheit gilt für jedes Monom x^α mit $\alpha = |d|$ wegen $(\lambda x)^\alpha = (\lambda x_0)^{\alpha_1} \cdots (\lambda x_n)^{\alpha_n} = \lambda^d x^\alpha$ und damit auch für f. Insbesondere ist die Frage, ob $f(v)$ gleich 0 ist oder ungleich 0 von der Skalierung unabhängig. Deshalb kann man die Nullstellenmenge von homogenen Polynomen im projektiven Raum sinnvoll definieren.

Ist $T \subset k[x_0, \dots, x_n]$ eine Menge von homogenen Polynomen, dann schreiben wir

$$\mathcal{V}_+(T) = \{p \in \mathbb{P}^n : f(p) = 0 \text{ für alle } f \in T\}$$

und nennen $\mathcal{V}_+(T)$ die durch T bestimmte **projektive k-Varietät**.

Beispiele 3.4. (1) (sei $k = K$) Jeder projektive Unterraum von $\mathbb{P}^n$ ist auch eine projektive Varietät. Denn ein linearer Unterraum $U \subset \mathbb{A}^{n+1}$ der Dimension $m+1$ ist die Lösungsmenge eines homogenen linearen Gleichungssystem $\ell_1 = \cdots = \ell_{n-m} = 0$ gegeben durch Linearformen $\ell_1, \dots, \ell_{n-m} \in k[x_0, \dots, x_n]_1$. Damit ist $\mathbb{P}U = \mathcal{V}_+(\ell_1, \dots, \ell_{n-m})$.

(2) Es sei $f \in k[x_0, \dots, x_n]$, $f \neq 0$, ein homogenes Polynom vom Grad $d > 0$. Die zugehörige projektive Varietät $\mathcal{V}_+(f)$ heißt eine **Hyperfläche vom Grad** d in $\mathbb{P}^n$. Hyperflächen vom Grad 1 sind Hyperebenen. Hyperflächen vom Grad 2 heißen **Quadriken**.

Ist $T \subset k[x_0, \dots, x_n]$ eine Menge von homogenen Polynomen, dann schreiben wir außerdem

$$\mathcal{D}_+(T) = \{p \in \mathbb{P}^n : f(p) \neq 0 \text{ für alle } f \in T\}.$$

Insbesondere ist dann $D_i = \mathcal{D}_+(x_i) \cong \mathbb{A}^n$ ein affiner Raum, wie im ersten Abschnitt beschrieben. Ist $X = \mathcal{V}_+(f_1, \dots, f_r) \subset \mathbb{P}^n$ eine projektive Varietät, dann ist der Schnitt von X mit dem affinen Raum D_i eine affine Varietät in D_i, nämlich

$$\begin{aligned} X \cap D_i &= \{[a_0, \dots, a_n] \in X : a_i \neq 0\} = \{[a_0, \dots, a_{i-1}, 1, a_i, a_n] \in X\} \\ &\cong \{(a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in \mathbb{A}^n : f_j(a_0, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n) = 0 \text{ für } j = 1, \dots, r\}. \end{aligned}$$

Wir setzen also in den *homogenen* Gleichungen, die die projektive Varietät X definieren, einfach $x_i = 1$ und erhalten *inhomogene* Gleichungen, die die affine Varietät $X \cap D_i$ definieren. Die inhomogenen Gleichungen entstehen durch **Dehomogenisieren** bezüglich der Variablen x_i.

Beispiele 3.5. (1) Eine Linearform $\ell = c_0x_0 + \cdots + c_nx_n$, $\ell \neq 0$, definiert die projektive Hyperebene $H = \mathcal{V}_+(\ell)$. Der Schnitt

$$H \cap D_0 = \{(a_1, \ldots, a_n) : c_0 + c_1a_1 + \cdots + c_na_n = 0\}$$

mit dem affinen Raum $D_0 = \mathcal{D}_+(x_0)$ ist eine affine Hyperebene in $\mathbb{A}^n$, es sei denn, es gilt $c_1 = \cdots = c_n = 0$. In diesem Fall ist $c_0 \neq 0$ und H ist die Hyperebene $\mathcal{V}(x_0)$, also die Hyperebene im Unendlichen bezüglich D_0. Ihr Schnitt mit D_0 ist dann natürlich leer.

(2) Es gelte $\operatorname{char}(k) \neq 2$. Sei $f \in k[x_0, \ldots, x_n]$ eine quadratische Form. Wie aus der linearen Algebra bekannt, gibt es eine symmetrische Matrix $A \in \operatorname{Sym}_{n+1}(k)$ mit

$$f = \begin{bmatrix} x_0 & \cdots & x_n \end{bmatrix} \begin{bmatrix} a_{0,0} & \cdots & a_{0,n} \\ \vdots & \ddots & \vdots \\ a_{0,n} & \cdots & a_{n,n} \end{bmatrix} \begin{bmatrix} x_0 \\ \vdots \\ x_n \end{bmatrix}.$$

(Dabei ist also der Diagonaleintrag $a_{i,i}$ der Koeffizient von x_i^2 und die Einträge $a_{i,j} = a_{j,i}$ für $j \neq i$ sind jeweils der Koeffizient von x_ix_j halbiert.) Sei r der Rang von A. Falls $r = n + 1$ gilt, heißt die quadratische Form f **nicht-ausgeartet**, andernfalls **ausgeartet**. Die Matrix A kann man diagonalisieren, d.h. es gibt eine invertierbare Matrix $P \in \mathrm{GL}_{n+1}(k)$ mit $P^tAP = \operatorname{Diag}(b_0, \ldots, b_n)$, wobei $b_1, \ldots, b_n \in k$. (Das sind im Allgemeinen *nicht* die Eigenwerte von A, es sei denn $P^t = P^{-1}$.) Durch Vertauschen von Zeilen und Spalten können wir annehmen, dass $b_0, \ldots, b_{r-1} \neq 0$, $b_r = \cdots = b_n = 0$ gilt. Die transformierte Matrix hat dann die Form

$$P^tAP = \begin{bmatrix} b_0 & & & & & \\ & \ddots & & & & \\ & & b_{r-1} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}.$$

Das transformierte Polynom $g = f(P^{-1}x)$ ist also

$$g = b_0x_0^2 + \cdots + b_{r-1}x_{r-1}^2.$$

Wie man g nun weiter vereinfachen kann, hängt vom Körper k ab. Wenn k algebraisch abgeschlossen ist, dann können wir durch Multiplikation mit einer Diagonalmatrix jeden Diagonaleintrag ungleich 0 von links und von rechts mit $1/\sqrt{b_i}$ multiplizieren und damit $b_0 = \cdots = b_{r-1} = 1$ erreichen. Insbesondere gibt es im nicht-ausgearteten Fall nur eine einzige Normalform, nämlich

$$g = x_0^2 + \cdots + x_n^2.$$

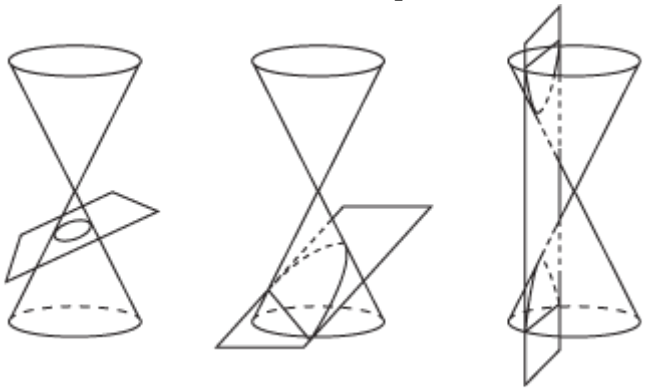
Ist dagegen $k = \mathbb{R}$, dann gibt es nur positive Quadratwurzeln, und wir können jeden Diagonaleintrag $b_i \neq 0$ beidseitig entweder mit $1/\sqrt{b_i}$ oder mit $1/\sqrt{-b_i}$ multiplizieren. Die Diagonaleinträge werden damit alle zu +1, −1 oder 0. Ist r_+ die Anzahl der Einträge +1 und r_- die Anzahl der Einträge −1, dann heißt $s = r_+ - r_-$ die *Sylvester-Signatur* von A. Zusammen mit dem Rang ist sie also die einzige reelle Invariante einer quadratischen Form. Da wir uns letztlich nur für die Nullstellenmenge interessieren, können wir immer f durch $-f$ ersetzen, die ganze Matrix also mit −1 multiplizieren. Wir können daher immer annehmen, dass $s \geqslant 0$ gilt.

Betrachten wir den Fall $n = 2$. Es gibt dann genau zwei Normalformen von nicht-ausgearteten quadratischen Formen, nämlich

$$g = x_0^2 + x_1^2 + x_2^2 \qquad \text{oder} \qquad g = x_0^2 + x_1^2 - x_2^2.$$

Im ersten Fall hat die Quadrik $\mathcal{V}_+(g)$ keine reellen Punkte, wir können also kein Bild zeichnen. Bleiben wir beim zweiten Fall $g = x_0^2 + x_1^2 - x_2^2$. Wenn wir diese Form bezüglich x_2 dehomogenisieren, dann erhalten wir $g(x_0, x_1, 1) = x_0^2 + x_1^2 - 1$, was einen Kreis definiert. Wenn wir andererseits nach x_0 dehomogenisieren, erhalten wir $g(1, x_1, x_2) = 1 + x_1^2 - x_2^2 = 1 + (x_1 + x_2)(x_1 - x_2)$. Die Nullstellenmenge dieses Polynoms ist eine Hyperbel.

Das können wir folgendermaßen visualisieren: Das reelle Bild der durch g definierten affinen Varietät $\mathcal{V}(g) \subset \mathbb{A}^3$ ist ein Kegel in $\mathbb{R}^3$. Die affinen Varietäten $\mathcal{V}_+(g) \cap D_i$ entstehen durch Schnitt von $\mathcal{V}(g)$ mit der Ebene $\mathcal{V}(x_i - 1)$. Je nachdem, wie der Kegel jeweils zur Ebene liegt, entstehen dabei qualitativ drei verschiedene Bilder, nämlich Ellipse (oder Kreis), Parabel oder Hyperbel.



Ellipse, Parabel und Hyperbel

Bildquelle: Cliffsnotes.com (modifiziert)

Dieses Bild erklärt, warum ebene Quadriken als **Kegelschnitte** oder **Koniken** bezeichnet werden.

Frage 3.6. Wie muss man den Kegel $\mathcal{V}(x_0^2 + x_1^2 - x_2^2)$ schneiden, um eine Parabel zu bekommen?

Zwei allgemeine Dinge haben wir gerade im Fall von Quadriken gesehen:
(1) Ist $X = \mathcal{V}_+(f_1, \ldots, f_r) \subset \mathbb{P}^n$ eine projektive Varietät und $[P]\colon \mathbb{P}^n \to \mathbb{P}^n$ eine Projektivität gegeben durch eine Matrix $P \in \mathrm{GL}_{n+1}(k)$, dann ist $[P](X) \subset \mathbb{P}^n$ die projektive Varietät

$$[P](X) = \mathcal{V}_+\big(f_1(P^{-1}x), \ldots, f_r(P^{-1}x)\big).$$

Zwei projektive Varietäten $X, X' \subset \mathbb{P}^n$ heißen **projektiv äquivalent (über k)**, wenn es eine Projektivität $[P] \in \mathrm{PGL}_{n+1}(k)$ mit $[P](X) = X'$ gibt.

Im Fall von Quadriken haben wir also gesehen, dass jede nicht-ausgeartete Quadrik in $\mathbb{P}^n$ über einem algebraisch abgeschlossenen Körper zu $\mathcal{V}(x_0^2 + \cdots + x_n^2)$ projektiv äquivalent ist.

Ist $k = K$, so sind alle Mengen von $n + 2$ Punkten in allgemeiner Lage projektiv äquivalent (Satz 3.2). In $\mathbb{P}^1$ sind zwei Mengen von vier $(= n + 3)$ Punkten genau dann projektiv äquivalent, wenn sie, bis auf Vertauschung, dasselbe Doppelverhältnis besitzen (siehe dazu Übung 3.5).

(2) Ist $T \subset k[x_0, \ldots, x_n]$ eine Menge von homogenen Polynomen, so gehört dazu einerseits die projektive Varietät $V = \mathcal{V}_+(T)$, andererseits auch die affine k-Varietät $\widehat{V} = \mathcal{V}(T)$. Die Varietät

$\widehat{V}$ heißt der **affine Kegel über** V. Dann gilt

$$(a_0, \ldots, a_n) \in \widehat{V} \quad \Leftrightarrow \quad (\lambda a_0, \ldots, \lambda a_n) \in \widehat{V} \text{ für alle } \lambda \in K,$$

was die Bezeichnung als Kegel erklärt (vgl. Bild oben).

Die Korrespondenz zwischen Varietäten und Idealen geht ganz ähnlich wie im Affinen, nur dass man sich auf Ideale beschränken muss, die von homogenen Polynomen erzeugt werden.

Es ist sinnvoll, das gleich wieder in der Sprache der Ringe anstatt nur der Polynome zu sagen. Ein **graduierter Ring** ist ein Ring S (kommutativ mit Eins) zusammen mit einer Zerlegung der additiven Gruppe $(S, +)$ in eine direkte Summe

$$S = \bigoplus_{d \geqslant 0} S_d,$$

derart[12], dass für die Multiplikation gilt

$$S_d \cdot S_e \subset S_{d+e}.$$

Die Elemente von S_d heißen die **homogenen Elemente vom Grad** d in S. Jedes Element $s \in S$ hat also eine eindeutige Darstellung

$$s = s_0 + \cdots + s_N$$

als Summe von homogenen Elementen $s_d \in S_d$ (für ein $N \geqslant 0$). Für $s \in S$ bezeichnet s_d immer den homogenen Anteil vom Grad d von s. Das wichtigste Beispiel ist natürlich der Polynomring

$$k[x_0, \ldots, x_n] = \bigoplus_{d \geqslant 0} k[x_0, \ldots, x_n]_d,$$

wobei $k[x_0, \ldots, x_n]_d$ den Raum der homogenen Polynome vom Grad d bezeichnet[13]. Eine **graduierte k-Algebra** ist ein graduierter Ring S, der k als Teilring enthält, mit $k \subset S_0$. Der Polynomring ist offensichtlich eine graduierte k-Algebra.

Lemma und Definition 3.7. Es sei S ein graduierter Ring. Ein Ideal I von S heißt **homogen**, wenn es die folgenden äquivalenten Bedingungen erfüllt:

(1) Das Ideal I wird von homogenen Elementen erzeugt.
(2) Für jedes $s \in S$ gilt: Genau dann liegt s in I, wenn alle homogenen Teile s_d in I liegen.
(3) Es gilt $I = \bigoplus_{d \geqslant 0} (I \cap S_d)$, d.h. jedes Element von $f \in I$ hat eine eindeutige Zerlegung $f = f_0 + \cdots + f_N$ in homogene Elemente $f_d \in I \cap S_d$.

Beweis. Übung 3.11. ∎

Korollar 3.8. *Summen, Produkte, Durchschnitte und Radikale homogener Ideale sind homogen.*

Beweis. Bei Summen und Produkten ist es klar aus Lemma 3.7(1), bei Durchschnitten aus (2). Für das Radikal, siehe Übungen. ∎

Korollar 3.9. *Genau dann ist ein homogenes Ideal I ein Primideal, wenn gilt: Sind $f, g \in S$ homogene Elemente mit $fg \in I$, so folgt $f \in I$ oder $g \in I$.*

[12] Allgemeiner können die S_d statt durch $\mathbb{Z}_+$ auch durch $\mathbb{Z}$, $\mathbb{Z}_+^n$ oder sogar ein beliebiges Monoid indiziert sein.
[13] Das Nullpolynom hat den Grad $-\infty$. Nach dieser Definition ist es aber gleichzeitig homogen von jedem Grad.

Beweis. Folgt aus Lemma 3.7(2). ∎

Proposition 3.10. *Die Vereinigung endlich vieler projektiver k-Varietäten ist wieder eine projektive k-Varietät, ebenso der Durchschnitt beliebig vieler projektiver k-Varietäten. Der ganze Raum $\mathbb{P}^n$ und die leere Menge sind projektive k-Varietäten.*

Beweis. Völlig analog zum Fall affiner k-Varietäten (Prop. 1.2). ∎

Wie im affinen Fall bilden die projektiven k-Varietäten in $\mathbb{P}^n$ die abgeschlossenen Teilmengen einer Topologie, die wieder die k-**Zariski-Topologie** genannt wird. Die projektiven k-Varietäten sind die **Zariski-abgeschlossenen** oder k-**abgeschlossenen Teilmengen** von $\mathbb{P}^n$. Die kleinste projektive k-Varietät, die eine Menge $M \subset \mathbb{P}^n$ enthält, heißt der k-**Zariski-Abschluss** von M.

Ist $M \subset \mathbb{P}^n$ eine Teilmenge, dann bilden wir dazu das **homogene k-Verschwindungsideal**

$$\mathcal{I}_+(M) = \left\langle \{ f \in k[x_0, \ldots, x_n] \text{ homogen mit } f(p) = 0 \text{ für alle } p \in M \} \right\rangle.$$

Der Zariski-Abschluss von M ist genau die Menge $\overline{M} = \mathcal{V}_+(\mathcal{I}_+(M))$. Irreduzibilität und irreduzible Komponenten projektiver Varietäten verhalten sich genauso wie im Affinen. Genau dann ist eine projektive k-Varietät irreduzibel über k, wenn ihr homogenes k-Verschwindungsideal prim ist (vgl. Prop. 1.9). Jede projektive k-Varietät ist in eindeutiger Weise die Vereinigung ihrer irreduziblen Komponenten (vgl. Satz 1.13). Die Beweise sind die gleichen.

Als nächstes übertragen wir den Nullstellensatz in die homogene Situation. Dabei muss man die folgende wichtige Feinheit beachten: Natürlich gilt $\mathcal{V}_+(1) = \varnothing$, aber es gilt auch $\mathcal{V}_+(x_0, \ldots, x_n) = \varnothing$, da die homogenen Koordinaten eines Punktes niemals alle 0 sein können.

Definition 3.11. Das Ideal $\langle x_0, \ldots, x_n \rangle$ heißt das **irrelevante Ideal** von $k[x_0, \ldots, x_n]$.

Das irrelevante Ideal ist das einzige homogene, maximale Ideal von $k[x_0, \ldots, x_n]$. Der Name ist irreführend, denn das irrelevante Ideal ist für die kommutative Algebra enorm wichtig.

Satz 3.12 (Projektiver Nullstellensatz)**.** *Es sei $I \subset k[x_0, \ldots, x_n]$ ein homogenes Ideal.*

(1) Genau dann gilt $\mathcal{V}_+(I) = \varnothing$, wenn $\langle x_0, \ldots, x_n \rangle \subset \sqrt{I}$.

(2) Falls $\mathcal{V}(I) \neq \varnothing$, so gilt $\mathcal{I}_+(\mathcal{V}_+(I)) = \sqrt{I}$.

Beweis. Es sei $V = \mathcal{V}_+(I) \subset \mathbb{P}^n$ und $\widehat{V} = \mathcal{V}(I) \subset \mathbb{A}^{n+1}$. (1) Es gilt $V = \varnothing$ genau dann, wenn $\widehat{V} \subset \{(0, \ldots, 0)\}$. Dies wiederum ist nach dem starken Nullstellensatz (Satz 1.34) äquivalent zu $\langle x_0, \ldots, x_n \rangle \subset \mathcal{I}(\widehat{V}) = \sqrt{I}$.

(2) Es gelte $V \neq \varnothing$. Nach dem starken Nullstellensatz gilt $\mathcal{I}(\widehat{V}) = \sqrt{I}$. Wir müssen also $\mathcal{I}(\widehat{V}) = \mathcal{I}_+(V)$ zeigen. Die Inklusion von rechts nach links ist klar. Ist umgekehrt $f \in \mathcal{I}(\widehat{V})$ und $p \in \widehat{V}$, so folgt $\lambda p \in \widehat{V}$ und damit $f(\lambda p) = 0$ für alle $\lambda \in K$. Ist $f = f_0 + \cdots + f_N$ die Zerlegung von f in seine homogenen Teile, so folgt daraus $f_d(p) = 0$ für $d = 0, \ldots, N$, da K als algebraisch abgeschlossener Körper unendlich viele Elemente enthält. Also folgt $f_d \in \mathcal{I}(\widehat{V})$, damit auch $f_d \in \mathcal{I}_+(V)$ für alle d und somit $f \in \mathcal{I}_+(V)$. ∎

Korollar 3.13. *Es sei $S = k[x_0, \dots, x_n]$ und $I \subset S$ ein homogenes Ideal. Äquivalent sind:*

(i) $\mathcal{V}_+(I) = \varnothing$;

(ii) es gibt ein $d \geqslant 0$ *mit* $S_d \subset I$;

(iii) es gibt ein $d \geqslant 0$ *mit* $x_0^d, \dots, x_n^d \in I$;

(iv) es gibt ein $d \geqslant 0$ *mit* $\langle x_0, \dots, x_n \rangle^d \subset I$;

Beweis. (i)⇔(iii) ist Satz 3.12(a). Ist $x_i^d \in I$ für $i = 0, \dots, n$, so gilt $S_e \subset I$ für $e > (n+1)(d-1)$; denn für solches e kommt in jedem Monom vom Grad e mindestens eine der Variablen mit Exponent mindestens d vor. Das zeigt (iii)⇒(ii). Die Implikationen (ii)⇒(iv) und (iv)⇒(i) sind klar. ∎

Korollar 3.14. *Die Zuordnungen $V \mapsto \mathcal{I}_+(V)$ und $I \mapsto \mathcal{V}_+(I)$ sind zwischen den Mengen*

$$\big\{\textit{projektive } k\textit{-Varietäten in } \mathbb{P}^n\big\} \leftrightarrow \big\{\textit{Homogene Radikalideale} \subsetneq k[x_0, \dots, x_n]\big\}$$
$$\big\{\textit{irreduzible projektive } k\textit{-Varietäten in } \mathbb{A}^n\big\} \leftrightarrow \big\{\textit{Homogene Primideale} \subsetneq \langle x_0, \dots, x_n \rangle\big\}$$

zueinander invers und definieren jeweils eine Bijektion, wobei wir der leeren Varietät das irrelevante Ideal $\langle x_0, \dots, x_n \rangle$ zuordnen. ∎

Wie bei affinen Varietäten kann man vom Polynomring zum Restklassenring modulo dem Verschwindungsideal übergehen. Es sei $X \subset \mathbb{P}^n$ eine projektive k-Varietät. Dann heißt

$$k_+[X] = k[x_0, \dots, x_n]/\mathcal{I}_+(X)$$

der **homogene Koordinatenring von** X. Da Polynome schon keine Funktionen auf $\mathbb{P}^n$ definieren, sind die Elemente von $k_+[X]$ auch keine Funktionen auf X. Dafür erbt $k_+[X]$ vom Polynomring die Graduierung: Sei $f \in k[x_0, \dots, x_n]$ ein homogenes Polynom, $f \neq 0$, und sei $\overline{f}$ die Restklasse von f in $k_+[X]$. Dann definieren wir

$$\deg(\overline{f}) = \deg(f).$$

Dass das wohldefiniert ist, liegt daran, dass $\mathcal{I}_+(X)$ ein homogenes Ideal ist. Denn sind $f_1, f_2 \in k[x_0, \dots, x_n]$ homogen mit $\overline{f_1} = \overline{f_2}$, dann gilt also $f_1 - f_2 \in \mathcal{I}_+(X)$. Da $\mathcal{I}_+(X)$ homogen ist, bedeutet das nach Lemma 3.7, dass alle homogenen Teile von $f_1 - f_2$ in $\mathcal{I}_+(X)$ liegen. Weil f_1 und f_2 homogen sind, folgt daraus $\deg(f_1) = \deg(f_2)$ oder $f_1, f_2 \in \mathcal{I}_+(X)$ und damit $\overline{f_1} = \overline{f_2} = 0$ in $k_+[X]$. Wir haben bewiesen:

Proposition 3.15. *Der homogene Koordinatenring $k_+[X]$ einer projektiven k-Varietät $X \subset \mathbb{P}^n$ ist eine graduierte k-Algebra, mit der vom Polynomring induzierten Graduierung.* ∎

Sei $S = k_+[X]$ und $d \geqslant 0$. Die Gruppe S_d der homogenen Elemente vom Grad d ist ein endlich-dimensionaler k-Vektorraum. Ist nämlich $I = \mathcal{I}_+(X)$ und

$$I_d = \big\{f \in I \colon f \text{ homogen vom Grad } d\big\},$$

dann ist I_d ein Untervektorraum von $k[x_0, \dots, x_n]_d$ und S_d der Quotientenvektorraum

$$S_d = k[x_0, \dots, x_n]/I_d.$$

Die Dimensionen der verschiedenen homogenen Teile S_d (bzw. I_d) enthalten eine Reihe von Informationen über die Varietät X. Darauf kommen wir später zurück.

Übungen

Übung 3.10. Zeigen Sie: Der Vektorraum $k[x_0, \ldots, x_n]_d$ hat die Dimension $\binom{n+d}{n}$.

Übung 3.11. Beweisen Sie Lemma 3.7.

Übung 3.12. Sei I ein homogenes Ideal in einem graduierten Ring S. Zeigen Sie, dass auch das Radikal $\sqrt{I}$ ein homogenes Ideal ist.

Übung 3.13. Es sei $k = K$ und $\Gamma = \{p_1, \ldots, p_d\}$ eine Menge von d Punkten in $\mathbb{P}^n$. Zeigen Sie: Wenn Γ nicht in einer Geraden enthalten ist, dann gibt es homogene Polynome vom Grad $\leqslant d-1$, die Γ beschreiben.

Übung 3.14. Sei $k = K$ und sei $L \subset \mathbb{P}^n$ ein projektiver Unterraum der Dimension r. Zeigen Sie, dass das homogene Verschwindungsideal $\mathcal{I}_+(L) \subset k[x_0, \ldots, x_n]$ von $n-r$ Linearformen erzeugt wird. Zeigen Sie außerdem, dass es nicht möglich ist, $\mathcal{I}_+(L)$ mit weniger als $n-r$ Elementen zu erzeugen.

Übung 3.15. Sei $k = \mathbb{R}$. Bestimmen Sie
(a) alle Normalformen von Kegelschnitten in $\mathbb{P}^2$.
(b) alle Normalformen von nicht-ausgearteten Quadriken in $\mathbb{P}^3$.
(c) die affinen Quadriken, die als Schnitt mit $D_0 = \mathbb{A}^2$ bzw. $D_0 = \mathbb{A}^3$ entstehen.

Übung 3.16. Formulieren und beweisen Sie die projektive Version von Kor. 1.49: Sei $X \subset \mathbb{P}^n$ eine projektive k-Varietät. Wie sieht die Korrespondenz zwischen abgeschlossenen Untervarietäten von X und Idealen in $k_+[X]$ aus? Wie sehen im Fall $k = K$ die Ideale aus, die Punkten von X entsprechen?

Übung 3.17*. Es sei K ein algebraisch abgeschlossener Körper und seien $L_1, \ldots, L_4 \in \mathbb{P}^3_K$ vier Geraden. Beweisen Sie, dass es mindestens eine Gerade gibt, die jede der Geraden $L_1, \ldots, L_4$ schneidet.

3.4. Homogenisierung und projektiver Abschluss

Wir haben schon gesehen, wie man von homogenen Gleichungen, die eine projektive Varietät definieren, durch Dehomogenisieren zu inhomogenen Gleichungen übergeht, die eine affine Varietät definieren: Sind $f_1, \ldots, f_r \in k[x_0, \ldots, x_n]$ homogen und ist $X = \mathcal{V}_+(f_1, \ldots, f_r)$, dann definieren $\widetilde{f_i} = f_i(1, x_1, \ldots, x_n)$ die affine Varietät $X \cap D_0 = \mathcal{V}(\widetilde{f_1}, \ldots, \widetilde{f_r}) \subset \mathbb{A}^n$.

Es geht auch umgekehrt: Sei $g \in k[x_1, \ldots, x_n]$ ein inhomogenes Polynom. Setze

$$g^* = x_0^{\deg(g)} g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

Das Polynom g^* ist homogen vom Grad $\deg(g)$ und heißt die **Homogenisierung von g bezüglich** x_0. Noch expliziter kann man das so ausschreiben: Ist $g = \sum_{\alpha \in \mathbb{Z}_+^n} c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, dann ist

$$g^* = \sum_{\alpha \in \mathbb{Z}_+^n} c_\alpha x_0^{\deg(g)-|\alpha|} x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Beispiel 3.16. Die Homogenisierung von $x - y^2 + 1$ bezüglich der Varibalen z ist $xz - y^2 + z^2$.

Proposition 3.17. *Es seien $g, g_1, g_2 \in k[x_1, \ldots, x_n]$ und seien $f, f_1, f_2 \in k[x_0, \ldots, x_n]$ homogen. Es gelten die folgenden Aussagen:*

(1) $\widetilde{f_1 + f_2} = \widetilde{f_1} + \widetilde{f_2}$ und $\widetilde{f_1 f_2} = \widetilde{f_1}\widetilde{f_2}$;

(2) $(g_1 g_2)^* = g_1^* g_2^*$ und falls $\deg(g_1) = \deg(g_2)$, dann auch $(g_1 + g_2)^* = g_1^* + g_2^*$;

(3) $g = \widetilde{g^*}$;
(4) $f = x_0^m(\widetilde{f})^*$ *für ein* $m \geqslant 0$.

Beweis. Übung 3.18. ∎

Bemerkung 3.18. Ist $f \in k[x_0, \ldots, x_n]$ homogen vom Grad d, dann kann der Totalgrad von $\widetilde{f}$ kleiner als d sein. Nach (4) passiert das genau dann, wenn in f keines der Monome $x_1^d, \ldots, x_n^d$ vorkommt oder, äquivalent, wenn f durch x_0 teilbar ist. Ist zum Beispiel $f = x_0^3 + x_0x_1^2 + x_0x_1x_2$, dann ist $\widetilde{f} = 1 + x_1^2 + x_1x_2$ und damit $(\widetilde{f})^* = x_0^2 + x_1^2 + x_1x_2$.

Als erstes diskutieren wir kurz den Fall $n = 1$. Homogene Polynome in zwei Variablen heißen auch **binäre Formen**. Damit kann man im Prinzip fast genauso rechnen wie mit inhomogenen Polynomen in einer Variablen.

Satz 3.19. *Es sei K ein algebraisch abgeschlossener Körper und $f \in K[x_0, x_1]$ eine binäre Form vom Grad d. Dann gibt es $a_1, \ldots, a_d, b_1, \ldots, b_d, c \in K$ mit*

$$f = c \cdot (b_1x_0 - a_1x_1)\cdots(b_dx_0 - a_dx_1) \text{ und damit}$$
$$\mathcal{V}_+(f) = \{[a_1, b_1], \ldots, [a_d, b_d]\} \subset \mathbb{P}^1.$$

Beweis. Das folgt leicht aus der entsprechenden Aussage für inhomogene Polynome in einer Variablen. Sei $\widetilde{f} = f(1, x_1) \in K[x_1]$ die Dehomogenisierung von f, $e = \deg(\widetilde{f}) \leqslant d$. Weil K algebraisch abgeschlossen ist, zerfällt $\widetilde{f}$ in Linearfaktoren, also

$$\widetilde{f} = c \cdot (x_1 - c_1)\cdots(x_1 - c_e)$$

für $c, c_1, \ldots, c_e \in K$. Wegen $f = x_0^{d-e}(\widetilde{f})^*$ folgt daraus

$$f = c \cdot (x_1 - c_1x_0)\cdots(x_1 - c_ex_0) \cdot x_0^{d-e}.$$ ∎

Ist f eine binäre Form ungleich 0, dann heißen die endlich vielen Punkte $\mathcal{V}_+(f)$ in $\mathbb{P}^1$ die Nullstellen von f. Ob zwei binäre Formen eine gemeinsame Nullstelle haben, kann man wieder mit Resultanten testen. Es ist sogar etwas einfacher als im inhomogenen Fall, weil man nicht aufpassen muss, ob der Leitkoeffizient ungleich 0 ist. Sind f und g zwei binäre Formen mit $\deg(f) = d$ und $\deg(g) = e$, dann definieren wir die Resultante von f und g als $\operatorname{Res}(f, g) = \operatorname{Res}_{d,e}(\widetilde{f}, \widetilde{g})$.

Korollar 3.20 (zu Satz 1.25)**.** *Es seien $f, g \in k[x_0, x_1]$ zwei binäre Formen vom Grad d bzw. e. Genau dann haben f und g eine gemeinsame Nullstelle in $\mathbb{P}^1$, wenn* $\operatorname{Res}(f, g) = 0$ *gilt.*

Beweis. Aus der Zerlegung in Linearfaktoren über $\overline{k}$ wie im obigen Satz sehen wir: Genau dann haben f und g eine gemeinsame Nullstelle, wenn $\widetilde{f}$ und $\widetilde{g}$ eine gemeinsame Nullstelle haben oder wenn x_0 ein Teiler von f und g ist. Im zweiten Fall haben f und g die gemeinsame Nullstelle $[0, 1]$. Wenn $\deg(\widetilde{f}) = d$ und $\deg(\widetilde{g}) = e$, dann ist x_0 kein Teiler von f und g und die Behauptung folgt aus Satz 1.25. Tatsächlich zeigt der Beweis (Lemma 1.24), dass es auch ausreicht, wenn nur eine der Gleichheiten $\deg(\widetilde{f}) = d$ und $\deg(\widetilde{g}) = e$ gilt. Es bleibt also nur der Fall $\deg(\widetilde{f}) < d$ und $\deg(\widetilde{g}) < e$. In diesem Fall sind f und g beide durch x_0 teilbar. Die Sylvestermatrix $\operatorname{Syl}_{d,e}(f, g)$ hat dann eine Nullspalte, also ist die Resultante 0. ∎

Ist I ein Ideal in $k[x_1, \dots, x_n]$, dann schreiben wir

$$I^* = \langle f^* : f \in I \rangle,$$

ein homogenes Ideal in $k[x_0, \dots, x_n]$.

Proposition 3.21. *Es sei $V \subset \mathbb{A}^n$ eine affine Varietät mit Verschwindungsideal $\mathcal{I}(V)$ und sei $X \subset \mathbb{P}^n$ der Zariski-Abschluss von V (als Teilmenge von $D_0 \subset \mathbb{P}^n$) in $\mathbb{P}^n$. Dann gilt*

$$\mathcal{I}_+(X) = \mathcal{I}(V)^*.$$

Die projektive Varietät X heißt der **projektive Abschluss von** V.

Beweis. Ist $f \in \mathcal{I}(V)$, so verschwindet f^* auf V und damit auch auf X. Also gilt $\mathcal{I}(V)^* \subset \mathcal{I}_+(X)$. Umgekehrt sei $f \in \mathcal{I}_+(X)$ homogen. Schreibe $f = x_0^m g$ mit $x_0 \nmid g$, $m \geqslant 0$. Dann verschwindet $\widetilde{g}$ auf V, also gilt $g \in \mathcal{I}(V)$. Wegen $x_0 \nmid g$, folgt $g = (\widetilde{g})^* \in \mathcal{I}(V)^*$, also auch $f \in \mathcal{I}(V)^*$. ∎

Ist X der projektive Abschluss von V und $H = \mathcal{V}(x_0)$ die Hyperebene im Unendlichen, dann ist

$$V_\infty = X \cap H$$

die Varietät der **unendlich fernen Punkte von** V. Das Verschwindungsideal von V_∞ ist

$$\mathcal{I}_+(V_\infty) = \{ f(0, x_1, \dots, x_n) : f \in \mathcal{I}(V)^* \}.$$

Man kann dieses Ideal auch ohne den Umweg über $\mathcal{I}(V)^*$ als das Ideal der Leitformen beschreiben (siehe Übung 3.20).

Warnung 3.22. Man muss vorsichtig sein, wenn man die Homogenisierung eines Ideals über seine Erzeuger beschreiben will. Ist zum Beispiel $n = 2$ und $f_1 = x_1$ und $f_2 = x_1 + 1$, dann gilt $\langle f_0, f_1 \rangle = k[x_0, \dots, x_n]$ und somit $\mathcal{V}(f_1, f_2) = \varnothing$, aber $\langle f_0^*, f_1^* \rangle = \langle x_1, x_0 + x_1 \rangle = \langle x_0, x_1 \rangle$, also $\mathcal{V}_+(f_0^*, f_1^*) = \{[0, 0, 1]\}$.

Dieses Problem tritt nicht auf, wenn man nur eine Gleichung hat, d.h. für $f \in k[x_1, \dots, x_n]$ ist der projektive Abschluss der affinen Hyperfläche $\mathcal{V}(f)$ immer $\mathcal{V}_+(f^*)$ (siehe Übung 3.19).

Im allgemeinen lässt sich das Problem vermeiden, indem man mit einer Gröbnerbasis arbeitet. Es sei $\leqslant$ eine Monomordnung auf $k[x_1, \dots, x_n]$ mit $x^\alpha < x^\beta$ für alle $\alpha, \beta \in \mathbb{Z}_+^n$ mit $|\alpha| < |\beta|$ (z.B. glex oder grevlex). Dann definieren wir eine Monomordnung auf $k[x_0, \dots, x_n]$ durch

$$x_0^a x^\alpha \leqslant' x_0^b x^\beta \quad \Leftrightarrow \quad \big(\alpha < \beta \text{ oder } \alpha = \beta \wedge a \leqslant b\big).$$

(Es ist leicht zu überprüfen, dass $\leqslant'$ tatsächlich eine Monomordnung ist.

Proposition 3.23. *Es sei I ein Ideal in $k[x_1, \dots, x_n]$ und G eine Gröbnerbasis von I bezüglich $\leqslant$. Dann ist $G^* = \{g^* : g \in G\}$ eine Gröbnerbasis von I^* bezüglich $\leqslant'$. Insbesondere gilt $I^* = \langle G^* \rangle$.*

Beweis. Da I^* von homogenen Polynomen erzeugt wird, genügt es zu zeigen: Ist $f \in I^*$ homogen, dann gibt es $g \in G$ derart, dass $\mathrm{LM}_{\leqslant'}(f)$ von $\mathrm{LM}_{\leqslant'}(g^*)$ geteilt wird. Sei also $f \in I^*$ homogen vom Grad d, $f \neq 0$, dann hat f die Gestalt

$$f = \sum_{i=0}^{d} x_0^{d-i} f_i^*,$$

mit $f_i \in I$ und $\deg(f_i) = i$ (oder $f_i = 0$), für $i = 0, \dots, d$. Sei i der größte Index mit $f_i \neq 0$. Es folgt

$$\mathrm{LM}_{\leqslant'}(f) = \mathrm{LM}_{\leqslant'}(x_0^{d-i} f_i^*) = x_0^{d-i} \mathrm{LM}_{\leqslant}(f_i).$$

Da G eine Gröbnerbasis von I ist, gibt es dann $g \in G$ derart, dass $\mathrm{LM}_{\leqslant}(f_i)$ von $\mathrm{LM}_{\leqslant}(g)$ geteilt wird. Also wird $\mathrm{LM}_{\leqslant'}(f)$ von $\mathrm{LM}_{\leqslant'}(g^*)$ geteilt und die Behauptung folgt. ∎

Übungen

Übung 3.18. Beweisen Sie Prop. 3.17.

Übung 3.19. Zeigen Sie: Für $f \in k[x_1, \dots, x_n]$ gilt $\langle f \rangle^* = \langle f^* \rangle$.

Übung 3.20. Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät, $X \subset \mathbb{P}^n$ ihr projektiver Abschluss. Für $f \in k[x_1, \dots, x_n]$ mit $\deg(f) = d$ bezeichne $\mathrm{LF}(f) = f_d$ den homogenen Teil vom höchsten Grad, die **Leitform** von f. Zeigen Sie:

$$\mathcal{I}_+(V_\infty) = \langle \mathrm{LF}(f) \colon f \in \mathcal{I}(V) \rangle.$$

Übung 3.21. Bestimmen Sie die unendlich-fernen Punkte von Kreis, Parabel und Hyperbel in der Ebene.

Übung 3.22. (a) Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät. Zeigen Sie, dass V genau dann irreduzibel ist, wenn der projektive Abschluss von V in $\mathbb{P}^n$ irreduzibel ist.

(b) Sei $X \subset \mathbb{P}^n$ eine irreduzible projektive k-Varietät. Zeigen Sie: Ist X irreduzibel und $X \not\subset \mathcal{V}_+(x_0)$, so ist auch $X \cap D_0$ irreduzibel.

Übung 3.23. Es seien $A, B \in \mathrm{Mat}_{n\times n}(k)$ zwei Matrizen und setze

$$L_i = \{(a_{i1}t + b_{i1}, \dots, a_{in}t + b_{in}) \colon t \in K\} \subset \mathbb{A}^n.$$

Die Mengen $L_1, \dots, L_n$ sind parametrisierte Geraden in $\mathbb{A}^n$. Betrachte die Inklusion $\mathbb{A}^n = D_0 \subset \mathbb{P}^n$ und sei $\overline{L_i}$ der projektive Abschluss von L_i. Zeige, dass die Schnitpunkte $L_i \cap \mathcal{V}_+(x_0)$ mit der Hyperebene im Unendlichen genau dann projektiv unabhängig sind, wenn die Matrix A invertierbar ist.

3.5. Abbildungen zwischen projektiven Varietäten

Es sei $X \subset \mathbb{P}^m$ eine projektive Varietät. Ähnlich wie bei affinen Varietäten können wir polynomiale Abbildungen $X \to \mathbb{P}^n$ definieren. Dabei gibt es aber einiges zu beachten. Seien $f_0, \dots, f_n \in k[x_0, \dots, x_m]$ Polynome. Welche Bedingungen müssen die Polynome erfüllen, damit

$$\varphi\colon \begin{cases} X & \to & \mathbb{P}^n \\ p & \mapsto & [f_0(p), \dots, f_n(p)] \end{cases}$$

eine wohldefinierte Abbildung ist? Ist $p = [v]$ für $v \in K^{n+1}$, dann muss $[f_0(v), \dots, f_n(v)] = [f_0(\lambda v), \dots, f_m(\lambda v)]$ für alle $\lambda \in K^\times$ gelten. Das ist der Fall, wenn $f_0, \dots, f_n$ alle homogen vom selben Grad d sind. Denn dann gilt

$$[f_0(\lambda v), \dots, f_n(\lambda v)] = [\lambda^d f_0(v), \dots, \lambda^d f_n(v)] = [f_0(v), \dots, f_n(v)].$$

Da außerdem nicht alle homogenen Koordinaten eines Punkts gleichzeitig Null sein können, dürfen $f_0, \dots, f_n$ nicht gleichzeitig auf X verschwinden. Zusammengefasst muss also gelten:

(1) $f_0, \dots, f_n$ sind alle homogen vom selben Grad;
(2) $\mathcal{V}_+(f_0, \dots, f_n) \cap X = \varnothing$.

Sind diese beiden Bedingungen erfüllt, dann ist φ wohldefiniert. Ist $Y \subset \mathbb{P}^n$ eine projektive Varietät mit $\varphi(X) \subset Y$, dann können wir φ wieder als Abbildung

$$\varphi\colon X \to Y$$

auffassen. Wie im Affinen ist jede solche Abbildung ein *Morphismus von projektiven k-Varietäten*. Im Unterschied zum Affinen ist dies aber nicht die *Definition*, sondern nur ein Spezialfall. Wir werden später sehen, warum das so ist. Einen Morphismus, der in dieser Weise definiert ist, nennen wir eine **globale Polynomabbildung**[14] zwischen projektiven k-Varietäten.

Beispiel 3.24. Betrachte die Abbildung

$$\varphi\colon \mathbb{P}^1 \to \mathbb{P}^3, [x, y] \mapsto [x^3, x^2y, xy^2, y^3].$$

Die angegebenen Polynome sind homogen vom Grad 3 und verschwinden nicht gleichzeitig auf $\mathbb{P}^1$, so dass φ eine globale Polynomabbildung ist. Das Bild $C = \varphi(\mathbb{P}^1)$ heißt die **verdrehte Kubik in** $\mathbb{P}^3$. Der Schnitt von C mit $D_0 \cong \mathbb{A}^3$ ist genau die verdrehte Kubik in $\mathbb{A}^3$. Die verdrehte Kubik ist eine projektive Varietät, es gilt nämlich

$$C = \mathcal{V}_+(f_0, f_1, f_2), \quad \text{mit} \quad \begin{cases} f_0 = z_0z_2 - z_1^2, \\ f_1 = z_0z_3 - z_1z_2, \\ f_2 = z_1z_3 - z_2^2. \end{cases}$$

Die Kurve ist also der Durchschnitt von drei Quadriken in $\mathbb{P}^3$. Man kann aber keine der drei Gleichungen f_0, f_1, f_2 weglassen. Das ist aus folgendem Grund bemerkenswert: C ist eine Kurve in $\mathbb{P}^3$, hat also die Dimension 1 (auch wenn wir die Dimension immer noch nicht formal definiert haben). Jede Gerade in $\mathbb{P}^3$ ist der Durchschnitt von zwei Ebenen. Man könnte deshalb erwarten, dass jede Kurve in $\mathbb{P}^3$ der Durchschnitt von zwei Flächen ist. Die verdrehte Kubik ist aber minimal als Durchschnitt von drei Flächen gegeben.

Allgemeiner ist die **rationale Normalkurve in** $\mathbb{P}^n$ das Bild der globalen Polynomabbildung

$$\varphi\colon \mathbb{P}^1 \to \mathbb{P}^n, [x, y] \mapsto [x^n, x^{n-1}y, \dots, xy^{n-1}, y^n].$$

Das alles werden wir in den Übungen genauer betrachten (Übungen 3.24 und 3.25).

Niemand sagt, dass Abbildungen überall definiert sein müssen. Es sei $X \subset \mathbb{P}^m$ eine irreduzible projektive k-Varietät und seien $f_0, \dots, f_n \in k[x_0, \dots, x_m]$ Polynome mit folgenden Eigenschaften:

(1) $f_0, \dots, f_m$ sind homogen vom selben Grad;
(2) X ist nicht in $\mathcal{V}_+(f_0, \dots, f_n)$ enthalten.

Dann heißt die Zuordnung

$$\varphi\colon \begin{cases} X & \dashrightarrow & \mathbb{P}^n \\ p & \mapsto & [f_0(p), \dots, f_n(p)] \end{cases}$$

[14] Diese Terminologie ist nicht sehr üblich. Wir verwenden sie nur übergangsweise, bis zur allgemeinen Definition eines Morphismus.

eine **lokale Polynomabbildung** [15] von X nach $\mathbb{P}^n$ (über k). Sie ist als Abbildung nur in den Punkten $p \in X \setminus \mathcal{V}_+(f_0, \ldots, f_n)$ definiert, was durch den gestrichelten Pfeil angedeutet wird. Bedingung (2) stellt sicher, dass es solche Punkte überhaupt gibt. Das **Bild** einer lokalen Polynomabbildung ist definiert als $\varphi(X \setminus \mathcal{V}_+(f_0, \ldots, f_n))$. Falls das Bild in einer Varietät $Y \subset \mathbb{P}^n$ enthalten ist, dann fassen wir φ wieder als lokale Polynomabbildung zwischen X und Y auf und schreiben

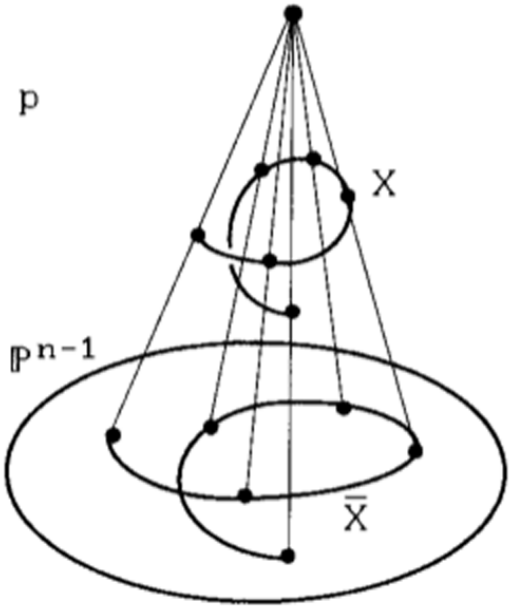
$$\varphi\colon X \dashrightarrow Y.$$

Das wichtigste Beispiel für eine lokale Polynomabbildung ist die Projektion $\pi_p\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$ von $\mathbb{P}^n$ mit Zentrum p. Wie wir gesehen haben, ist die Projektion im Zentrum p selbst undefiniert. Für $p = [1, 0, \ldots, 0]$ ist sie als lokale Polynomabbildung durch

$$\pi_p[x_0, \ldots, x_n] = [x_1, \ldots, x_n]$$

gegeben. Dabei gilt $p = \mathcal{V}_+(x_1, \ldots, x_n)$, was bestätigt, dass π_p genau im Zentrum undefiniert ist.

Sei weiterhin $p = [1, 0, \ldots, 0]$ und sei $X \subset \mathbb{P}^n$ eine irreduzible projektive k-Varietät. Falls $p \in X$, aber nicht $X = \{p\}$, so ist die Einschränkung der Projektion π_p auf X eine lokale Polynomabbildung $\pi_p\colon X \dashrightarrow \mathbb{P}^{n-1}$. Falls $p \notin X$, dann ist $\pi_p\colon X \to \mathbb{P}^{n-1}$ sogar eine globale Polynomabbildung. Indem wir $\mathbb{P}^{n-1}$ mit $H = \mathcal{V}_+(x_0)$ identifizieren, können wir π_p wie zuvor geometrisch interpretieren: Das Bild eines Punktes $q \in X$ unter π_p ist der Schnittpunkt der Gerade $\overline{pq}$ mit H.



Projektion einer Raumkurve in die Ebene. *Bildquelle:* [Harris], S. 35

[15] Auch diese Terminologie ist nur provisorisch und wird später durch den Begriff der rationalen Abbildung abgelöst.

Übungen

Übung 3.24. Es sei $C \subset \mathbb{P}^3$ die verdrehte Kubik, das Bild der Abbildung $\mathbb{P}^1 \to \mathbb{P}^3, [x, y] \mapsto [x^3, x^2y, xy^2, y^3]$.

(a) Es seien $f_0 = z_0z_2 - z_1^2$, $f_1 = z_0z_3 - z_1z_2$, $f_2 = z_1z_3 - z_2^2$. Beweisen Sie, dass $C = \mathcal{V}(f_0, f_1, f_2)$ gilt.
(b) Zeigen Sie, dass das Verschwindungsideal $\mathcal{I}_+(C)$ von f_0, f_1, f_2 erzeugt wird. (*Vorschlag:* Macaulay2)
(c) Beweisen Sie, dass C in keiner Ebene in $\mathbb{P}^3$ enthalten ist.
(d) Bestimmen Sie die Varietät $\mathcal{V}_+(f_0, f_1)$.
(e) Zeigen Sie, dass $\mathcal{I}_+(C)$ nicht von zwei Elementen erzeugt wird. (*Hinweis:* Welche linearen und quadratischen Polynome liegen in $\mathcal{I}_+(C)$?)
(f) Es seien

$$g_1 = z_0z_2 - z_1^2 \quad \text{und} \quad g_2 = z_2(z_1z_3 - z_2^2) - z_3(z_0z_3 - z_1z_2).$$

Zeigen Sie, dass $\mathcal{V}_+(g_1, g_2) = C$ gilt. Erklären Sie den Zusammenhang mit (e).

Übung 3.25. Es sei $C \subset \mathbb{P}^n$ die rationale Normalkurve, also das Bild der Abbildung

$$\varphi\colon \mathbb{P}^1 \to \mathbb{P}^n, [x, y] \mapsto [x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n].$$

(a) Bestimmen Sie quadratische Formen, die C definieren.
(b) Zeigen Sie: Jede Menge von $d + 1$ verschiedenen Punkten auf C ist projektiv unabhängig (also ein homogenes Koordinatensystem). (*Hinweis:* Vandermonde-Matrizen)
(c) Sei m eine natürliche Zahl, $1 \leqslant m \leqslant n-1$. Zeigen Sie, dass C genau die Menge der Punkte $[a_0, \ldots, a_n] \in \mathbb{P}^n$ ist, für welche die $(n - m + 1) \times (m + 1)$-matrix

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdot & a_{m-1} & a_m \\ a_1 & a_2 & \cdot & \cdot & \cdot & a_{m+1} \\ a_2 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & a_{n-1} \\ a_{n-m} & \cdot & \cdot & \cdot & a_{n-1} & a_n \end{bmatrix}$$

den Rang 1 hat.

Übung 3.26. Berechnen Sie das Bild der verdrehten Kubik $C \subset \mathbb{P}^3$ unter den Projektionen mit den folgenden Zentren $p \in \mathbb{P}^3$: (a) $p = [1, 0, 0, 1]$; (b) $p = [0, 1, 0, 0]$; (c) $p = [1, 0, 0, 0]$.
(Projiziert wird auf das orthogonale Komplement des Zentrums, in (a) z.B. auf die Ebene $\mathcal{V}_+(x_0 + x_3)$.)
Was passiert mit der Projektion $C \dashrightarrow \mathbb{P}^2$ im Zentrum p?

Übung 3.27. Es seien S und T zwei graduierte k-Algebren. Ein Homomorphismus $\alpha\colon S \to T$ von k-Algebren heißt **homogen vom Grad** d, wenn $\alpha(S_e) \subset T_{e+d}$ für alle $e \geqslant 0$ gilt.

Zeigen Sie: Sind $X \subset \mathbb{P}^m$ und $Y \subset \mathbb{P}^n$ zwei projektive k-Varietäten und ist $\varphi\colon X \to Y$ eine globale Polynomabbildung, dann induziert φ einen homogenen Homomorphismus $k_+[Y] \to k_+[X]$ von graduierten k-Algebren. Wie sieht es mit der Umkehrung aus?

Übung 3.28*. Es sei C die verdrehte Kubik in $\mathbb{P}^3$ und $\widehat{C} \subset \mathbb{A}^4$ der affine Kegel über C. Zeigen Sie, dass C nicht zu $\mathbb{A}^2$ isomorph ist. (*Vorschlag:* Zeigen Sie, dass der Koordinatenring $k[\widehat{C}] = k[z_0, z_1, z_2, z_3]/\mathcal{I}_+(\widehat{C})$ nicht zu $k[x, y]$ isomorph ist. Betrachten Sie dazu $M = \langle z_0, z_1, z_2, z_3 \rangle \subset k[\widehat{C}]$ und bestimmen Sie M/M^2.)

3.6. Ebene Kurven und der Satz von Bézout

Im ersten Kapitel haben wir die irreduziblen k-Varietäten in der affinen Ebene bestimmt (Satz 1.20). Diese Klassifikation überträgt sich auf die projektive Ebene. Eine **ebene projektive Kurve** ist eine Hyperfläche in $\mathbb{P}^2$, also von der Form $\mathcal{V}_+(f)$ für ein reduziertes homogenes Polynom $f \in k[x_0, x_1, x_2]$, $f \notin k$. Der **Grad** der Kurve $\mathcal{V}_+(f)$ ist der Totalgrad von f. Wie in der affinen Ebene sind die Kurven die einzigen echten, unendlichen k-Varietäten in $\mathbb{P}^2$.

Satz 3.25. *Es sei X eine irreduzible projektive k-Varietät in der Ebene $\mathbb{P}^2$. Dann tritt genau einer der folgenden drei Fälle ein:*

(1) X enthält höchstens endlich viele Punkte;

(2) $X = \mathbb{P}^2$;

(3) X ist eine Kurve in $\mathbb{P}^2$.

Beweis. Falls X endlich ist, sind wir im ersten Fall. Falls X unendlich ist, dann ist auch einer der affinen Teile $X \cap D_i$ ($i = 0, 1, 2$) unendlich. Durch Vertauschen der Koordinaten können wir annehmen, dass $X \cap D_0$ unendlich ist. Falls $X \cap D_0 = D_0$, so folgt $X = \mathbb{P}^2$. Andernfalls ist $X \cap D_0$ nach Satz 1.20 eine affine Kurve, es gibt also ein irreduzibles, nicht-konstantes Polynom $f \in k[x_1, \ldots, x_n]$ derart, dass $X \cap D_0 = \mathcal{V}(f)$ (beachte Übung 3.22). Der projektive Abschluss $\mathcal{V}_+(f^*)$ von $\mathcal{V}(f)$ ist dann in X enthalten und da X irreduzibel ist, folgt $X = \mathcal{V}_+(f^*)$. ∎

Satz 3.26 (Satz von Bézout[16])**.** *Seien X und Y zwei Kurven in $\mathbb{P}^2$ vom Grad d bzw. e, ohne gemeinsame irreduzible Komponenten. Dann ist $X \cap Y$ nicht leer und besteht aus höchstens $d \cdot e$ Punkten.*

Beweis. Es sei $X = \mathcal{V}_+(f)$ und $Y = \mathcal{V}_+(g)$, mit $f, g \in k[x_0, x_1, x_2]$ homogen, $\deg(f) = d$, $\deg(g) = e$. Aus Satz 3.25 wissen wir bereits, dass $X \cap Y$ nur endlich viele Punkte enthalten kann, wenn f und g teilerfremd sind. Wir können $k = K$ annehmen, da dies auf die Aussage keinen Einfluss hat. Da K ein unendlicher Körper ist, gibt es einen Punkt $p_0 \in \mathbb{P}^2$, der folgende Bedingung erfüllt:

(∗) Der Punkt p_0 liegt nicht auf X oder Y und auch nicht auf einer der endlich vielen Verbindungsgeraden $\overline{pq}$, für $p, q \in X \cap Y$, $p \neq q$.

Durch einen projektiven Koordinatenwechsel können wir $p_0 = [1, 0, 0]$ erreichen.

Betrachte die Resultante $\mathrm{Res}(f, g)$ von f und g bezüglich der Variablen x_0. Aufgrund der Struktur der Sylvestermatrix ist $\mathrm{Res}(f, g)$ eine binäre Form vom Grad de in x_1, x_2 (siehe Übung 3.29). Nach Satz 3.19 hat $\mathrm{Res}(f, g)$ also mindestens eine und höchstens de verschiedene Nullstellen. Wir behaupten, dass diese Nullstellen mit $X \cap Y$ in Bijektion stehen. Denn ist $[a_1, a_2] \in \mathbb{P}^1$ mit $\mathrm{Res}(f, g)(a_1, a_2) = 0$, dann bedeutet das nach Kor. 3.20, dass $f(x_0, a_1, a_2)$ und $g(x_0, a_1, a_2)$ eine gemeinsame Nullstelle a_0 haben. Mit anderen Worten, es gilt dann $[a_0, a_1, a_2] \in X \cap Y$. Nach Wahl von p_0 kann zur Nullstelle $[a_1, a_2]$ nicht mehr als ein Schnittpunkt von X und Y korrespondieren. Umgekehrt gelangt man genauso von einem Schnittpunkt von X und Y zu einer Nullstelle von $\mathrm{Res}(f, g)$. Damit ist der Satz bewiesen. ∎

Korollar 3.27. *Je zwei unendliche projektive k-Varietäten in $\mathbb{P}^2$ haben einen gemeinsamen Punkt.*

[16] Étienne Bézout (1730–1783), französischer Mathematiker

Beweis. Nach Satz 3.25 enthält jede unendliche projektive k-Varietät in $\mathbb{P}^2$ eine projektive Kurve. Nach dem Satz von Bézout haben je zwei Kurven in $\mathbb{P}^2$ einen Schnittpunkt. ∎

Die obige Version des Satzes ist nur eine schwache Form, weil sie Vielfachheiten von Schnittpunkten nicht berücksichtigt. Ist z.B. $X = \mathcal{V}_+(x_0x_1 - x_2^2)$ und $Y = \mathcal{V}_+(x_1)$, so besteht $X \cap Y$ nur aus dem einen Punkt $[1,0,0]$. Die Gerade Y ist aber in diesem Punkt an die Konik X tangential, deshalb sollte der Schnittpunkt doppelt gezählt werden.

Im Allgemeinen kann man das folgendermaßen tun: Seien $f, g \in k[x_0, x_1, x_2]$ zwei homogene Polynome ohne gemeinsame irreduzible Faktoren mit $\deg(f) = d$ und $\deg(g) = e$ und sei $\mathrm{Res}(f,g)$ die Resultante von f und g bezüglich x_0. Seien $X = \mathcal{V}_+(f)$ und $Y = \mathcal{V}_+(g)$ die zugehörigen Kurven. Angenommen für den Punkt $p_0 = [1,0,0]$ ist die Bedingung $(*)$ aus dem Beweis des Satzes von Bézout erfüllt. Andernfalls wechseln wir die Koordinaten so, dass die Bedingung erfüllt ist. Wie gerade gezeigt gibt es dann eine Bijektion zwischen den Nullstellen von $\mathrm{Res}(f,g)$ und den Schnittpunkten von X und Y.

Es sei $p \in X \cap Y$. Definiere die **Schnittmultiplizität** $I_p(f,g)$ von f und g in p als die Vielfachheit der zugehörigen Nullstelle von $\mathrm{Res}(f,g)$. Das Problem mit dieser Definition der Schnittmultiplizität ist, dass wir im allgemeinen einen Koordinatenwechsel brauchen, um die Bedingung $(*)$ herzustellen, und wir wissen nicht, dass die Schnittmultiplizität von diesem Koordinatenwechsel unabhängig ist. (Mit anderen Worten, wir müssen beweisen, dass die Schnittmultiplizität unabhängig von der Wahl des Punktes p_0 mit der Eigenschaft $(*)$ ist.) Diesen Schritt lassen wir hier aus; siehe [Cox-Little-O'Shea], §8.7, Lemma 11, für einen direkten Beweis.

Wenn wir die Wohldefiniertheit der Schnittmultiplizität als gegeben voraussetzen, erhalten wir die folgende Verstärkung:

Satz 3.28 (Satz von Bézout — starke Form)**.** *Seien $f, g \in k[x_0, x_1, x_2]$ zwei homogene Polynome ohne gemeinsame irreduzible Faktoren mit $\deg(f) = d$ und $\deg(g) = e$ und seien $X = \mathcal{V}_+(f)$ und $Y = \mathcal{V}_+(g)$ die zugehörigen ebenen projektiven Kurven. Dann gilt*

$$\sum_{p \in X \cap Y} I_P(f,g) = de.$$

Beweis. Dies folgt aus dem, was wir bereits bewiesen haben, zusammen mit der Tatsache, dass die Resultante den Grad de hat und damit genau de Nullstellen mit Vielfachheit. ∎

Bemerkung. Wir haben f und g hier nicht als reduziert vorausgesetzt. Es gilt zum Beispiel $I_{[1,0,0]}(x_1^2, x_2) = 2$ aber $I_{[1,0,0]}(x_1, x_2) = 1$. Nur die zweite Gleichung entspricht der Tatsache, dass sich die beiden Geraden $\mathcal{V}_+(x_1^2) = \mathcal{V}_+(x_1)$ und $\mathcal{V}_+(x_2)$ in $[1,0,0]$ mit Vielfachheit 1 schneiden.

Beispiel 3.29. Hier ein Beispiel aus [Cox-Little-O'Shea] über den Schnitt von zwei Kubiken in $\mathbb{P}^2$, das wir der Bequemlichkeit halber mit Macaulay2 rechnen.

```
i1 : R = QQ[x,y,z];
i2 : f0 = x^3+y^3-2*x*y*z;
i3 : g0 = 2*x^3-4*x^2*y+3*x*y^2+y^3-2*y^2*z;
i4 : r0 = resultant(f0,g0,z)
          4       3 2     2 3       4     5
```

```
o4 = - 4x y + 10x y  - 6x y  - 2x*y  + 2y
```

Die Resultante von zwei Kubiken sollte Grad 9 haben, hier sehen wir aber nur Grad 5. Das liegt daran, dass der Punkt $[0,0,1]$ auf den beiden Kubiken liegt. Also ist die Bedingung $(*)$ verletzt. Versuchen wir es ersatzweise mit dem Punkt $[0,1,0]$. Wir könnten einfach mit der Resultante bezüglich y rechnen. Alternativ können wir die Variablen vertauschen.

```
i5 : phi = map(R,R,{z,x,y})

o5 = map(R,R,{z, x, y})
o5 : RingMap R <--- R

i6 : f = phi(f0);
i7 : g = phi(g0);

i8 : r = resultant(f,g,z)
          9       8       7 2       6 3      5 4
o8 = - 56x  + 104x y + 24x y  - 136x y  + 64x y
```

Diesmal hat die Resultante r den richtigen Grad. Das Beispiel ist so gewählt, dass r über $\mathbb{Q}$ faktorisiert:

```
i9 : factor(r)
         5       3
o9 = (x) (x - y) (7x + 8y)(-8)
o9 : Expression of class Product
```

Die Resultante hat also die drei Nullstellen $[0,1]$, $[1,1]$ und $[-8,7]$ mit Vielfachheiten 5, 3 und 1. Wir setzen diese Werte in f und g ein, um die korrespondierenden Schnittpunkte zu finden.

```
i10 : f1=sub(f,{x=>0,y=>1});
i11 : g1=sub(g,{x=>0,y=>1});
i12 : decompose(ideal(f1,g1))
o12 = {ideal z}

i13 : f2=sub(f,{x=>1,y=>1});
i14 : g2=sub(g,{x=>1,y=>1});
i15 : decompose(ideal(f2,g2))
o15 = {ideal(z - 1)}

i16 : f3=sub(f,{x=>-8,y=>7});
i17 : g3=sub(g,{x=>-8,y=>7});
i18 : decompose(ideal(f3,g3))
o18 = {ideal(z - 4)}
```

Der Befehl `decompose` findet dabei die irreduziblen Komponenten, in diesem Fall die Punkte. Insgesamt erhalten wir die drei Schnittpunkte $[0,0,1]$ (mit Schnittmultiplizität 5), $[1,1,1]$ (mit Multiplizität 3) und $[4,-8,7]$ (mit Multiplizität 1). (Weil wir zu jeder Nullstelle der Resultanten nur einen Schnittpunkt gefunden haben, wissen wir jetzt auch, dass Bedingung $(*)$ diesmal erfüllt ist.)

Natürlich hätten wir das alles in Macaulay2 auch direkt rechnen können.

```
i43 : decompose(ideal(f,g))
```

```
o43 = {ideal (x - z, y - z), ideal (z, x), ideal (x + 2z, 4y - 7z)}
```

Das liefert die drei Punkte sofort, allerdings ohne die Schnittmultiplizitäten. Um diese auch zu sehen, hilft hier der mysteriöse Befehl

```
i44 : distinguishedAndMult(ideal(f,g))
o44 = {{3, ideal(y-z, x-z)}, {5, ideal (z,x)}, {1, ideal (4y-7z, x+2z)}}
```

Übungen

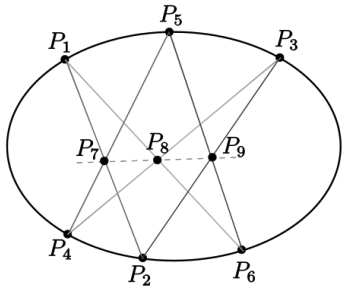
Übung 3.29. Es seien $f, g \in k[x_0, \ldots, x_n]$ Formen vom Grad d bzw. e. Zeigen Sie: Die Resultante $\mathrm{Res}(f, g)$ von f und g bezüglich x_0 ist eine Form vom Grad $d \cdot e$ in $x_1, \ldots, x_n$. (*Vorschlag:* Betrachten Sie die Leibniz-Formel für die Determinante der Sylvester-Matrix.)

Übung 3.30. Verwenden Sie die Methode aus Abschnitt 2.5.4 um einen alternativen Beweis für die Schranke im Satz von Bézout mit Hilfe von Gröbnerbasen zu geben.

Übung 3.31. (**Satz von Pascal**[17] **über das Hexagrammum Mysticum**). Es sei C ein irreduzibler Kegelschnitt in $\mathbb{P}^2$ und seien $p_1, \ldots, p_6$ sechs verschiedene Punkte auf C. Dann liegen die drei Schnittpunkte

$$p_7 = L_1 \cap L_4 \text{ mit } L_1 = \overline{p_1 p_2} \text{ und } L_4 = \overline{p_4 p_5},$$
$$p_8 = L_2 \cap L_5 \text{ mit } L_2 = \overline{p_6 p_1} \text{ und } L_5 = \overline{p_3 p_4},$$
$$p_9 = L_3 \cap L_6 \text{ mit } L_3 = \overline{p_2 p_3} \text{ und } L_6 = \overline{p_5 p_6}$$

von Verbindungsgeraden auf einer Geraden.



Bildquelle: Wikimedia Commons (Ag2gaeh)

Beweisen Sie den Satz nach folgender Skizze: Sei $f \in k[x_0, x_1, x_2]_2$ mit $C = \mathcal{V}_+(f)$. Betrachte die Kubiken

$$X_1 = L_1 \cup L_5 \cup L_6 \qquad \text{und} \qquad X_2 = L_2 \cup L_3 \cup L_4$$

und seien $g_1, g_2 \in k[x_0, x_1, x_2]_3$ mit $X_1 = \mathcal{V}_+(g_1)$, $X_2 = \mathcal{V}_+(g_2)$. Sei $p \in C$, $p \notin \{p_1, \ldots, p_6\}$ und setze

$$g = g_2(p) g_1 - g_1(p) g_2.$$

Zeigen Sie, dass $g \neq 0$, aber $g(p) = g(p_1) = \cdots = g(p_6) = 0$. Schließen Sie mit Hilfe des Satzes von Bézout, dass f ein Teiler von g sein muss und folgern Sie daraus die Aussage des Satzes.

[17] Blaise Pascal (1623–1662), französischer Mathematiker und Universalgelehrter

3.7. Segre- und Veronese-Varietäten

Das Produkt von zwei affinen Räumen ist natürlich wieder ein affiner Raum, denn es gilt $\mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}$. Bei projektiven Räumen ist das nicht so. Zum Beispiel ist $\mathbb{P}^1 \times \mathbb{P}^1$ nicht dasselbe wie $\mathbb{P}^2$. Die homogenen Koordinaten sehen völlig anders aus (vier statt drei). Auch die Geometrie ist tatsächlich verschieden: Zum Beispiel haben in $\mathbb{P}^2$ je zwei unendliche k-Varietäten einen gemeinsamen Punkt (Kor. 3.27). In $\mathbb{P}^1 \times \mathbb{P}^1$ gibt es dagegen die Geraden

$$L_p = \{p\} \times \mathbb{P}^1, \text{ für } p \in \mathbb{P}^1,$$

und es gilt offensichtlich[18] $L_p \cap L_q = \varnothing$ für $p \neq q$. Das Produkt von zwei projektiven Räumen ist also kein projektiver Raum, sondern etwas Neues.

Es gibt zwei Arten mit dem Produkt von projektiven Räumen zu arbeiten. Ein Polynom $f \in k[x_0, \ldots, x_m, y_0, \ldots, y_n]$ heißt **bihomogen vom Bigrad** (d, e), wenn es homogen vom Grad d in $x_0, \ldots, x_m$ und homogen vom Grad e in $y_0, \ldots, y_n$ ist. Ist $T \subset k[x_0, \ldots, x_m, y_0, \ldots, y_n]$ eine endliche Menge von bihomogenen Polynomen (nicht unbedingt vom gleichen Bigrad), dann ist

$$X = \left\{(p, q) \in \mathbb{P}^m \times \mathbb{P}^n \colon f(p, q) = 0 \text{ für alle } f \in T\right\}$$

eine wohldefinierte Teilmenge von $\mathbb{P}^m \times \mathbb{P}^n$, und man kann Untervarietäten des Produkts, die k-Zariski-Topologie auf $\mathbb{P}^m \times \mathbb{P}^n$ usw. in dieser Weise definieren.

Allerdings ist $\mathbb{P}^m \times \mathbb{P}^n$ auch in natürlicher Weise eine projektive k-Varietät, mit Hilfe der folgenden Konstruktion. Betrachte den projektiven Raum

$$\mathbb{P}(\mathrm{Mat}_{(m+1)\times(n+1)}(K)) \cong \mathbb{P}(K^{mn+m+n+1}) = \mathbb{P}^{mn+m+n}$$

aller Matrizen der Größe $(m+1) \times (n+1)$. Das ist ein stinknormaler projektiver Raum, nur mit doppelter Indizierung der Koordinaten. Betrachte weiter die Abbildung

$$\sigma_{m,n} \colon \begin{cases} \mathbb{P}^m \times \mathbb{P}^n & \to & \mathbb{P}^{mn+m+n} \\ ([u], [v]) & \mapsto & [u \cdot v^T] \end{cases}.$$

Dabei ist $u \cdot v^T$ also die $(m+1) \times (n+1)$-Matrix, die als Matrixprodukt des $(m+1)$-Spaltenvektors[19] u mit dem $(n+1)$-Zeilenvektor v^T entsteht. Als Vektor ausgeschrieben sieht das also so aus:

$$\sigma_{m,n}([u], [v]) = \left[u_0 v_0, \ldots, u_0 v_n, u_1 v_0, \ldots, u_1 v_n, \ldots, u_m v_0, \ldots, u_m v_n\right].$$

Die Abbildung $\sigma_{m,n}$ heißt die **Segre-Einbettung**[20] von $\mathbb{P}^m \times \mathbb{P}^n$. Ihr Bild heißt eine **Segre-Varietät** und wird mit $\Sigma_{m,n}$ bezeichnet.

Proposition 3.30. *Die Abbildung $\sigma_{m,n}$ ist injektiv. Ihr Bild $\Sigma_{m,n}$ ist k-abgeschlossen und besteht genau aus allen $(m+1) \times (n+1)$-Matrizen vom Rang* 1.

[18] Nicht offensichtlich ist allenfalls, in welchem Sinn die Teilmengen L_p überhaupt 'Geraden' sind, wenn $\mathbb{P}^1 \times \mathbb{P}^1$ gar keine Ebene ist.

[19] Zwar schreiben wir Punkte die ganze Zeit als Zeilen, aber wenn wir sie als Vektoren interpretieren, sehen wir sie, wie in der linearen Algebra üblich, als Spaltenvektoren.

[20] Corrado Segre (1863–1924), italienischer Mathematiker und Mitbegründer der 'italienischen Schule' der algebraischen Geometrie

Beweis. Dass $\Sigma_{m,n}$ genau aus den Rang-1-Matrizen besteht, ist Übung 3.32. Damit ist $\Sigma_{m,n}$ die projektive k-Varietät, die von allen 2×2-Minoren ausgeschnitten wird (Übung 1.14), d.h. es gilt

$$\Sigma_{m,n} = \mathcal{V}_+\big([z] : z_{ij}z_{kl} - z_{il}z_{kj} = 0 \text{ für } i,k = 0,\dots,m,\ j,l = 0,\dots,n\big).$$

Ist $uv^T = u'v'^T$ mit $u, u' \in K^{m+1}$, $v, v' \in K^{n+1}$, alle $\neq 0$, dann gibt es j mit $v_j, v'_j \neq 0$. Ist $v'_j = \lambda v_j$, $\lambda \in K^\times$, so folgt $uv_j = \lambda u'v_j$ und damit $u = \lambda u'$, also $[u] = [u']$. Genauso folgt $[v] = [v']$. ∎

Mittels der Segre-Einbettung haben wir auch einen neuen Begriff davon, wann eine Teilmenge von $X \subset \mathbb{P}^m \times \mathbb{P}^n$ k-abgeschlossen ist. Dieser passt zum Glück mit der vorigen Beschreibung durch bihomogene Polynome zusammen, wie die folgende Aussage zeigt.

Proposition 3.31. *Sei $X \subset \mathbb{P}^m \times \mathbb{P}^n$ eine Teilmenge. Genau dann ist $\sigma_{m,n}(X) \subset \Sigma_{m,n} \subset \mathbb{P}^{mn+m+n}$ eine projektive k-Varietät, wenn es eine endliche Menge $T \subset k[x_0,\dots,x_m,y_0,\dots,y_n]$ von bihomogenen Polynomen gibt derart, dass*

$$X = \big\{(p,q) \in \mathbb{P}^m \times \mathbb{P}^n : f(p,q) = 0 \text{ für alle } f \in T\big\}.$$

Beweis. Angenommen $\sigma_{m,n}(X)$ ist k-abgeschlossen, d.h. es gibt homogene Polynome $f_1,\dots,f_r \in k[z_{i,j} : i = 0,\dots,m,\ j = 0,\dots,n]$ vom Grad $d_i = \deg(f_i)$ mit $\sigma_{m,n}(X) = \mathcal{V}_+(f_1,\dots,f_r)$. Dann folgt

$$X = \{(p,q) : f_1(\sigma_{m,n}(p,q)) = \cdots = f_r(\sigma_{m,n}(p,q)) = 0\}.$$

Dabei ist $f_i(\sigma_{m,n}(x,y)) \in k[x_0,\dots,x_m,y_0,\dots,y_n]$ bihomogen vom Bigrad (d_i,d_i), für $i = 1,\dots,r$.

Sei umgekehrt $T = \{g_1,\dots,g_r\}$ eine Menge von bihomogenen Polynomen vom Bigrad (d_i,e_i), $i = 1,\dots,r$, die X definiert. Falls $d_i \geqslant e_i$ für ein i, so setze $h_{i,j} = y_j^{d_i-e_i} g_i$ für $j = 0,\dots,n$ und falls $d_i < e_i$, so setze $h_{i,j} = x_j^{e_i-d_i} g_i$ für $j = 0,\dots m$. Dann wird X auch durch die Menge aller $h_{i,j}$ beschrieben und jedes $h_{i,j}$ ist bihomogen vom Bigrad $(d_{i,j},d_{i,j})$. Ersetzt man in $h_{i,j}$ jedes Produkt x_iy_j durch z_{ij} (diese Ersetzung ist nicht eindeutig), so erhält man ein homogenes Polynom $\widetilde{h}_{i,j}$ vom Grad $d_{i,j}$ in $k[z]$ mit $\widetilde{h}_{i,j}(\sigma_{m,n}(x,y)) = h_{i,j}$, so dass $\sigma_{m,n}(X)$ von allen $\widetilde{h}_{i,j}$ definiert wird. ∎

Bemerkung 3.32. Etwas subtiler ist der Zusammenhang zwischen globalen Polynomabbildungen auf $\mathbb{P}^m \times \mathbb{P}^n$ (gegeben durch bihomogene Polynome) und globalen Polynomabbildungen auf $\Sigma_{m,n}$. Wir kommen darauf im nächsten Kapitel zurück.

Die einzigen solchen Abbildungen, die uns im Moment interessieren, sind die Projektionen auf einen der Faktoren, zum Beispiel auf den ersten:

$$\pi : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^m,\ (p,q) \mapsto p.$$

Die Abbildung $\pi \circ \sigma_{m,n}^{-1} : \Sigma_{m,n} \to \mathbb{P}^m$ ist *keine* globale Polynomabbildung (siehe dazu Satz 4.45).

Beispiel 3.33. Die Segre-Varietät $\Sigma_{1,1}$ ist das Bild der Abbildung

$$\sigma_{1,1} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3,\ ([x_0,x_1],[y_0,y_1]) \mapsto [x_0y_0, x_0y_1, x_1y_0, x_1y_1].$$

Sie wird durch eine quadratische Gleichung beschrieben, nämlich

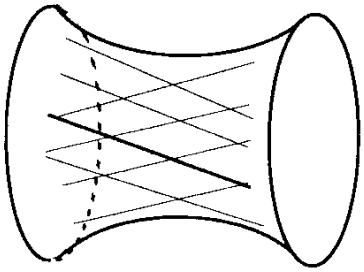
$$\Sigma_{1,1} = \mathcal{V}_+(z_{0,0}z_{1,1} - z_{0,1}z_{1,0}).$$

Die 'Geraden' $L_p = \{p\} \times \mathbb{P}^1$ und $M_p = \mathbb{P}_1 \times \{p\}$ für $p \in \mathbb{P}^1$ entsprechen dabei tatsächlich Geraden auf $\Sigma_{1,1}$. Und zwar wird die Gerade L_p mit $p = [a, b]$ unter $\sigma_{1,1}$ auf die Gerade

$$\mathcal{V}_+(bz_{0,0} - az_{1,0}, bz_{0,1} - az_{1,1})$$

in $\mathbb{P}^3$ abgebildet (und analog für M_p).

Das reelle affine Bild $\Sigma_{1,1} \cap D_+(z_{0,0})$ zeigt ein Hyperboloid (Kühlturm). Die beiden Scharen von Geraden auf dem Hyperboloid sind die genau die Scharen $\{L_p : p \in \mathbb{P}^1\}$ und $\{M_p : p \in \mathbb{P}^1\}$.



Segre-Quadrik $\Sigma_{1,1}$; *Bildquelle:* [Harris], S. 26

Ist $X \subset \mathbb{P}^m$ eine projektive k-Varietät und $\varphi: X \to \mathbb{P}^n$ eine globale Polynomabbildung, dann heißt

$$\Gamma_\varphi = \left\{(p, q) \in \mathbb{P}^m \times \mathbb{P}^n : p \in X,\ q = \varphi(p)\right\}$$

der **Graph von** φ.

Proposition 3.34. *Der Graph einer globalen Polynomabbildung ist k-abgeschlossen.*

Beweis. Es sei $X = \mathcal{V}_+(h_1, \ldots, h_r)$ und $\varphi = (f_0, \ldots, f_n)$ mit homogenen Polynomen $f_0, \ldots, f_n \in k[x_0, \ldots, x_m]$ vom gleichen Grad d. Es gilt $[v] = \varphi([u])$ genau dann, wenn die Zeilen der Matrix

$$\begin{pmatrix} v_0 & v_1 & \cdots & v_n \\ f_0(u) & f_1(u) & \cdots & f_n(u) \end{pmatrix}$$

linear abhängig sind, die Matrix also Rang 1 hat. Setze $g_{i,j} = y_i f_j - y_j f_i$ für $i < j$. Die Polynome $g_{i,j}$ sind bihomogen vom Bigrad $(d, 1)$, die Polynome h_i vom Bigrad $(\deg(h_i), 0)$, und es gilt

$$\Gamma_\varphi = \left\{(p, q) : g_{i,j}(p, q) = 0, h_l(p, q) = 0 \text{ für } 0 \leqslant i < j \leqslant n, l = 1, \ldots, r\right\}.$$

Also ist Γ_φ abgeschlossen, nach Prop. 3.31. ∎

Genauso wichtig wie die Segre-Varietäten sind die Veronese-Varietäten[21]. Der Raum aller Formen vom Grad d in $n+1$ Variablen hat bekanntlich die Dimension

$$N = \binom{n+d}{d}$$

(siehe Übung 2.1). Die **Veronese-Abbildung vom Grad** d ist gegeben durch

$$v_d: \begin{cases} \mathbb{P}^n & \to & \mathbb{P}^{N-1} \\ [x_0, \ldots, x_n] & \mapsto & [x^\alpha : \alpha \in \mathbb{Z}_+^n, |\alpha| = d] \end{cases}.$$

[21] Giuseppe Veronese (1854–1917), italienischer Mathematiker

Die Veronese-Abbildung schickt einen Punkt p also auf die Auswertung aller Monome vom Grad d in p. Damit die Abbildung wohldefiniert ist, muss man sich natürlich auf eine Reihenfolge der Monome festlegen. Wir nehmen die lexikographische Ordnung.

Beispiele 3.35. (1) ($n = 1$, d beliebig) In diesem Fall ist die Veronese-Abbildung also

$$v_d\colon \mathbb{P}^1 \to \mathbb{P}^d, [x_0, x_1] \mapsto [x_0^d, x_0^{d-1}x_1, \ldots, x_0x_1^{d-1}, x_1^d].$$

Das ist gerade die rationale Normalkurve vom Grad d in $\mathbb{P}^d$ (Übung 3.25).

(2) (n beliebig, $d = 2$) Es sei $\mathrm{Sym}_{n+1}(K)$ der Raum aller symmetrischen Matrizen der Größe $n+1$ mit Einträgen in K und

$$\mathbb{P}(\mathrm{Sym}_{n+1}(K)) = \mathbb{P}^{\binom{n+2}{2}-1} = \mathbb{P}^{N-1}$$

Die Veronese-Abbildung v_2 ist dann gerade gegeben durch

$$v_2\colon \begin{cases} \mathbb{P}^n & \to & \mathbb{P}^{N-1} \\ [u] & \mapsto & [u \cdot u^T] \end{cases}.$$

Denn die Einträge der symmetrischen $(n+1) \times (n+1)$-Matrix $u \cdot u^T$ sind ja gerade die quadratischen Monome $(u_iu_j\colon i, j = 0, \ldots, n)$. Deshalb kann man mit der Veronese-Abbildung v_2 ganz ähnlich verfahren, wie mit der Segre-Abbildung. Das Bild von v_2 besteht gerade aus allen symmetrischen Matrizen vom Rang 1 und wird durch die Menge aller symmetrischen 2×2-Minoren definiert (siehe Übung 3.33).

Proposition 3.36. *Die Veronese-Abbildung ist injektiv und ihr Bild ist k-abgeschlossen in* $\mathbb{P}^{N-1}$.

Das Bild $v_d(\mathbb{P}^n)$ heißt die **Veronese-Varietät vom Grad** d **der Dimension** n.

Beweis. Die Veronese-Abbildung ist eine globale Polynomabbildung auf $\mathbb{P}^n$. Wir zeigen im nächsten Abschnitt, dass ihr Bild damit automatisch abgeschlossen ist (Kor. 3.42). Wir geben jetzt aber einen unabhängigen Beweis und bestimmen explizite Gleichungen für die Veronese-Varietät.

Auf $\mathbb{P}^{N-1}$ arbeiten wir mit homogenen Koordinaten z_α, $\alpha \in \Sigma$, $\Sigma = \{\alpha \in \mathbb{Z}_+^{n+1}\colon |\alpha| = d\}$. Wir zeigen, dass das Bild von v_d genau die Varietät

$$Z = \mathcal{V}_+\big(z_\alpha z_\beta - z_\gamma z_\delta : \alpha + \beta = \gamma + \delta, \alpha, \beta, \gamma, \delta \in \Sigma\big).$$

ist. Die Inklusion $v_d(\mathbb{P}^n) \subset Z$ ist klar. Sei umgekehrt $[w] \in Z$. Dann gibt es ein $\alpha \in \Sigma$ mit $w_\alpha \neq 0$. Durch Vertauschen der Indizes können wir annehmen, dass $\alpha_0 > 0$. Falls $\alpha_0 < d$, dann gibt es $\gamma, \delta \in \Sigma$ mit $2\alpha = \gamma + \delta$ und $\gamma_0 > \alpha_0$. Wegen $w_\alpha^2 = w_\gamma w_\delta$ gilt dann $w_\gamma \neq 0$. Wir können also α durch γ ersetzen und schließlich $\alpha = (d, 0, \ldots, 0)$ annehmen. Durch Skalieren von w erreichen wir außerdem $w_\alpha = 1$. Setze

$$u_0 = 1 \qquad \text{und} \qquad u_j = w_{(d-1,0,\ldots,1,\ldots,0)}$$

(wobei auf der rechten Seite die 1 an der Stelle j steht). Dann folgt $v_d([u]) = [w]$. Dasselbe Argument zeigt auch die Injektivität von v_d. ∎

Der Sinn der Veronese-Abbildung besteht darin, dass sie Monome vom Grad d *linearisiert*. Ist $f \in k[x_0, \ldots, x_n]$ homogen vom Grad d, $f = \sum_{|\alpha|=d} c_\alpha x^\alpha$, so gilt per Definition

$$v_d(\mathcal{V}_+(f)) = v_d(\mathbb{P}^n) \cap \mathcal{V}_+\big(\textstyle\sum_{|\alpha|=d} c_\alpha z_\alpha\big).$$

Dabei ist die Gleichung auf der rechten Seite linear in den neuen Variablen z_α. Natürlich linearisiert die Veronese-Abbildung immer in nur einem Grad auf einmal. Das ist aber keine wesentliche Einschränkung, wie die folgende Aussage zeigt.

Proposition 3.37. *Es sei $X = \mathcal{V}_+(f_1, \dots, f_r) \subset \mathbb{P}^n$. Dann gibt es homogene Polynome $g_1, \dots, g_s \in k[x_0, \dots, x_n]$ vom Grad $d = \max\{\deg(f_i) : i = 1, \dots, r\}$ mit $X = \mathcal{V}_+(g_1, \dots, g_s)$.*

Beweis. Ist $d_i = \deg(f_i)$ und $d = \max\{d_i : i = 1, \dots, r\}$, dann setze $g_{ij} = x_j^{d-d_i} f_i$. Die g_{ij} sind homogen vom Grad d und X wird von allen g_{ij} definiert. ∎

Korollar 3.38. *Es sei $X \subset \mathbb{P}^n$ eine projektive k-Varietät. Dann gibt es $d \geqslant 1$ und einen linearen Unterraum L von $\mathbb{P}^{N-1}$, $N = \binom{n+d}{d}$, mit*

$$\nu_d(X) = \nu_d(\mathbb{P}^n) \cap L.$$ ∎

Da die Veronese-Varietät selbst durch quadratische Gleichungen definiert wird (Beweis von Prop. 3.36), erhalten wir als Konsequenz die folgende Aussage.

> Jedes homogene polynomiale Gleichungssystem ist zu einem System aus linearen und quadratischen Gleichungen äquivalent.

Für algorithmische Zwecke ist die Übersetzung in ein solches quadratisch/lineares System meistens nicht sehr effizient, da sowohl die Zahl der Variablen als auch der Gleichungen stark zunimmt. Trotzdem spielt diese Tatsache z.B. für Komplexitätsfragen in der algebraischen Geometrie und auch in der theoretischen Informatik eine Rolle. (Zum Beispiel kann man damit zeigen, dass das Lösen quadratischer Gleichungssysteme in einem gewissen wohldefinierten Sinn nicht wesentlich 'einfacher' sein kann, als das Lösen allgemeiner Systeme.)

Übungen

Übung 3.32. Zeigen Sie: (a) Genau dann hat eine Matrix $A \in \mathrm{Mat}_{m\times n}(K)$ den Rang 1, wenn es $u \in K^m$ und $v \in K^n$, $u, v \neq 0$, gibt derart, dass $A = u \cdot v^T$. (b) Genau dann hat eine symmetrische Matrix $A \in \mathrm{Sym}_n(K)$ den Rang 1, wenn es $u \in K^n$, $u \neq 0$, gibt derart, dass $A = u \cdot u^T$.

Übung 3.33. Zeigen Sie, dass die Veronese-Varietät $\nu_2(\mathbb{P}^n)$ als Teilmenge von $\mathbb{P}(\mathrm{Sym}_{n+1}(K))$ aus den Matrizen vom Rang 1 besteht und damit von allen symmetrischen 2×2-Minoren definiert wird.

Übung 3.34. Es seien L_1, L_2, L_3 drei paarweise disjunkte Geraden in $\mathbb{P}^3$ und sei

$$S = \bigcup \{L \subset \mathbb{P}^3 : L \text{ ist eine Gerade mit } L \cap L_i \neq \varnothing \text{ für } i = 1, 2, 3\}.$$

Zeigen Sie, dass S projektiv äqiuvalent ist zur Segre-Varietät $\Sigma_{1,1}$.

3.8. Der Hauptsatz der Eliminationstheorie

Wir haben uns schon in den ersten beiden Kapiteln mit der Rolle von Eliminationsidealen befasst. Die Elimination einer Variablen aus einem Ideal entspricht der Projektion der Varietät auf die übrigen Variablen. Im allgemeinen ist jedoch die affine Varietät, die durch das Eliminationsideal definiert wird, größer als das Bild der Projektion (Beispiel 1.21(3)): Das Bild der Hyperbel $\mathcal{V}(xy-1)$ in $\mathbb{A}^2$ unter der Projektion auf die erste Koordinate ist $\mathbb{A}^1 \setminus \{0\}$, während das Eliminationsideal $\langle xy-1\rangle \cap k[x] = k[x]$ die ganze affine Gerade definiert. Gleichheit gilt nur unter speziellen Voraussetzungen, so wie in Lemma 1.32. Wenn man dagegen Variablen eliminiert, die nur homogen vorkommen, tritt dieses Problem nicht auf. Das ist der folgende fundamentale Satz.

Satz 3.39. *Es seien $f_1, \dots, f_r \in k[x_0, \dots, x_m, y_1, \dots, y_n]$ Polynome, die homogen in $x_0, \dots, x_m$ sind. Es sei*

$$X = \big\{(p,q) \in \mathbb{P}^m \times \mathbb{A}^n : f_1(p,q) = \cdots = f_r(p,q) = 0\big\}$$

und sei $\pi : \mathbb{P}^m \times \mathbb{A}^n \to \mathbb{A}^n, (p,q) \mapsto q$ die Projektion auf den zweiten Faktor.
Dann ist $\pi(X)$ eine k-abgeschlossene Teilmenge von $\mathbb{A}^n$.

Beweis. Es sei $q \in \mathbb{A}^n$. Genau dann ist $q \in \pi(X)$, wenn

$$\mathcal{V}_+(f_1(x,q), \dots, f_r(x,q)) \neq \varnothing$$

gilt. Nach dem projektiven Nullstellensatz (Kor. 3.13) ist das genau dann der Fall, wenn

$$S_d \not\subset \langle f_1(x,q), \dots, f_r(x,q)\rangle$$

für alle $d \geqslant 1$ gilt, wobei $S = k[x_0, \dots, x_m]$. Für $d \geqslant 1$ sei daher

$$Y_d = \{q \in \mathbb{A}^n : S_d \not\subset \langle f_1(x,q), \dots, f_r(x,q)\rangle\}.$$

Dann gelten $Y_1 \supset Y_2 \supset Y_3 \supset \cdots$ und $\pi(X) = \bigcap_{d\geqslant 1} Y_d$. Deshalb reicht es zu zeigen, dass Y_d für alle hinreichend großen d eine k-abgeschlossene Teilmenge ist.

Es sei d_j der Totalgrad von f_j in den Variablen $x_0, \dots, x_m$ und sei $d \geqslant \max\{d_1, \dots, d_r\}$. Für festes $q \in \mathbb{A}^n$, betrachte die lineare Abbildung

$$\Phi_q : \begin{cases} S_{d-d_1} \times \cdots S_{d-d_r} & \to & S_d \\ (g_1, \dots, g_r) & \mapsto & \sum_{i=1}^r g_i f_i(x,q) \end{cases}$$

Genau dann liegt $q \in Y_d$, wenn Φ_q nicht surjektiv ist, die Abbildung Φ_q also Rang kleiner als $\dim(S_d) = \binom{n+d}{n}$ hat. Schreibt man Φ_q als Matrix bezüglich der Monombasis hin, dann bedeutet das, dass alle Minoren der Größe $\binom{n+d}{n}$ verschwinden (Übung 1.14). Diese Minoren sind Polynome in q, die die Varietät Y_d definieren. Damit ist der Satz bewiesen. ∎

Bemerkung 3.40. Natürlich kann man das Ideal, das die Varietät $\pi(X)$ beschreibt, auch explizit angeben. Ist $I = \langle f_1, \dots, f_r\rangle$, dann heißt

$$\widehat{I} = \big\{f \in k[y_1, \dots, y_n] : \text{Für jedes } i = 0, \dots, n \text{ gibt es } e_i \geqslant 0 \text{ mit } x_i^{e_i} f \in I\big\}$$

das **projektive Eliminationsideal** von I und es gilt $\pi(X) = \mathcal{V}(\widehat{I})$. Wir verzichten hier auf den Beweis (siehe z.B. [Cox-Little-O'Shea, §8, Thm. 6). Wir werden aber gleich zeigen, dass das übliche Eliminationsideal in diesem Kontext der Projektion mit Zentrum entspricht (Kor. 3.43).

Korollar 3.41. *Es sei $X \subset \mathbb{P}^m \times \mathbb{P}^n$ eine k-abgeschlossene Teilmenge und $\pi\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$, $(p, q) \mapsto q$ die Projektion auf den zweiten Faktor. Dann ist $\pi(X)$ eine k-abgeschlossene Teilmenge von $\mathbb{P}^n$.*

Beweis. Nach Prop. 3.31 wird X durch bihomogene Polynome in $k[x_0, \dots, x_m, y_0, \dots, y_n]$ definiert. Betrachte die durch die gleichen Polynome definierte Varietät $\widehat{X} \subset \mathbb{P}^m \times \mathbb{A}^{n+1}$. Nach dem Hauptsatz der Eliminationstheorie ist dann $\pi(\widehat{X})$ abgeschlossen in $\mathbb{A}^{n+1}$. Diese Varietät ist genau der affine Kegel über $\widehat{\pi(X)}$. ∎

Korollar 3.42. *Es sei $X \subset \mathbb{P}^m$ eine projektive k-Varietät und $\varphi\colon X \to \mathbb{P}^n$ eine globale Polynomabbildung. Dann ist das Bild $\varphi(X)$ wieder eine projektive k-Varietät.*

Beweis. Nach Prop. 3.34 ist der Graph $\Gamma_\varphi \subset \mathbb{P}^m \times \mathbb{P}^n$ eine k-abgeschlossene Teilmenge. Das Bild $\varphi(X)$ ist die Projektion von Γ_φ auf $\mathbb{P}^n$ und damit abgeschlossen nach Kor. 3.41. ∎

Korollar 3.43. *Es sei $p = [1, 0, \dots, 0] \in \mathbb{P}^n$. Sei $I \subset k[x_0, \dots, x_n]$ ein homogenes Ideal und $X = \mathcal{V}_+(I)$. Es gelte $p \notin X$. Dann ist $\pi_p(X)$ wieder eine projektive k-Varietät, nämlich*

$$\pi_p(X) = \mathcal{V}_+(I \cap k[x_1, \dots, x_n]).$$

Beweis. Wegen $p \notin X$ ist $\pi_p\colon X \to \mathbb{P}^{n-1}$ eine globale Polynomabbildung. Deshalb ist das Bild $\pi_p(X)$ eine k-abgeschlossene Teilmenge von $\mathbb{P}^{n-1}$. Sei $J = I \cap k[x_1, \dots, x_n]$. Die Inklusion $\pi_p(X) \subset \mathcal{V}_+(J)$ ist leicht zu sehen: Sei $q = [a_1, \dots, a_n] \in \pi_p(X)$, dann gibt es also $a_0 \in K$ mit $[a_0, \dots, a_n] \in X$. Ist $f \in I \cap k[x_1, \dots, x_n]$, dann gilt also $f(a_0, \dots, a_n) = f(a_1, \dots, a_n) = 0$ und damit $q \in \mathcal{V}_+(J)$. Die umgekehrte Inklusion zeigen wir genauso wie in Satz 1.42: Ist $r \notin \pi_p(X)$, dann gibt es also $f \in k[x_1, \dots, x_n]$ mit $f(\pi_p(q)) = 0$ für alle $q \in X$, aber $f(r) \neq 0$, weil $\pi_p(X)$ eine k-abgeschlossene Menge ist. Nach dem projektiven Nullstellensatz gibt es $m \geqslant 1$ mit $f^m \in I$. Also gilt $f^m(r) \neq 0$ und $f^m \in I \cap k[x_1, \dots, x_n]$ und damit $r \notin \mathcal{V}_+(I \cap k[x_1, \dots, x_n])$. ∎

Beispiel 3.44. Um auf das Beispiel der Hyperbel zurückzukommen: Das Bild der affinen Kurve $C = \mathcal{V}(1 - x_1x_2)$ unter der Projektion $(x_1, x_2) \mapsto x_1$ ist nicht abgeschlossen. Der projektive Abschluss von C ist $\overline{C} = \mathcal{V}_+(x_0^2 - x_1x_2)$ und die Projektion entspricht der Projektion $[x_0, x_1, x_2] \mapsto [x_0, x_1]$ mit Zentrum $[0, 0, 1]$. Dieses Zentrum liegt allerdings auf $\overline{C}$, so dass Kor. 3.43 nicht anwendbar ist. Projiziert man $\overline{C}$ von einem anderen Punkt, der nicht auf $\overline{C}$ liegt, zum Beispiel $[1, 0, 0]$, so ist die Projektion auf $\mathbb{P}^1$ surjektiv.

Übungen

Übung 3.35. Führen Sie Satz 3.43 im Fall $k = K$ auf Lemma 1.32 zurück (oder imitieren Sie den Beweis des Lemmas) und geben Sie dadurch einen alternativen Beweis.

Übung 3.36. Es sei $C \subset \mathbb{P}^n$ die rationale Normalkurve und sei $p = [1, 0, \ldots, 0] \in C$. Zeigen, Sie dass $\overline{\pi_p(C \smallsetminus \{p\})}$ eine rationale Normalkurve in $\mathbb{P}^{n-1}$ ist. Was fällt auf? Vergleichen Sie das Ergebnis im Fall der verdrehten Kubik ($n = 3$) mit Übung 3.26.

Übung 3.37*. Es sei $\nu\colon \mathbb{P}^1 \to \mathbb{P}^2$ die quadratische Veronese-Abbildung und $\sigma\colon \mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^5$ die Segre-Abbildung. Es sei $\mathrm{id} \times \nu\colon \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^2$, $(p, q) \mapsto (p, \nu(q))$. Setze $\varphi = \sigma\colon (\mathrm{id} \times \nu)$ und $X = \varphi(\mathbb{P}^1 \times \mathbb{P}^1)$.
(a) Bestimmen Sie Gleichungen für X.
(b) Finden Sie eine Hyperebene $H \subset \mathbb{P}^5$ so, dass $H \cap X \subset \mathbb{P}^4$ eine rationale Normalkurve vom Grad 4 ist.

3.9. Die Primärzerlegung

In einem faktoriellen Ring R ist jedes Element $f \in R$ ein Produkt $f = f_1^{i_1} \cdots f_r^{i_r}$ von irreduziblen Elementen mit $f_i \nsim f_j$ für $i \neq j$. Für die erzeugten Ideale bedeutet das gerade

$$\langle f \rangle = \langle f_1 \rangle^{i_1} \cap \cdots \cap \langle f_r \rangle^{i_r}.$$

Für allgemeine Ideale ist das aber nicht der Fall, nicht in faktoriellen Ringen und in allgemeineren Ringen schon erst recht nicht. Für die algebraische Geometrie hängen solche Zerlegungen von Idealen mit der Zerlegung einer Varietät in ihre irreduziblen Komponenten zusammen. Wir brauchen zunächst einige algebraische Grundlagen.

Proposition 3.45. *Es sei R ein Ring. Ein Ideal von R ist genau dann ein Durchschnitt von Primidealen, wenn es ein Radikalideal ist.*

Beweis. Wir betrachten den Fall $R = k[x_1, \ldots, x_n]$. Ist I ein Radikalideal und $V = \mathcal{V}(I) \subset \mathbb{A}^n$ die zugehörige affine Varietät mit irreduziblen Komponenten $V = V_1 \cup \cdots \cup V_r$, so folgt $I = \mathcal{I}(V) = \mathcal{I}(V_1) \cap \cdots \cap \mathcal{I}(V_r)$. Dabei sind die $\mathcal{I}(V_i)$ Primideale, weil die V_i irreduzibel sind.

Der Beweis der allgemeinen Aussage ist Übung 3.40. ∎

Gegeben ein Ideal I im Polynomring, dann können wir also das Radikalideal $\sqrt{I}$ als einen Durchschnitt von Primidealen ausdrücken und dies entspricht gerade der Zerlegung von $\mathcal{V}(I)$ in irreduzible Komponenten. Was aber, wenn man I selbst statt $\sqrt{I}$ zerlegen möchte?

Beispiel 3.46. Es sei $I = \langle x^2, xy \rangle \subset k[x, y]$. Wegen $x^2 \in I$, $x \notin I$, ist I offenbar kein Radikalideal. Außerdem ist das einzige Primideal, das I enthält, das maximale Ideal $M = \langle x, y \rangle$. Aber $M^2 = \langle x^2, xy, x^2 \rangle$ ist immer noch größer als I, während $M^3 = \langle x^3, x^2y, xy^2, y^3 \rangle$ kleiner als I ist. Also kann I nicht als ein Durchschnitt von Potenzen von Primidealen geschrieben werden.

Statt nur Potenzen von Primidealen braucht man den folgenden allgemeineren Typ von Idealen:

Definition 3.47. Ein Ideal J in einem Ring R heißt **primär**, wenn $J \neq R$ und für alle $f, g \in R$ gilt:

$$fg \in J \quad \Longrightarrow \quad f \in J \text{ oder } g \in \sqrt{J}.$$

Beispiele 3.48. (1) Ist R ein faktorieller Ring und $f \in R$ ein irreduzibles Element, dann ist $\langle f \rangle^m = \langle f^m \rangle$ für jedes $m \geqslant 1$ ein primäres Ideal. Denn falls $gh \in \langle f^m \rangle$, so folgt entweder $f^m | h$ und damit $h \in \langle f^m \rangle$ oder $f | g$ und damit $g \in \langle f \rangle = \sqrt{\langle f^m \rangle}$. (In allgemeinen Ringen ist dagegen nicht jede Potenz eines Primideals primär.)

(2) Das Ideal $\langle x^2, y\rangle \subset k[x, y]$ ist primär, aber nicht Potenz eines Primideals (Übung).

Lemma 3.49. *Das Radikal eines primären Ideals ist prim.*

Beweis. Sind $f, g \in R$ mit $fg \in \sqrt{J}$ so bedeutet dies $f^m g^m \in J$ für ein $m \geqslant 1$ und damit $f^m \in J$ oder $g^m \in \sqrt{J}$, also $f \in \sqrt{J}$ oder $g \in \sqrt{\sqrt{J}} = \sqrt{J}$. ∎

Eine **Primärzerlegung** eines Ideals I ist eine Darstellung

$$I = I_1 \cap \cdots I_r$$

von I als Durchschnitt von primären Idealen.
Ein Ideal I von R heißt **irreduzibel**, wenn für alle Ideale J_1, J_2 von R gilt

$$I = J_1 \cap J_2 \qquad \Longrightarrow \qquad I = J_1 \text{ oder } I = J_2.$$

Dieser Begriff verallgemeinert offensichtlich die Irreduzibilität eines Elements.

Lemma 3.50. *In einem noetherschen Ring ist jedes irreduzible Ideal primär.*

Beweis. Es sei R ein noetherscher Ring und I ein irreduzibles Ideal in R. Dann ist das Nullideal in R/I irreduzibel. Außerdem ist I genau dann primär, wenn das Nullideal in R/I primär ist (Übung 3.38). Es genügt daher, die Behauptung für das Nullideal zu beweisen. Angenommen also $\langle 0\rangle$ ist in R irreduzibel. Seien $f, g \in R$ mit $fg = 0$ und $g \neq 0$. Für jedes $m \geqslant 1$ betrachte das Ideal

$$\operatorname{Ann}(f^m) = \{h \in R \colon hf^m = 0\}.$$

Dann ist $\operatorname{Ann}(f) \subset \operatorname{Ann}(f^2) \subset \cdots$ eine aufsteigende Kette von Idealen in R. Da R noethersch ist, wird diese Kette stationär, d.h. es gibt $n \geqslant 1$ mit $\operatorname{Ann}(f^{n+1}) = \operatorname{Ann}(f^n)$. Es folgt

$$\langle f^n\rangle \cap \langle g\rangle = \{0\}.$$

Denn ist $h \in \langle f^n\rangle \cap \langle g\rangle$, so folgt $fh = 0$ (wegen $gh = 0$) und $h = af^n$ mit $a \in R$. Also gilt $af^{n+1} = hf = 0$ und damit $a \in \operatorname{Ann}(f^{n+1}) = \operatorname{Ann}(f^n)$. Es folgt $h = af^n = 0$. Da $\{0\}$ irreduzibel ist und $g \neq 0$, muss $f^n = 0$ gelten, was zeigt, dass $\{0\}$ primär ist. ∎

Satz 3.51 (Lasker[22]-Noether)**.** *In einem noetherschen Ring ist jedes Ideal ein endlicher Durchschnitt von irreduziblen Idealen. Insbesondere besitzt jedes Ideal eine Primärzerlegung.*

Beweis. (Noethersche Induktion) Es sei R ein noetherscher Ring und $\mathcal{A}$ die Menge aller Ideale von R, die nicht endlicher Durchschnitt von irreduziblen Idealen in R sind. Da R noethersch ist, besitzt $\mathcal{A}$ ein (bezüglich Inklusion) maximales Element I. Wegen $I \in \mathcal{A}$ ist I insbesondere nicht irreduzibel. Es gibt also Ideale J_1, J_2 von R mit $I = J_1 \cap J_2$ und $I \subsetneq J_1$, $I \subsetneq J_2$. Wegen der Maximalität von I, sind J_1 und J_2 Durchschnitt von irreduziblen Idealen, also auch I, ein Widerspruch. ∎

Korollar 3.52. *In einem graduierten noetherschen Ring ist jedes Ideal ein endlicher Durchschnitt von homogenen irreduziblen Idealen und besitzt damit eine homogene Primärzerlegung.*

Beweis. Der Beweis geht exakt genauso wie im vorigen Satz. ∎

[22] Emanuel Lasker (1868–1941) deutscher Mathematiker und Schachweltmeister

Wir diskutieren nun die geometrische Interpretation der Primärzerlegung. Sei I ein Ideal in $k[x_1, \dots, x_n]$ und $I = I_1 \cap \dots \cap I_r$ eine Primärzerlegung. Für die zugehörigen Varietäten heißt das

$$\mathcal{V}(I) = \mathcal{V}(I_1) \cup \dots \cup \mathcal{V}(I_r).$$

Wir wissen, dass die Ideale $\sqrt{I_j}$ alle prim sind, nach Lemma 3.49. Deshalb gibt es für jede der Varietäten $\mathcal{V}(I_j)$ nur zwei Möglichkeiten:

(i) $\mathcal{V}(I_j)$ ist eine irreduzible Komponente von $\mathcal{V}(I)$.

(ii) $\mathcal{V}(I_j)$ ist eine irreduzible Varietät, die in einer irreduziblen Komponente von $\mathcal{V}(I)$ echt enthalten ist. Dann heißt I_j eine **eingebettete Komponente** von I.

Da $\mathcal{V}(I)$ die Vereinigung der $\mathcal{V}(I_j)$ ist, müssen die irreduziblen Komponenten von $\mathcal{V}(I)$ unter den $\mathcal{V}(I_j)$ alle vorkommen. Welche eingebetteten Komponenten es noch gibt, hängt dagegen nicht nur von I, sondern auch von der gewählten Primäerzerlegung ab.

Bemerkungen 3.53. Während die Existenz der Primärzerlegung relativ leicht zu beweisen war, sind Fragen der Struktur und der Eindeutigkeit deutlich komplizierter.

(1) Die Primideale $\sqrt{I_j}$ in einer Primärzerlegung eines Ideals I heißen die **assoziierten Primideale** von I. Die Menge der assoziierten Primideale ist von der gewählten Primärzerlegung unabhängig. Im Fall des Polynomrings (oder einer endlich-erzeugten k-Algebra) ist das klar für die **minimalen assoziierten Primideale**, da diese zu einer irreduziblen Komponente von $\mathcal{V}(I)$ gehören.

(2) Wenn zwei Primärideale I_i und I_j in einer Primärzerlegung von I dieselbe Varietät $\mathcal{V}(I_i) = \mathcal{V}(I_j)$ liefern, dann ist auch $I_i \cap I_j$ primär (Übung 3.39) und man kann die Primärzerlegung entsprechend verkürzen. Jedes assoziierte Primideal gehört also zu genau einem Primärideal in einer minimalen Primärzerlegung.

(3) Unter den Primäridealen sind nur die eindeutig, die zu den minimalen assoziierten Primidealen (also zu den irreduziblen Komponenten) gehören. Die übrigen Primärideale sind dagegen im allgemeinen nicht eindeutig (siehe nachfolgendes Beispiel).

In Macaulay2 kann man eine Primärzerlegung mit durch `primaryDecomposition` berechnen.

```
i1 : R = QQ[x,y,z];
i2 : I = ideal((y^2-x*z)*(z^2-x^2*y),(y^2-x*z)*z);
o2 : Ideal of R
i3 : primaryDecomposition I
             2                    2              3
o3 = {ideal(y  - x*z), ideal (z, x ), ideal (z, y )}
o3 : List
```

Dagegen zeigt der Befehl `decompose`, den wir schon verwendet haben, nur die minimalen assoziierten Primideale.

```
i4 : decompose I
             2
o4 = {ideal(y  - x*z), ideal (x, z)}
o4 : List
```

Frage 3.54. Wie sieht das reelle Bild der Komponenten in diesem Beispiel aus?

Beispiele 3.55. Das Ideal $\langle x^2, xy\rangle \subset k[x,y]$ aus Beispiel 3.46 hat zwei verschiedene minimale Primärzerlegungen, nämlich

$$\langle x^2, xy\rangle \;=\; \langle x\rangle \cap \langle x^2, xy, y^2\rangle \;=\; \langle x\rangle \cap \langle x^2, y\rangle.$$

Die assoziierten Primideale sind $\langle x\rangle$ und $\langle x, y\rangle$. Geometrisch entspricht das in $\mathbb{A}^2$ der Geraden $\mathcal{V}(x)$ als irreduzible Komponente und dem Nullpunkt $\mathcal{V}(x,y)$ als eingebettete Komponente. Die beiden Primärideale zum Nullpunkt sind verschieden.

Bis jetzt war die Geometrie affin. In der projektiven Situation geht nach Kor. 3.52 alles genauso, mit einem Unterschied. Ist $I \subset k[x_0,\dots,x_n]$ ein homogenes Ideal und

$$I = I_1 \cap \cdots \cap I_r$$

eine homogene Primärzerlegung, so gibt es für die irreduziblen projektiven Varietäten $\mathcal{V}_+(I)$ drei verschiedene Fälle zu unterscheiden:

(i) $\mathcal{V}_+(I_j)$ ist eine irreduzible Komponente von $\mathcal{V}_+(I)$.
(ii) $\mathcal{V}_+(I_j)$ gehört zu einer eingebetteten Komponente von I.
(iii) $\mathcal{V}_+(I_j) = \varnothing$; dann gilt $\langle x_0,\dots,x_n\rangle \subset \sqrt{I_j}$ nach dem projektiven Nullstellensatz 3.12.

In einer minimalen Primärzerlegung gibt es höchstens ein Primärideal vom Typ (iii), dessen assoziiertes Primideal gerade das irrelevante Ideal $\langle x_0,\dots,x_n\rangle$ ist. Wenn man statt der projektiven Varietät $\mathcal{V}_+(I)$ den affinen Kegel $\mathcal{V}(I)$ betrachtet, dann entspricht ein solches Primärideal also einer einbetteten Komponenten im Ursprung $\{0\} = \mathcal{V}(x_0,\dots,x_n)$.

Beispiel 3.56. Betrachtet man zum Ideal $I = \langle x^2, xy\rangle$ aus Beispiel 3.46 die projektive Varietät $\mathcal{V}_+(x^2,xy) = \{[0,1]\} \subset \mathbb{P}^1$, dann ist nur das minimale assoziierte Primideal $\langle x\rangle$ geometrisch relevant, während das assoziierte Primideal $\langle x,y\rangle$ sich in der Geometrie nicht widerspiegelt.

Im Zusammenhang mit der Primärzerlegung erwähnen wir noch kurz das folgende nützliche Lemma, das wir später verwenden. Aussage und Beweis verallgemeinern direkt Lemma 1.30.

Lemma 3.57 (Primvermeidung)**.** *Es seien $P_1,\dots,P_r$ Primideale in einem Ring R und I ein weiteres Ideal. Falls $I \subset \bigcup_{i=1}^r P_i$ gilt, so ist I bereits in einem der Primideale P_i enthalten.*

Beweis. Induktion nach r: Für $r = 1$ ist nichts zu zeigen. Sei also $r \geqslant 2$. Angenommen falsch, also $I \subset \bigcup_{i=1}^r P_i$ aber $I \not\subset P_i$ für alle i. Nach Induktionsvoraussetzung ist I dann in keiner Vereinigung von weniger als r der Ideale $P_1,\dots,P_r$ enthalten. Es gibt also für jedes $i = 1,\dots,r$ ein Element $f_i \in I$, $f_i \notin \bigcup_{j\neq i} P_j$. Wegen $I \subset \bigcup_{i=1}^r P_i$ muss also $f_i \in P_i$ gelten. DDann ist $f_1 + f_2 \cdots f_r \in I$ in keinem der Primideale $P_1,\dots,P_r$ enthalten, ein Widerspruch. ∎

Übungen

Sei stets R ein Ring.

Übung 3.38. Es sei $I \neq R$ ein Ideal. Zeigen Sie, dass folgende Aussagen äquivalent sind:

(i) Das Ideal I ist primär;

(ii) Jeder Nullteiler in R/I ist nilpotent;
(iii) Das Nullideal in R/I ist primär.

Übung 3.39. Seien I, J Primärideale in R. Zeigen Sie: Falls $\sqrt{I} = \sqrt{J}$, so ist $I \cap J$ primär mit $\sqrt{I \cap J} = \sqrt{I}$.

Übung 3.40. Zeigen Sie: Ein Ideal in R ist genau dann ein Radikalideal, wenn es ein Durchschnitt von Primidealen ist. (*Anleitung:* Sei I ein Radikalideal. Zeigen Sie, dass I der Durchschnitt aller Primideale ist, die I enthalten, wie folgt: Ist $f \notin I$, dann hat die Menge

$$\{J \subset R\text{: } J \text{ ist Ideal von R mit } I \subset J \text{ und } f^r \notin J \text{ für alle } r \geqslant 1\}$$

ein maximales Element P. Zeigen Sie, dass P prim ist.)

3.10. Hilbert-Funktion und Hilbert-Polynom

Wir betrachten nun genauer die Struktur des homogenen Koordinatenrings einer projektiven Varietät. Es sei im folgenden immer

$$S = k[x_0, \ldots, x_n]$$

der Polynomring mit der Graduierung durch den Totalgrad. Sei I ein homogenes Ideal in S. Wie zuvor bezeichne S_d den homogenen Teil vom Grad d von S und $I_d = I \cap S_d$ den von I. Sei T der graduierte Restklassenring $T = S/I$ und $T_d = S_d/I_d$ der homogene Teil vom Grad d. Nach der Dimensionsformel gilt dann

$$\dim(I_d) + \dim(T_d) = \dim(S_d) = \binom{n+d}{n}.$$

Definition 3.58. Die **Hilbert-Funktion** von I ist die Funktion

$$H_I\text{:} \begin{cases} \mathbb{Z}_+ & \to & \mathbb{Z}_+ \\ d & \mapsto & \dim(T_d) \end{cases}.$$

Ist $X \subset \mathbb{P}^n$ eine projektive k-Varietät mit homogenem Verschwindungsideal $\mathcal{I}_+(X)$, so schreiben wir für $H_{\mathcal{I}_+(X)}$ auch einfach H_X, die Hilbert-Funktion von X.

Die Dimension von $\mathcal{I}(X)_d$ ist die Anzahl unabhängiger Formen vom Grad d, die auf X verschwinden, also die Anzahl der Hyperflächen, die X enthalten. Die Hilbert-Funktion von X drückt dies aus durch die **Co-Dimension** von $\mathcal{I}(X)_d$ in S_d.

Beispiele 3.59. (1) Die Hilbert-Funktion des Nullideals (und damit die Hilbert-Funktion von $\mathbb{P}^n$) ist einfach

$$H_{\mathbb{P}^n}(d) = \dim S_d = \binom{n+d}{n}.$$

(2) Es sei $k = K$ und die Varietät $X = \{p, q, r\}$ bestehe aus drei verschiedenen Punkten in $\mathbb{P}^2$. Ob das Ideal $\mathcal{I}_+(X)$ eine Linearform enthält oder nicht, sagt gerade, ob die drei Punkte p, q, r kollinear sind oder nicht. Der Wert $H_X(1)$ beantwortet also genau diese Frage, nämlich

$$H_X(1) = \begin{cases} 2 & \text{falls } p, q, r \text{ kollinear sind,} \\ 3 & \text{falls nicht.} \end{cases}$$

Andererseits gilt immer $H_X(2) = 3$. Um das einzusehen, betrachte die Abbildung[23]

$$\Phi\colon \begin{cases} k[x_0, x_1, x_2]_2 & \to & k^3 \\ f & \mapsto & \big(f(p), f(q), f(r)\big) \end{cases}.$$

Für jede Wahl von zwei der drei Punkte p, q, r gibt es eine quadratische Form, die in diesen beiden Punkten verschwindet, aber nicht in dem verbleibenden Punkt. (Zum Beispiel ein Produkt von zwei geeigneten Linearformen). Deshalb liegen die drei Einheitsvektoren im Bild von Φ, so dass Φ surjektiv ist. Damit hat der Kern von Φ, welcher genau $\mathcal{I}(X)_2$ ist, nach der Dimensionsformel die Dimension 3 (siehe hierzu auch Übung 3.41 und 3.42).

Proposition 3.60. *Es sei I ein homogenes Ideal in S und $\leqslant$ eine Monomordnung auf S.*

(1) Ist $f \in S$ homogen vom Grad d, dann auch jeder Standardrest von f modulo I bzgl. $\leqslant$.

(2) Das Ideal I und sein Leitideal $L(I)$ bezüglich $\leqslant$ haben dieselbe Hilbert-Funktion.

Beweis. (1) Sei r ein Standardrest von f modulo I bezüglich $\leqslant$. Per Definition gilt $f - r \in I$ und r enthält kein Monom aus $L(I)$. Für $e \neq d$ gilt also $r_e = (f - r)_e \in I_e$. Wäre $r_e \neq 0$, so läge das Leitmonom von r_e also in $L(I)$, ein Widerspruch dazu, dass r ein Standardrest ist.

(2) Sei $d \geqslant 1$. Nach Lemma 2.3 liegt eine Form f vom Grad d genau dann im monomialen Ideal $L(I)_d$, wenn alle in f vorkommenden Monome in $L(I)_d$ liegen. Deshalb bilden die Monome x^α vom Grad d, die nicht in $L(I)_d$ enthalten sind, eine Basis des Vektorraums $S_d/L(I)_d$.

Ist $f \in S$ homogen vom Grad d, so ist ein Standardrest r von f modulo I bezüglich $\leqslant$ wieder homogen vom Grad d, nach (1). Außerdem gilt $f - r \in I_d$ und kein Monom in r liegt in $L(I)$. Deshalb bilden die Monome x^α vom Grad d, die nicht in $L(I)_d$ liegen, auch eine Vektorraum-Basis von S_d/I_d. Damit haben beide Räume die gleiche Dimension und die Hilbert-Funktionen damit denselben Wert an der Stelle d. ∎

Das Hauptergebnis für diesen Abschnitt ist der folgende Satz.

Satz 3.61 (Hilbert)**.** *Für jedes homogene Ideal I in $k[x_0, \ldots, x_n]$ gibt es eine Zahl $d_0 \geqslant 0$ und ein eindeutig bestimmtes Polynom $P_I \in \mathbb{Q}[z]$ mit*

$$H_I(d) = P_I(d)$$

für alle $d \geqslant d_0$.

Das Polynom P_I heißt das **Hilbert-Polynom** von I. Ist $I = \mathcal{I}_+(X)$ das homogene Verschwindungsideal einer projektiven Varietät, dann schreiben wir wieder P_X anstelle von $P_{\mathcal{I}_+(X)}$.

Beweis. Nach Prop. 3.60(2) können wir I durch sein Leitideal bezüglich irgendeiner Monomordnung ersetzen und deshalb ohne Einschränkung annehmen, dass I ein monomiales Ideal ist. Es sei also I erzeugt von r Monomen, und wir zeigen die Behauptung durch Induktion nach r. Für

[23] Streng genommen ist dies keine wohldefinierte Abbildung: Wie wir schon bemerkt haben, sind homogene Polynome keine Funktionen auf $\mathbb{P}^n$. Wir müssten also eigentlich Vertreter $u, v, w \in K^3 \setminus \{0\}$ mit $p = [u]$, $q = [v]$, $r = [w]$ wählen und die Abbildung Φ durch Auswertung in diesen Vektoren definieren. Da wir uns aber nur für die Dimension von Kern und Bild interessieren und diese nicht von der Wahl der Vertreter abhängen, verzichten wir auf den zusätzlichen Aufwand.

$r = 0$ ist $I = \langle 0 \rangle$ und die Hilbert-Funktion ist $H_{\langle 0 \rangle}(d) = \binom{n+d}{n}$. Dies ist ein Polynom in d, nämlich

$$P_{\langle 0 \rangle}(z) = \binom{n+z}{n} = \frac{1}{n!}(z+1)\cdots(z+n).$$

Sei $r \geqslant 0$ und sei $I = J + \langle x^\beta \rangle$, wobei J von r Monomen erzeugt ist, etwa

$$J = \langle x^{\alpha_1}, \ldots, x^{\alpha_r} \rangle.$$

Setze

$$J' = (J : x^\beta) = \{ f \in S : x^\beta f \in J \}.$$

(Der Idealquotient $(J : x^\beta)$ ist dabei durch die rechte Seite definiert.) Nach Lemma 2.3 gilt nun

$$J' = \left\langle \frac{x^{\alpha_i}}{\mathrm{ggT}(x^{\alpha_i}, x^\beta)} : i = 1, \ldots, r \right\rangle.$$

Setze $e = |\beta|$ und betrachte für $d \geqslant e$ die lineare Abbildung

$$S_{d-e} \to (I/J)_d, f \mapsto \overline{x^\beta f}.$$

Sie ist surjektiv und ihr Kern ist gerade J'_{d-e}. Nach der Dimensionsformel gilt deshalb $\dim(S_{d-e}) = \dim(J'_{d-e}) + \dim(I/J)_d$. Außerdem ist $\dim(I/J)_d = \dim(I_d) - \dim(J_d)$ und deshalb zusammen

$$\dim(S_{d-e}) = \dim(J'_{d-e}) + \dim(I_d) - \dim(J_d).$$

Daraus folgt $\dim(S_{d-e}) - \dim(J'_{d-e}) = (\dim(S_d) - \dim(J_d)) - (\dim(S_d) - \dim(I_d))$, also

$$H_I(d) = H_J(d) - H_{J'}(d-e).$$

Nach Induktionsvoraussetzung angewandt auf J und J' gibt es also $d_0 \geqslant e$ mit

$$H_I(d) = P_J(d) - P_{J'}(d-e)$$

für alle $d \geqslant d_0$. Also ist $P_J(z) - P_{J'}(z-e)$ das Hilbert-Polynom von I. Die Eindeutigkeit folgt daraus, dass zwei Polynome, die an unendlich vielen Stellen übereinstimmen, gleich sind. ■

Bemerkungen 3.62. (1) Der Beweis enthält einen Algorithmus zur Berechnung des Hilbert-Polynoms eines homogenen Ideals: Berechne das Leitideal (mit Hilfe einer Gröbnerbasis) und verfahre dann induktiv mit den Erzeugern wie im Beweis.

(2) Der kleinste Grad d_0 mit der Eigenschaft, dass Hilbert-Funktion und Hilbert-Polynom in allen größeren Graden übereinstimmen, wird die **Hilbert-Regularität** eines homogenen Ideals genannt. Zwar liefert der Beweis eine Schranke für die Hilbert-Regularität über die Grade der Erzeuger des Leitideals, aber es ist nicht klar, wie diese wiederum vom Ideal selbst abhängen.

(3) Das Hilbert-Polynom eines homogenen Ideals ist ein **numerisches Polynom**, das heißt es nimmt auf allen (hinreichend großen) ganzen Zahlen auch ganzzahlige Werte an. Natürlich ist jedes Polynom mit ganzzahligen Koeffizienten ein numerisches Polynom, aber die Koeffizienten des Hilbert-Polynoms sind in der Regel nicht ganzzahlig; siehe dazu Übung 3.48.

Beispiele 3.63. (1) Die Hilbert-Funktion von $\mathbb{P}^n$ ist bereits ein Polynom und stimmt deshalb mit dem Hilbert-Polynom überein, nämlich

$$P_{\mathbb{P}^n}(z) = \binom{z+n}{n}.$$

(2) Es sei $X \subset \mathbb{P}^2$ eine Kurve, gegeben durch ein reduziertes homogenes Polynom $f \in k[x_0, x_1, x_2]$ vom Grad d. Dann gilt $\mathcal{I}_+(X) = \langle f \rangle$, und für $e \geqslant d$ besteht der homogene Teil $\langle f \rangle_e$ gerade aus allen Formen vom Grad e, die durch f teilbar sind. Mit anderen Worten, die Multiplikation mit f definiert einen Vektorraumisomorphismus

$$k[x_0, x_1, x_2]_{e-d} \xrightarrow{\sim} \langle f \rangle_e, g \mapsto g \cdot f.$$

Es folgt

$$\dim(\langle f \rangle_e) = \begin{cases} \binom{e-d+2}{2} & \text{für } e \geqslant d \\ 0 & \text{für } e < d. \end{cases}$$

und damit

$$H_X(e) = \binom{e+2}{2} - \binom{e-d+2}{2} = d \cdot e - \frac{d(d-3)}{2} \quad (\text{für } e \geqslant d),$$
$$P_X(z) = dz - \frac{d(d-3)}{2}.$$

(3) Genauso geht das für $n > 2$. Das Hilbert-Polynom einer Hyperfläche $X \subset \mathbb{P}^n$ vom Grad d ist

$$P_X(z) = \binom{z+n}{n} - \binom{z-d+n}{n} = \frac{1}{n!}\big((z+n)\cdots(z+1) - (z-d+n)\cdots(z-d+1)\big)$$
$$= \frac{d}{(n-1)!} z^{n-1} + \text{Terme von niedrigerem Grad in } z$$

Die Werte des Hilbert-Polynoms in den natürlichen Zahlen stimmen per Definition ab einem gewissen Grad mit der Hilbert-Funktion überein. Aber auch der *Grad* und die *Koeffizienten* des Hilbert-Polyoms einer projektiven Varietät enthalten wichtige Informationen. Als erstes bekommen wir endlich eine Definition für die *Dimension*.

Definition 3.64. Die **Dimension** einer projektiven k-Varietät $X \subset \mathbb{P}^n$ ist der Grad ihres Hilbert-Polynoms.

Diese Definition der Dimension ist natürlich vollkommen unanschaulich. Der Vorteil ist, dass man ganz gut damit rechnen kann.

Beispiele 3.65. Die folgenden Dimensionen ergeben sich sofort aus den Berechnungen des Hilbert-Polynoms in den Beispiel 3.63 und den Übungen.

(1) Der projektive Raum $\mathbb{P}^n$ hat die Dimension n.
(2) Eine Hyperfläche $\mathcal{V}_+(f)$ in $\mathbb{P}^n$ hat die Dimension $n-1$.
(3) Die rationale Normalkurve in $\mathbb{P}^n$ hat die Dimension 1 (siehe Übung 3.43).
(4) Die Veronese-Varietät $v_d(\mathbb{P}^n)$ hat die Dimension n (siehe Übung 3.44).
(5) Die Segre-Varietät $\Sigma_{m,n}$ hat die Dimension $m+n$ (siehe Übung 3.45).
(6) Jede endliche Varietät hat die Dimension 0 (falls $k = K$; allgemeiner Fall später).

Bemerkung 3.66. Das Hilbert-Polynom enthält noch weitere sogenannte Invarianten der Varietät. Ist $X \subset \mathbb{P}^n$ eine projektive Varietät der Dimension m, dann ist der Leitkoeffizient von P_X multipliziert mit $m!$ eine positive ganze Zahl (siehe Übung 3.48). Diese Zahl heißt der **Grad von** X. Aus der Berechnung des Hilbert-Polynoms in Beispiel 3.63(3) folgt, dass der Grad einer Hyperfläche $\mathcal{V}_+(f)$ mit $\deg(f) = d$ gerade d ist, so dass die Definition des Grades in diesem Fall mit der üblichen übereinstimmt.

Auch der konstante Term des Hilbert-Polynoms hat einen Namen. Ist X eine projektive Varietät der Dimension m, so heißt die Zahl $(-1)^m(p_X(0)-1)$ das **arithmetische Geschlecht von** X. Besonders wichtig ist diese Invariante für Kurven, also im Fall $m = 1$. Nach Beispiel 3.63(2) hat eine ebene Kurve vom Grad d das arithmetische Geschlecht

$$g_a = \binom{d-1}{2} = \frac{(d-1)(d-2)}{2}.$$

Das arithmetische Geschlecht spielt eine große Rolle in der systematischen Theorie der algebraischen Kurven und ihrer Gegenstücke in der komplexen Geometrie, den Riemannschen Flächen. Das Geschlecht ist eine bestimmende Größe im *Satz von Riemann-Roch*, dessen Aussage man als eine verfeinerte und abstrahierte Version der Hilbert-Funktion verstehen kann.

Übungen

Übung 3.41. Es gelte $k = K$. Es sei X eine Menge von m Punkten in $\mathbb{P}^n$ und sei H_X die Hilbert-Funktion von X. Zeigen Sie: Für alle $d \geqslant m-1$ gilt $H_X(d) = m$.

Übung 3.42. Es gelte $k = K$. Es sei $X \subset \mathbb{P}^n$ eine Menge von m Punkten und sei $d \geqslant 0$. Beweisen Sie, dass die folgenden Aussagen äquivalent sind.

(i) Die Hilbert-Funktion H_X erfüllt $H_X(d) = m$.
(ii) Die Punktauswertungen $\{\mu_p : p \in X\}$, gegeben durch $\mu_p : k[x_0,\dots,x_n], f \mapsto f(p)$, sind linear unabhängige Elemente des Dualraums $k[x_0,\dots,x_n]^*$.
(iii) Für jedes $p \in X$ gibt es ein $f \in k[x_0,\dots,x_n]_d$ mit $f(q) = 0$ für alle $q \in X$, $q \neq p$ und $f(p) \neq 0$.

Übung 3.43. Bestimmen Sie das Hilbert-Polynom, den Grad und das arithmetische Geschlecht der rationalen Normalkurve in $\mathbb{P}^n$.

Übung 3.44. Bestimmen Sie das Hilbert-Polynom der Veronese-Varietät $v_d(\mathbb{P}^n)$.

Übung 3.45. Bestimmen Sie das Hilbert-Polynom der Segre-Varietät $\Sigma_{m,n}$.

Übung 3.46. Zeigen Sie: Eine Hyperfläche vom Grad d in $\mathbb{P}^n$ hat das arithmetische Geschlecht $\binom{d-1}{n}$.

Übung 3.47. Zeigen Sie: Ist $I \subset k[x_0,\dots,x_n]$ ein homogenes Ideal mit $\mathcal{V}_+(I) = \varnothing$, so gilt $P_I = 0$.
(*Hinweis:* Verwenden Sie Kor. 3.13).

Übung 3.48. Ein Polynom $f \in \mathbb{Q}[z]$ heißt **numerisch**, wenn es $f(n) \in \mathbb{Z}$ für alle $n \in \mathbb{Z}$ erfüllt. Beweisen Sie die folgenden Aussagen.

(a) Die Polynome
$$F_m(z) = \binom{z}{m} = \frac{1}{m!}z(z-1)\cdots(z-m+1)$$
für $m \geqslant 1$ sind numerisch und $1 = F_0, F_1, \dots, F_d$ bilden eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}[z]_{\leqslant d}$.
(b) Ein Polynom $f \in \mathbb{Q}[z]$ erfüllt $f(n) \in \mathbb{Z}$ für alle hinreichend großen $n \in \mathbb{Z}$ genau dann, wenn es eine $\mathbb{Z}$-Linearkombination der F_i ist. Jedes solche Polynom ist numerisch. (*Vorschlag:* Drücken Sie f durch die Basis-Polynome aus und betrachten Sie die Differenz $f(n+1) - f(n)$ für hinreichend großes n.)
(c) Das Hilbert-Polynom eines homogenen Ideals in $k[x_0,\dots,x_n]$ ist numerisch.
(d) Sei f ein numerisches Polynom vom Grad d. Dann ist der Leitkoeffizient von f multipliziert mit $d!$ ganzzahlig und der konstante Term von f ist ganzzahlig.

Daniel Plaumann
Technische Universität Dortmund
Sommersemester 2016
Fassung vom 17. Juli 2016

4. LOKALE GEOMETRIE

Wir haben im vorigen Kapitel einige der Vorteile gesehen, die die projektive Geometrie gegenüber der affinen Geometrie bietet. Auf der algebraischen Seite entsprach das dem Übergang von Algebren zu graduierten Algebren. Im Gegensatz dazu konzentriert sich die lokale Geometrie auf Umgebungen von Punkten. Auf der algebraischen Seite entspricht das dem Lokalisieren, dem Übergang zu lokalen Ringen. Die algebraische Geometrie wird dadurch insgesamt abstrakter. Wir werden aber auch sehen, wie sich einige der Probleme aus dem vorigen Kapitel, vor allem das allgemeine Studium von Morphismen, in dieser Weise lösen lassen. Außerdem kümmern wir uns um eine saubere Behandlung der geometrischen Begriffe Dimension und Glattheit.

4.1. Lokalisierungen und lokale Ringe

Es sei R ein Ring (kommutativ mit Eins). Wenn R ein Integritätsring ist, dann kann man zu R den Quotientenkörper $\mathrm{Quot}(R)$ bilden, der aus allen Brüchen $\frac{f}{g}$ mit $f, g \in R$, $g \neq 0$ besteht. Es sei $S \subset R$ eine **multiplikative Teilmenge**, d.h. es gelte $S \cdot S \subset S$ und $1 \in S$. Dann ist

$$R_S = \left\{ \frac{f}{s} \in \mathrm{Quot}(R) \colon s \in S \right\}$$

ein Teilring von $\mathrm{Quot}(R)$, der $R = \{\frac{f}{1} \colon f \in R\}$ enthält. Da Nenner sowohl bei der Addition als auch bei der Multiplikation von Brüchen multipliziert werden, ist es klar, dass R_S ein Teilring von $\mathrm{Quot}(R)$ ist. Es gilt $\mathrm{Quot}(R) = R_{R \setminus \{0\}}$. Der Ring R_S heißt die **Lokalisierung von R nach S**. Der Grund für diese Bezeichnung wird in den Beispielen klar werden.

Beispiel 4.1. Es sei $R = k[x_1, \ldots, x_n]$ und $p \in k^n$. Setze

$$S = \{f \in R \colon f(p) \neq 0\}.$$

Offenbar ist S multiplikativ, so dass wir die Lokalisierung

$$R_S = \left\{ \frac{f}{s} \in k(x_1, \ldots, x_n) \colon s(p) \neq 0 \right\}$$

bilden können. Diese Art Beispiel ist für die Geometrie am wichtigsten.

Es gibt noch eine kleine technische Schwierigkeit: Manchmal braucht man den Begriff der Lokalisierung auch im Fall, dass R kein Integritätsring ist, also Nullteiler besitzt. Angenommen $S \subset R$ ist eine multiplikative Teilmenge und es gibt $f \in R \setminus \{0\}$ und $s \in S$ mit

$$f \cdot s = 0.$$

Wenn wir s nun zu einer Einheit machen, dann kann man diese Gleichung anschließend mit $\frac{1}{s}$ multiplizieren und es folgt $f = 0$. In der Lokalisierung müssen wir f also zu Null machen.

Deshalb muss die Definition von Brüchen gegenüber dem Quotientenkörper eines Integritätsbereichs angepasst werden. Definiere dazu die Relation

$$(f_1, s_1) \sim (f_2, s_2) \qquad \Longleftrightarrow \qquad \exists t \in S\colon t(f_1 s_2 - f_2 s_1) = 0$$

auf der Menge $R \times S$. Auf diese Weise entsteht ein Ring von Brüchen wie zuvor.

Proposition 4.2. *Sei R ein Ring und $S \subset R$ eine multiplikative Teilmenge. Die Relation $\sim$ ist eine Äquivalenzrelation. Wir schreiben $\frac{f}{s}$ für die Äquivalenzklasse von (f, s) und R_S für die Menge aller Äquivalenzklassen. Mit den üblichen Rechenregeln*

$$\frac{f}{s} \cdot \frac{g}{t} = \frac{fg}{st} \qquad \textit{und} \qquad \frac{f}{s} + \frac{g}{t} = \frac{ft + gs}{st}$$

wird R_S zu einem kommutativen Ring mit Eins $\frac{1}{1}$ und Null $\frac{0}{1}$.

Beweis. Übung 4.2 ∎

Wie zuvor heißt R_S die **Lokalisierung** von R nach S. Sie kommt zusammen mit einem Ringhomomorphismus

$$\varphi_S\colon R \to R_S,\ f \mapsto \frac{f}{1},$$

der **Lokalisierungsabbildung**. Nach Konstruktion werden die Elemente von S unter Lokalisierung zu Einheiten, das heißt $\varphi_S(S) \subset (R_S)^\times$. Es gilt $\varphi_S(f) = \frac{0}{1}$ per Definition genau dann, wenn es $t \in S$ gibt mit $tf = 0$. Also ist φ_S genau dann injektiv, wenn S keine Nullteiler von R enthält. (Auch $0 \in S$ haben wir nicht verboten. In diesem Fall ist dann R_S der Nullring.) Natürlich schreibt man häufig f statt $\frac{f}{1}$, obwohl R eben im allgemeinen kein Teilring von R_S ist.

Beispiel 4.3. Es sei $R = k[x, y]/\langle xy\rangle$ und $S = \{\overline{y}^i\colon i \geqslant 0\}$. In R gilt $\overline{x}\,\overline{y} = 0$ und in R_S deshalb

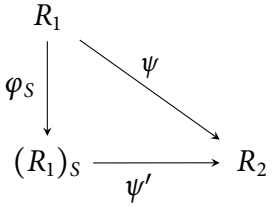
$$\frac{\overline{x}}{1} = \frac{\overline{x}}{1}\frac{\overline{y}}{1}\frac{1}{\overline{y}} = 0.$$

Es ist $\ker(\varphi_S) = \langle\overline{x}\rangle$ und

$$R_S \cong k[y]_y = \left\{\frac{f(y)}{y^j}\colon f \in k[y], j \geqslant 0\right\}.$$

Genauso wie der Quotientenkörper ist die Lokalisierung durch eine sogenannte **universelle Eigenschaft** bestimmt.

Proposition 4.4. *Es sei $\psi\colon R_1 \to R_2$ ein Ringhomomorphismus, $R_2 \neq 0$, und $S \subset R_1$ eine multiplikative Menge. Genau dann exisiert eine Abbildung $\psi'\colon (R_1)_S \to R_2$ mit $\psi = \psi' \circ \varphi_S$, wenn $\psi(S) \subset R_2^\times$ gilt. In diesem Fall ist ψ' eindeutig bestimmt.*



Beweis. Falls ein solches ψ' existiert, dann folgt aus $\varphi_S(S) \subset R_1^\times$ auch $\psi(S) = \psi'(\varphi_S(S)) \subset R_2^\times$ (denn jeder Ringhomomorphismus bildet Einheiten auf Einheiten ab). Ist umgekehrt diese Bedingung erfüllt, so definiere ψ' für $f \in R_1$ und $s \in S$ durch

$$\psi'\left(\frac{f}{s}\right) = \psi(f) \cdot \psi(s)^{-1}.$$

Dieses ψ' ist ein Ringhomomorphismus mit der gewünschten Eigenschaft. Da außerdem $\psi'(\frac{f}{1}) = \psi(f)$ und $\psi'(\frac{1}{s}) = \psi(s)^{-1}$ gelten müssen, folgt die Eindeutigkeit von ψ'. ∎

Als nächstes untersuchen wir die Beziehung zwischen Idealen in einem Ring und Idealen in einer Lokalisierung. Sei R ein Ring und S eine multiplikative Teilmenge. Ist J ein Ideal von R_S, so ist $\varphi_S^{-1}(J)$ ein Ideal von R. Ist J prim, so auch $\varphi_S^{-1}(J)$. (Das stimmt für jeden Homomorphismus zwischen beliebigen Ringen.) Ist I ein Ideal von R, dann schreiben wir I_S oder manchmal deutlicher $I \cdot R_S$ für das von $\varphi_S(I)$ in R_S erzeugte Ideal.

Proposition 4.5. *(1) Für jedes Ideal J von R_S gilt $J = \left(\varphi_S^{-1}(J)\right)_S$. Die Abbildung $J \mapsto \varphi_S^{-1}(J)$ ist also eine Injektion von der Menge der Ideale in R_S in die Ideale von R.*

(2) Die Abbildung $P \mapsto \varphi_S^{-1}(P)$ induziert eine Bijektion zwischen der Menge aller Primideale von R_S und der Menge aller Primideale P von R mit $P \cap S = \varnothing$. Die Bijektion erhält Inklusionen und Durchschnitte. Die Umkehrabbildung ist gegeben durch $P \mapsto P_S$.

Beweis. (1) Es sei $J \subset R_S$ ein Ideal und sei $I = \varphi_S^{-1}(J) = \{f \in R : \frac{f}{1} \in J\}$. Für jedes $\frac{f}{s} \in J$ gelten $s \cdot \frac{f}{s} = \frac{f}{1} \in J$ und $\frac{f}{s} = \frac{1}{s} \cdot \frac{f}{1}$. Das zeigt, dass J von $\varphi_S(I)$ erzeugt wird.

(2) Sei $Q \subset R_S$ ein Primideal. Wegen $Q \neq R_S$ muss dann $Q \cap R_S^\times = \varnothing$ und damit $\varphi^{-1}(Q) \cap S = \varnothing$ gelten. Ist andererseits $P \subset R$ ein Primideal mit $P \cap S = \varnothing$, so ist P_S ein Primideal; denn ist $\frac{f}{s} \cdot \frac{g}{t} = \frac{h}{u}$ mit $h \in P$ und $u \in S$, so gibt es nach Definition der Gleichheit in R_S ein $v \in S$ mit $v(fgu - hst) = 0$. Wegen $u, v \notin P$ folgt $f \in P$ oder $g \in P$, also $\frac{f}{s} \in P_S$ oder $\frac{g}{t} \in P_S$. Außerdem gilt $P = \varphi_S^{-1}(P_S)$. Denn ist $f \in R$ mit $\varphi_S(f) \in P_S$, so heißt das $\frac{f}{1} = \frac{g}{s}$ für ein $g \in P$ und ein $s \in S$. Also gibt es $t \in S$ mit

$$fst = gt.$$

Die rechte Seite liegt in P, also auch fst. Wegen $st \notin P$ folgt $f \in P$, da P ein Primideal ist. ∎

Beispiel 4.6. Betrachte wie in Beispiel 4.1 die Lokalisierung R_S mit

$$R = k[x_1, \ldots, x_n] \text{ und } S = \left\{f \in R : f(p) \neq 0\right\},$$

für $p \in \mathbb{A}^n$. Nach Prop. 4.5 sind die Primideale von R_S genau die Primideale P von R mit $P \cap S = \varnothing$, was gerade $p \in \mathcal{V}(P)$ bedeutet. Die Primideale von R_S entsprechen also genau den irreduziblen affinen k-Varietäten in $\mathbb{A}^n$, die den Punkt p enthalten.

Wie sieht es mit reduziblen Untervarietäten aus? Sei dazu etwa $n = 2$ und $p = (0, 0)$ und betrachte das Ideal $\langle (x-1)y \rangle$. Wegen $(x-1)(p) \neq 0$ gilt dann $x - 1 \in S$ und deshalb $\langle (x-1)y \rangle = \langle \frac{y}{1} \rangle = \langle y \rangle_S$ in R_S. Die Varietät $\mathcal{V}((x-1)y) \subset \mathbb{A}^2$ ist die Vereinigung der beiden Geraden $x = 1$ und $y = 0$, aber nur eine enthält den Punkt p. Deshalb verschwindet die andere in der Lokalisierung. In diesem Sinn sieht die Lokalisierung nur noch die Geometrie *lokal* um den Punkt p.

Besonders wichtig sind zwei Typen von Lokalisierung: (1) Ist $f \in R$, so ist $S = \{1, f, f^2, \dots\}$ eine multiplikative Menge und wir schreiben kurz R_f für R_S. Diese Lokalisierung nach den Potenzen eines Elements kann man auch anders beschreiben. Betrachte den Ringhomomorphismus

$$R[x] \to R_f, G(x) \mapsto G\left(\frac{1}{f}\right).$$

Dieser ist offenbar surjektiv und der Kern ist gerade das Ideal $\langle fx - 1\rangle$. Nach dem Homomorphiesatz gibt es also einen Isomorphismus von R-Algebren

$$R_f \cong R[x]/\langle fx - 1\rangle.$$

(2) Per Definition ist ein Ideal P von R genau dann ein Primideal, wenn $R \setminus P$ eine multiplikative Teilmenge ist. In diesem Fall schreibt man

$$R_P := R_{R\setminus P}.$$

(Das ist zwar auf den ersten Blick etwas verwirrend, aber wenn man aufpasst, ist die Verwechselungsgefahr gering: P selbst kann niemals multiplikativ sein, da es 1 nicht enthält.) Das ist genau die Situation in den Beispielen 4.1 und 4.6, in denen P das Verschwindungsideal eines Punkts ist.

Definition 4.7. Ein Ring heißt **lokal**, wenn er nur ein einziges maximales Ideal besitzt.

Korollar 4.8. *Ist $P \subset R$ ein Primideal, so sind die Primideale von R_P in inklusionserhaltender Bijektion mit den Primidealen von R, die in P enthalten sind. Insbesondere ist R_P ein lokaler Ring mit maximalem Ideal PR_P.*

Beweis. Das folgt einfach, indem man Prop. 4.5(2) auf $S = R \setminus P$ anwendet. ∎

Korollar 4.9. *Sei R ein noetherscher Ring und $S \subset R$ eine multiplikative Teilmenge. Dann ist R_S wieder noethersch.*

Beweis. Sei J ein Ideal von R_S. Nach Prop. 4.5(1) gilt $J = \varphi_S^{-1}(J)_S$. Da R noethersch ist, ist $\varphi_S^{-1}(J)$ endlich erzeugt, und J wird von den Bildern der Erzeuger unter φ_S erzeugt, ist also ebenfalls endlich erzeugt. ∎

Bemerkung 4.10. Es ist dagegen nicht wahr, dass eine Lokalisierung einer endlich erzeugten Algebra über einem Körper wieder eine endlich erzeugte Algebra ist. Das stimmt schon für den Quotientenkörper nicht. Zum Beispiel kann $k(x) = \mathrm{Quot}(k[x])$ keine endlich erzeugte k-Algebra sein, denn sonst wäre $k(x)$ nach Satz 1.47 algebraisch über k. (Das kann man auch direkt sehen; siehe Übung 4.3.)

Für nachher notieren wir noch:

Lemma 4.11. *Es sei R ein Integritätsring. Für jedes Primideal P von R ist dann R_P ein Teilring von* $\mathrm{Quot}(R)$ *und es gilt*

$$R = \bigcap_{\substack{M\subset R \\ \text{maximales Ideal}}} R_M.$$

Beweis. $R \subset \bigcap R_M$ ist klar. Sei $\frac{f}{s} \in \mathrm{Quot}(R) \setminus R$. Dann ist s keine Einheit in R, also $\langle s\rangle \subsetneq R$. Nach dem Zornschen Lemma ist s also in einem maximalen Ideal M enthalten. Es folgt $\frac{f}{s} \notin R_M$. ∎

Im Zusammenhang mit projektiven Varietäten brauchen wir auch noch eine homogene Version der Lokalisierung.

Lemma 4.12. *Es sei S ein $\mathbb{Z}_+$-graduierter Ring und T eine multiplikative Teilmenge von homogenen Elementen von S, $0 \notin T$. Dann wird durch*

$$(S_T)_d = \left\{ \frac{f}{t} \in S_T : f \text{ homogen mit } \deg(f) - \deg(t) = d \right\}$$

für $d \in \mathbb{Z}$ eine $\mathbb{Z}$-Graduierung auf S_T definiert.

Beweis. Übung 4.4. ∎

Übungen

Übung 4.1. Bestimmen Sie für $R = \mathbb{Z}/\langle 6\rangle$ und $P = \langle \overline{2}\rangle$ die Lokalisierung R_P.

Übung 4.2. Beweisen Sie Prop. 4.2.

Übung 4.3. Es sei k ein Körper, A eine endlich erzeugte k-Algebra und $S \subset A$ eine multiplikative Menge. Zeigen Sie: Falls A_S eine endlich erzeugte k-Algebra ist, so gibt es $f \in A$ mit $A_S = A_f$.

Übung 4.4. Beweisen Sie Lemma 4.12.

Übung 4.5. Es sei R ein Ring, $S \subset R$ eine multiplikative Teilmenge und $I \subset R$ ein Ideal. Zeigen Sie die Isomorphie $R_S/I_S \cong (R/I)_{\overline{S}}$.

Übung 4.6. Es sei R ein Ring und $S \subset R$ eine multiplikative Teilmenge mit $0 \notin S$. Sei $P \subset R$ ein Ideal, das maximal ist bezüglich der Eigenschaft $P \cap S = \varnothing$. Zeigen Sie, dass P ein Primideal ist.

4.2. Die Zariski-Topologie und quasiprojektive Varietäten

Erinnerung: Eine **Topologie** auf einer Menge X ist gegeben durch eine Menge $\mathcal{T}$ von Teilmengen von X, genannt die *offenen Mengen* (bezüglich der Topologie $\mathcal{T}$), mit den folgenden Eigenschaften. Der ganze Raum X und die leere Teilmenge $\varnothing$ sind offen, also in $\mathcal{T}$ enthalten. Außerdem ist der Durchschnitt von endlich vielen offenen Mengen wieder offen und die Vereinigung von beliebig vielen offenen Mengen ist wieder offen. Eine Teilmenge $A \subset X$ heißt *abgeschlossen* (bezüglich der Topologie $\mathcal{T}$), wenn das Komplement $X \setminus A$ offen ist. Man kann die Eigenschaften der Topologie auch genauso gut über die Menge aller abgeschlossenen Teilmengen von X charakterisieren. Diese erfüllen die folgenden Eigenschaften:

(1) Die leere Menge und der ganze Raum X sind abgeschlossen.
(2) Die Vereinigung von endlich vielen abgeschlossenen Mengen ist abgeschlossen.
(3) Der Durchschnitt von beliebig vielen abgeschlossenen Mengen ist abgeschlossen.

Die Menge aller affinen k-Varietäten in $\mathbb{A}^n$ und die Menge aller projektiven k-Varietäten in $\mathbb{P}^n$ erfüllen diese Eigenschaften und definieren die Zariski-Topologie auf $\mathbb{A}^n$ und $\mathbb{P}^n$.

Verglichen mit der euklidischen Topologie, die man aus der Analysis gewohnt ist, ist die Zariski-Topologie ziemlich schwach. Zum Beispiel sind in $\mathbb{A}^1$ alle abgeschlossenen Mengen endlich. Ist $k = K$, so sind die abgeschlossenen Teilmengen genau die endlichen Teilmengen. Die Zariski-Topologie ist in diesem Fall also gerade die sogenannte **co-endliche Topologie**.

Eine Abbildung $\varphi\colon X \to Y$ zwischen zwei topologischen Räumen heißt **stetig**, wenn $\varphi^{-1}(U)$ für jede offene Teilmenge U von Y offen in X ist. Eine stetige Bijektion zwischen X und Y mit stetiger Umkehrabbildung heißt ein **Homöomorphismus**.

Ist X ein topologischer Raum und $V \subset X$ eine Teilmenge, so wird V ebenfalls zu einem topologischen Raum, versehen mit der **Teilraumtopologie** (oft auch Spurtopologie genannt). Eine Teilmenge $U \subset V$ ist dann **offen in** V, wenn es eine offene Teilmenge W von X gibt mit $U = W \cap V$. (Dabei braucht U nicht offen in X zu sein, wenn V es nicht ist.) Deswegen erbt jede Teilmenge einer affinen oder projektiven k-Varietät von dieser die k-Zariski-Topologie.

Lemma und Definition 4.13. Es sei V eine affine k-Varietät. Für $f \in k[V]$ sei

$$\mathcal{D}(f) = \{p \in V\colon f(p) \neq 0\}.$$

Teilmengen der Form $\mathcal{D}(f)$ mit $f \in k[V]$ heißen **basis-offen**. Es gilt $\mathcal{D}(f) \cap \mathcal{D}(g) = \mathcal{D}(fg)$ und jede offene Teilmenge von V ist eine endliche Vereinigung von basis-offenen Mengen.

Beweis. Es gilt $\mathcal{D}(f) = V \setminus \mathcal{V}(f)$, also ist $\mathcal{D}(f)$ offen. Ist $U \subset V$ offen, so gibt es $f_1, \dots, f_r \in k[V]$ mit $V \setminus U = \mathcal{V}(f_1, \dots, f_r)$. Also gilt $U = \mathcal{D}(f_1) \cup \dots \cup \mathcal{D}(f_r)$. ∎

Eine entsprechende Aussage gibt es auch im Projektiven. Wie zuvor sei $\mathcal{D}_+(f)$ für ein homogenes Polynom $f \in k[x_0, \dots, x_n]$ die offene Teilmenge $\mathbb{P}^n \setminus \mathcal{V}_+(f)$. Jede offene Teilmenge von $\mathbb{P}^n$ ist eine endliche Vereinigung von solchen der Form $\mathcal{D}_+(f)$.

Proposition 4.14. *Die Bijektion*

$$\rho_i\colon \begin{cases} \mathbb{A}^n & \to & D_i \\ (a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) & \mapsto & [a_0, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n] \end{cases}$$

zwischen $\mathbb{A}^n$ und $D_i = \mathcal{D}_+(x_i) \subset \mathbb{P}^n$ ist ein Homöomorphismus bezüglich der k-Zariski-Topologie auf $\mathbb{A}^n$ und der Teilraumtopologie der k-Zariski-Topologie auf D_i.

Beweis. Es genügt zu zeigen, dass eine Teilmenge V von $\mathbb{A}^n$ genau dann k-abgeschlossen ist, wenn es eine k-abgeschlossene Teilmenge $X \subset \mathbb{P}^n$ gibt mit $\rho_i(V) = X \cap D_i$. Dies folgt leicht aus Prop. 3.21 (siehe Übung 4.9). ∎

Definition 4.15. Jede offene Teilmenge einer projektiven (bzw. affinen) k-Varietät heißt eine **quasiprojektive (bzw. quasiaffine)** k**-Varietät**.

Jede projektive Varietät ist auch quasiprojektiv, jede affine auch quasiaffin. Nach Prop. 4.14(3) ist jede quasiaffine Varietät homöomorph zu einer quasiprojektiven Varietät. Deshalb sagen wir einfach k-**Varietät** für eine k-Varietät die quasiaffin oder quasiprojektiv sein darf.

Korollar 4.16. *Jede projektive (bzw. quasiprojektive) k-Varietät W besitzt eine endliche Überdeckung $W = U_1 \cup \dots \cup U_n$ durch offene Teilmengen, die zu affinen (bzw. quasiaffinen) k-Varietäten homöomorph sind.*

Beweis. Ist $W \subset \mathbb{P}^n$, dann kann man nach Prop. 4.14(3) die Teilmengen $U_i = W \cap D_i$ nehmen. ∎

Definition 4.17. Ein topologischer Raum X heißt **noethersch**, wenn er die absteigende Kettenbedingung für abgeschlossene Mengen besitzt: Ist $Y_1 \supset Y_2 \supset \cdots$ eine Folge von abgeschlossenen Mengen, dann gibt es einen Index m mit $Y_m = Y_{m+1} = \cdots$.

Nach Kor. 1.12 ist $\mathbb{A}^n$ mit der k-Zariski-Topologie ein noetherscher topologischer Raum (im wesentlichen, weil der Polynomring noethersch ist). Ebenso ist $\mathbb{P}^n$ noethersch (gleicher Beweis).

Definition 4.18. Es sei X ein topologischer Raum. Eine nicht-leere Teilmenge Y von X heißt **reduzibel**, wenn es abgeschlossene Teilmengen Y_1, Y_2 von Y gibt mit

$$Y = Y_1 \cup Y_2 \qquad \text{und} \qquad Y_1, Y_2 \neq Y.$$

Eine nicht-leere Menge heißt **irreduzibel**, wenn sie nicht reduzibel ist. Die leere Menge ist nicht irreduzibel. Eine k-Varietät heißt irreduzibel, wenn sie irreduzibel in der k-Zariski-Topologie ist.

Offenbar stimmt diese Definition für affine oder projektive k-Varietäten mit der vorigen überein.

Bemerkung 4.19. Man beachte die große Ähnlichkeit zwischen der allgemeinen Definition von Irreduzibilität in topologischen Räumen und der von Zusammenhang. Jede irreduzible Teilmenge ist zusammenhängend, aber die Umkehrung ist völlig falsch (siehe auch Übung 4.8)

Lemma 4.20. *Sei $\varphi\colon X \to Y$ eine stetige Abbildung zwischen topologischen Räumen. Ist $Z \subset X$ irreduzibel, so ist auch $\varphi(Z)$ irreduzibel.*

Beweis. Ist $\varphi(Z) \subset Z_1 \cup Z_2$ mit $Z_1, Z_2 \subset Y$ abgeschlossen, so folgt $Z \subset \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)$. Da φ stetig ist, sind $\varphi^{-1}(Z_1)$ und $\varphi^{-1}(Z_2)$ abgeschlossen. Also folgt $Z \subset \varphi^{-1}(Z_1)$ oder $Z \subset \varphi^{-1}(Z_2)$ und damit $\varphi(Z) = Z_1$ oder $\varphi(Z) = Z_2$. ∎

Proposition 4.21. *In einem noetherschen topologischen Raum X ist jede nicht-leere abgeschlossene Teilmenge Y eine endliche Vereinigung*

$$Y = Y_1 \cup \cdots \cup Y_m$$

von irreduziblen abgeschlossenen Teilmengen $Y_1, \ldots, Y_m$ mit $Y_i \not\subset Y_j$ für $i \neq j$. Diese Teilmengen sind bis auf Vertauschung eindeutig bestimmt und heißen die irreduziblen Komponenten von X.

Beweis. Geht genauso wie Satz 1.13. ∎

Proposition 4.22. *Es sei X ein topologischer Raum.*

(1) Der Abschluss einer irreduziblen Teilmenge von X ist irreduzibel.

(2) Ist X irreduzibel, so ist jede nicht-leere offene Teilmenge von X irreduzibel und dicht in X, das heißt je zwei nicht-leere offene Teilmengen von X haben nicht-leeren Schnitt.

Beweis. (1) Sei $Y \subset X$ irreduzibel. Falls $\overline{Y} = Y_1 \cup Y_2$ mit Y_1, Y_2 abgeschlossen in $\overline{Y}$, so folgt $Y \subset Y_1$ oder $Y \subset Y_2$, weil Y irreduzibel ist. Weil Y_1 und Y_2 abgeschlossen sind, folgt $\overline{Y} = Y_1$ oder $\overline{Y} = Y_2$.

(2) Sei $U \subset X$ offen, $U \neq \varnothing$. Dann gilt $X = \overline{U} \cup (X \setminus U)$. Weil X irreduzibel ist und $X \setminus U \subsetneq X$, folgt $\overline{U} = X$. Seien Y_1 und Y_2 abgeschlossene Teilmengen von X mit $U = (Y_1 \cap U) \cup (Y_2 \cap U)$. Wäre $Y_1 \cup Y_2 \subsetneq X$, so wäre $\overline{U} \subsetneq X$. Also folgt $Y_1 = X$ oder $Y_2 = X$, weil X irreduzibel ist. ∎

Übungen

Übung 4.7. Zeigen Sie, dass die Zariski-Topologie auf $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ nicht die Produkttopologie ist.

Übung 4.8. Zeigen Sie: Eine Teilmenge von $\mathbb{R}^n$ ist in der euklidischen Topologie genau dann irreduzibel, wenn sie aus einem einzigen Punkt besteht.

Übung 4.9. Beweisen Sie Prop. 4.14.

Übung 4.10. Es sei X ein topologischer Raum, $W \subset X$ eine Teilmenge. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) Jeder Punkt $p \in W$ besitzt eine offene Umgebung U in X derart, dass $Y \cap U$ abgeschlossen in U ist;
(ii) es gibt eine offene Teilmenge $U \subset X$ mit $W \subset U$ derart, dass W abgeschlossen in U ist;
(iii) es gibt eine offene Teilmenge $U \subset X$ und eine abgeschlossene Teilmenge $Z \subset X$ mit $W = U \cap Z$.

Eine Teilmenge W von X mit diesen Eigenschaften heißt **lokal abgeschlossen**.

Die quasiprojektiven (bzw. quasiaffinen) k-Varietäten sind nach (iii) also genau die lokal abgeschlossenen Teilmengen von $\mathbb{P}^n$ (bzw. $\mathbb{A}^n$) in der k-Zariski-Topologie.

Übung 4.11. Ein topologischer Raum X heißt *quasikompakt*, wenn jede offene Überdeckung von X eine endliche Teilüberdeckung besitzt[1]. Zeigen Sie:

(a) Jeder noethersche topologische Raum ist quasikompakt.
(b) Jeder Teilraum eines noetherschen Raums ist noethersch.
(c) Jeder noethersche Hausdorffraum ist endlich und diskret. (Das heißt alle Teilmengen sind offen.)

4.3. Reguläre Funktionen

Zu jeder affinen Varietät haben wir den Koordinatenring als einen Ring von Polynomfunktionen definiert. Wir führen nun Funktionenringe für beliebige Varietäten ein.

Definition 4.23. (1) Es sei $V \subset \mathbb{A}^n$ eine quasiaffine k-Varietät und sei $p \in V$ ein Punkt. Eine Funktion $f\colon V \to K$ heißt **regulär in** p, wenn es eine offene Umgebung U von p in V gibt und Polynome $g, h \in k[x_1, \ldots, x_n]$ derart, dass

$$f(q) = \frac{g(q)}{h(q)} \qquad \text{und} \qquad h(q) \neq 0 \qquad \text{für alle } q \in U.$$

(2) Es sei $V \subset \mathbb{P}^n$ eine quasiprojektive k-Varietät und sei $p \in V$ ein Punkt. Eine Funktion $f\colon V \to K$ heißt **regulär in** p, wenn es eine offene Umgebung U von p in V gibt und homogene Polynome $g, h \in k[x_0, \ldots, x_n]$ mit $\deg(g) = \deg(h)$ derart, dass

$$f(q) = \frac{g(q)}{h(q)} \qquad \text{und} \qquad h(q) \neq 0 \qquad \text{für alle } q \in U.$$

In beiden Fällen heißt die Funktion f **regulär auf** V, wenn sie in jedem Punkt von V regulär ist.

Lemma 4.24. *Jede reguläre Funktion auf V ist stetig bezüglich der k-Zariski-Topologie.*

[1]Manche Autoren nennen diese Eigenschaft auch schon kompakt. In der hier verwendeten Terminologie heißt ein Raum kompakt, wenn er quasikompakt ist und die Hausdorffsche Trennungseigenschaft besitzt.

Beweis. Sei $V \subset \mathbb{P}^n$ quasiprojektiv und $f\colon V \to K$ eine reguläre Funktion. Es genügt zu zeigen, dass Urbilder abgeschlossener Mengen abgeschlossen sind. Sei also $Y \subset K = \mathbb{A}^1$ eine k-abgeschlossene Menge, also $Y = \mathcal{V}(r)$, $r \in k[x]$. Es genügt zu zeigen, dass V überdeckt durch offene Mengen U überdeckt wird, mit der Eigenschaft, dass $U \cap f^{-1}(Y)$ abgeschlossen in U ist. Sei $p \in V$ und U eine offene Umgebung mit $f(q) = g(q)/h(q)$ für alle $q \in U$, mit $g, h \in k[x_0, \dots, x_n]$ homogen und vom selben Grad. Dann gilt also $q \in f^{-1}(Y) \cap U$ genau dann, wenn $r(f(q)) = r\big(g(q)/h(q)\big) = 0$. Wir bereinigen die Nenner und setzen

$$F(x_0, \dots, x_n) = h^{\deg(r)} \cdot r\left(\frac{g}{h}\right) \in k[x_0, \dots, x_n],$$

dann ist F homogen und es folgt $f^{-1}(Y) \cap U = \mathcal{V}_+(F) \cap U$. Damit ist $f^{-1}(Y) \cap U$ abgeschlossen in U. Weil f auf V regulär ist, wird V von solchen offenen Umgebungen überdeckt und die Behauptung ist bewiesen. Für quasiaffines V geht der Beweis genauso. ∎

Lemma und Definition 4.25. Für jede k-Varietät V bilden die regulären Funktionen $V \to K$ eine k-Algebra $\mathcal{O}(V)$, den **Ring der regulären Funktionen** auf V.

Beweis. Es seien $f_1, f_2\colon V \to K$ zwei reguläre Funktionen. Ist p ein Punkt von V und U_i eine offene Umgebung von p mit $f_i(q) = g_i(q)/h_i(q)$ für Polynome g_i, h_i $(i = 1, 2)$, dann ist $U_1 \cap U_2$ eine offene Umgebung von p, auf der $f_1 + f_2$ bzw. $f_1 \cdot f_2$ durch $\frac{g_1h_2+g_2h_1}{h_1h_2}$ bzw. durch $\frac{g_1g_2}{h_1h_2}$ repräsentiert werden. Also sind $f_1 + f_2$ und f_1f_2 regulär. Dass die Ringgesetze erfüllt sind, ist klar, weil es sich um Funktionen handelt. ∎

Bemerkung 4.26. Die Abbildung $\mathcal{O}\colon U \mapsto \mathcal{O}(U)$, die jeder offenen Teilmenge der Varietät V einen Ring zuordnet, hat die Eigenschaften einer sogenannten *Garbe* und heißt die **Strukturgarbe von** V. Das systematische Studium von Garben und ihrer Cohomologie ist ein wichtiges Element der modernen algebraischen und komplexen Geometrie (siehe zum Beispiel [Hartshorne]).

Die Definition einer regulären Funktion ist *lokal* im Sinn der Topologie, d.h. sie spielt sich in Umgebungen von Punkten ab. Im allgemeinen ist es aber nicht so einfach, den ganzen Ring $\mathcal{O}(V)$ für eine beliebige Varietät zu bestimmen. Wir machen uns jetzt an diese Bestimmung für affine und projektive Varietäten. Dazu stellen wir als erstes die Beziehung zu lokalen Ringen her.

Lemma und Definition 4.27. Es sei V eine k-Varietät und $p \in V$ ein Punkt. Sind U_1 und U_2 offene Umgebungen von p und $f_1 \in \mathcal{O}(U_1)$ und $f_2 \in \mathcal{O}(U_2)$ reguläre Funktionen, so definiere

$$f_1 \sim f_2 \qquad \Longleftrightarrow \qquad f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}.$$

Die Relation $\sim$ ist eine Äquivalenzrelation auf der Menge der Paare (f, U) bestehend aus einer offenen Umgebung U von p und einer regulären Funktion $f \in \mathcal{O}(U)$. Wir schreiben $[f]$ für die Äquivalenzklasse von f und nennen $[f]$ den durch f bestimmten **Funktionenkeim in** p. Wir schreiben $\mathcal{O}_{p,V}$ für die Menge aller Funktionenkeime. Gegeben $[f_1], [f_2] \in \mathcal{O}_{p,V}$ mit $f_1 \in \mathcal{O}(U_1)$ und $f_2 \in \mathcal{O}(U_2)$, dann definieren wir Summe und Produkt durch

$$[f_1] \dot{+} [f_2] = [f_1|_{U_1 \cap U_2} \dot{+} f_2|_{U_1 \cap U_2}].$$

Mit diesen Operationen wird $\mathcal{O}_{p,V}$ zu einem Ring, genannt der **lokale Ring von** V **im Punkt** p. Die Konstruktion von $\mathcal{O}_{p,V}$ ist lokal um p, d.h. ist $W \subset V$ eine offene Umgebung von p, so ist durch $[f] \mapsto [f|_W]$ ein Isomorphismus $\mathcal{O}_{p,V} \to \mathcal{O}_{p,W}$ gegeben.

Beweis. Übung. ∎

Ein Funktionenkeim im Punkt p ist keine Funktion, da der Definitionsbereich variabel ist. Nur im Punkt p selbst ist der Wert wohldefiniert. Insbesondere können wir definieren:

$$m_{p,V} = \big\{[f] \in \mathcal{O}_{p,V} \colon f(p) = 0\big\}.$$

Proposition 4.28. *Der Ring $\mathcal{O}_{p,V}$ ist ein lokaler Ring mit maximalem Ideal $m_{p,V}$.*

Lemma 4.29. *Sei R ein Ring und M ein Ideal in R. Genau dann ist R ein lokaler Ring mit maximalem Ideal M, wenn $R \setminus M = R^\times$ gilt.*

Beweis. Sei R ein lokaler Ring und M sein maximales Ideal. Wegen $M \subsetneq R$ gilt $M \subset R \setminus R^\times$. Ist umgekehrt $f \in R \setminus R^\times$, so folgt $1 \notin \langle f \rangle$. Also ist $\langle f \rangle$ in einem maximalen Ideal enthalten (nach dem Zornschen Lemma). Da R lokal ist, muss $f \in M$ gelten. Umgekehrt gelte $R \setminus M = R^\times$. Ist $I \subsetneq R$ ein Ideal, so gilt $I \cap R^\times = \varnothing$, also $I \subset M$. Damit ist R lokal mit maximalem Ideal M. ∎

Beweis von Prop. 4.28. Dies folgt nun leicht aus dem Lemma. Denn ist $[f] \in \mathcal{O}_{p,V} \setminus m_{p,V}$ mit $f \in \mathcal{O}(U)$, so gilt also $f(p) \neq 0$. Dann ist $W = \{p \in U \colon f(p) \neq 0\}$ offen und nicht-leer und es gilt $\frac{1}{f} \in \mathcal{O}(W)$. Also ist $[\frac{1}{f}] \in \mathcal{O}_{p,V}$ das Inverse von $[f]$, so dass $[f]$ eine Einheit in $\mathcal{O}_{p,V}$ ist. ∎

Statt sich auf einen einzelnen Punkt zu konzentrieren, kann man auch Funktionen betrachten, die nur irgendwo regulär sind.

Lemma und Definition 4.30. Es sei V eine irreduzible k-Varietät. Eine **rationale Funktion** auf V ist eine Äquivalenzklasse $[f]$ von Paaren (f, U) bestehend aus einer nicht-leeren offenen Teilmenge U von V und einer regulären Funktion $f \in \mathcal{O}(U)$, wobei $[f_1] = [f_2]$ für $f_1 \in \mathcal{O}(U_1)$ und $f_2 \in \mathcal{O}(U_2)$ genau dann gilt, wenn $f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$, wie zuvor.

Die rationalen Funktionen auf V bilden einer Körper $k(V)$, den **Funktionenkörper** von V. Die lokalen Ringe $\mathcal{O}_{p,V}$ sind Teilringe von $k(V)$ und es gilt $k(V) = \bigcup_{p \in V} \mathcal{O}_{p,V}$. Ist $U \subset V$ eine beliebige nicht-leere offene Teilmenge von V, so gilt $k(V) \cong k(U)$.

Beweis. Die Addition und Multiplikation von Äquivalenzklassen sind definiert wie zuvor im Fall der lokalen Ringe.[2] Beachte, dass der Schnitt von je zwei nicht-leeren offenen Teilmengen nicht leer ist, weil V irreduzibel ist (siehe Prop. 4.22(2)). Ist außerdem $[f] \in k(V)$ gegeben durch $f \in \mathcal{O}(U)$, $f \neq 0$, so ist die Menge $W = \{p \in U \colon f(p) \neq 0\}$ offen und nicht-leer, also $1/f \in \mathcal{O}(W)$ und $[f] \cdot [1/f] = 1$ in $k(V)$. Die weiteren Behauptungen sind leicht zu überprüfen (Übung). ∎

Als nächstes stellen wir die Beziehung zwischen den abstrakt definierten Ringen und Körpern von regulären Funktionen und dem Koordinatenring einer affinen Varietät her.

[2] Die Konstruktionen von $k(V)$ und $\mathcal{O}_{p,V}$ kann man auch beide formal als einen direkten Limes der Ringe $\mathcal{O}(U)$ (indiziert über alle offenen Mengen bzw. alle Umgebungen von p) beschreiben und so auf einmal abhandeln.

Satz 4.31. *Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät.*

(1) Es gilt $k[V] \cong \mathcal{O}(V)$.

(2) Ist V irreduzibel, so gilt $\mathrm{Quot}(k[V]) \cong k(V)$.

(3) Für jedes $p \in V$ sei $m_p = \{f \in k[V] : f(p) = 0\}$. Dann gilt $k[V]_{m_p} \cong \mathcal{O}_{p,V}$.

Beweis. (3) Wir können den Isomorphismus explizit angeben. Ist $p \in V$ und $\frac{f}{s} \in k[V]_{m_p}$, dann ist also $s \in k[V]$ mit $s(p) \neq 0$. Ist U die offene Menge $V \setminus \mathcal{V}(s)$, so ist durch $q \mapsto f(q)/s(q)$ also eine reguläre Funktion $U \to K$ gegeben. Der so definierte Ringhomomorphismus $k[V]_{m_p} \to \mathcal{O}_{p,V}$ ist surjektiv nach Definition der Funktionenkeime. Er ist auch injektiv: Denn ist U eine offene Umgebung von p mit $f(q)/s(q) = 0$ für alle $q \in U$, dann gibt es nach Lemma 4.13 ein Element $h \in k[V] \setminus m_p$ mit $p \in \mathcal{D}(h) \subset U$. Damit gilt $(hf)(q) = 0$ für alle $q \in V$, also $h \cdot (f \cdot 1 - 0 \cdot s) = 0$ in $k[V]$ und damit $\frac{f}{s} = \frac{0}{1} = 0$ in $k[V]_{m_p}$.

(1) Sei zunächst V irreduzibel. Per Definition gilt dann $\mathcal{O}(V) = \bigcap_{p \in V} \mathcal{O}_{p,V}$ (wobei wir den Durchschnitt innerhalb von $k(V)$ bilden). Aus (3) folgt deshalb $\mathcal{O}(V) = \bigcap k[V]_{m_p}$. Nach Lemma 1.39 kommen unter den m_p, $p \in V$, alle maximalen Ideale von $k[V]$ vor (tatsächlich sind es genau die maximalen Ideale). Deshalb folgt $\bigcap k[V]_{m_p} = k[V]$ aus Lemma 4.11.

Ist $V = V_1 \cup \cdots \cup V_r$ die Zerlegung von V in irreduzible Komponenten, so können wir $\mathcal{O}(V)$ als Teilring des direkten Produkts $\mathcal{O}(V_1) \times \cdots \mathcal{O}(V_r)$ auffassen, durch die injektive Abbildung $f \mapsto (f|_{V_1}, \ldots, f|_{V_r})$. Das gleiche gilt für $k[V]$, das wir als Teilring von $k[V_1] \times \cdots \times k[V_r]$ interpretieren können. Damit folgt $\mathcal{O}(V) \cong k[V]$ aus dem irreduziblen Fall.

(2) Aus (3) folgt $\mathrm{Quot}(\mathcal{O}_{p,V}) = \mathrm{Quot}(k[V]_{m_p}) = \mathrm{Quot}(k[V])$ für jedes $p \in V$. Außerdem gilt $\mathrm{Quot}(\mathcal{O}_{p,V}) \subset k(V)$, einfach weil $k(V)$ ein Körper ist, der $\mathcal{O}_{p,V}$ enthält. Also folgt $\mathrm{Quot}(k[V]) \subset k(V)$. Andererseits ist jedes Element von $k(V)$ in einem der Ringe $\mathcal{O}_{p,V}$ enthalten, was die umgekehrte Inklusion zeigt. ∎

Bei einer projektiven Varietät sieht die Sache etwas anders aus, denn die Elemente des homogenen Koordinatenrings sind ja keine Funktionen auf der Varietät. Stattdessen muss man immer Brüche von homogenen Polynomen desselben Grades bilden.

Satz 4.32. *Es sei $X \subset \mathbb{P}^n$ eine projektive k-Varietät.*

(1) Für die affine Varietät $V_i = X \cap D_+(x_i)$ gilt $k[V_i] \cong (k_+[X]_{\overline{x_i}})_0$ (für $i = 0, \ldots, r$).

(2) Ist X irreduzibel, so gilt $k(X) \cong \mathrm{Quot}(k_+[V])_0$.

(3) Für jeden Punkt $p \in X$ sei $m_p = \mathcal{I}_+(\{p\}) \subset k_+[X]$. Dann gilt $\mathcal{O}_{p,X} \cong (k_+[X]_{m_p})_0$.

Der Index 0 bezieht sich dabei auf den graduierten Teil vom Grad 0, wie in Lemma 4.12.

Beweis. (1) Die Abbildung $\alpha : k[y_0, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n] \to (k[x_0, \ldots, x_n]_{x_i})_0$ gegeben durch $y_j \mapsto x_j/x_i$ ist ein Isomorphismus von k-Algebren, und es gilt

$$\alpha(\mathcal{I}(V_i)) = (\mathcal{I}_+(X)_{x_i})_0.$$

Denn ist $f \in \mathcal{I}(V_i)$, so gilt $\alpha(f) = g/x_i^d$ mit $g \in k[x_0, \ldots, x_n]$ homogen vom Grad d, und es folgt $x_i g \in \mathcal{I}_+(X)$, also $g/x_i^d \in (\mathcal{I}_+(X)_{x_i})_0$. Umgekehrt gilt für $f/x_i^d \in (\mathcal{I}_+(X)_{x_i})_0$ offenbar

$f/x_i^d = \alpha(g)$ mit $g = f(y_0, \dots, y_{i-1}, 1, y_{i+1}, \dots, n) \in \mathcal{I}(V_i)$. Außerdem gilt (Übung 4.5):

$$k_+[X]_{\overline{x_i}} \cong (k[x_0, \dots, x_n]_{x_i})/(\mathcal{I}_+(X)_{x_i})$$

Nach dem Homomorphiesatz induziert α einen Isomorphismus $\overline{\alpha}\colon k[V_i] \xrightarrow{\sim} (k_+[X]_{\overline{x_i}})_0$.

(2) Wähle $i \in \{0, \dots, n\}$ mit $V_i \neq \varnothing$, dann gilt $k(X) \cong k(V_i)$ und damit $k(X) \cong \mathrm{Quot}(k[V_i])$ nach 4.31(2). Damit folgt die Behauptung aus (1).

(3) Sei $p \in X$ und wähle i mit $p \in V_i$. Nach (1) und 4.31(3) gilt dann $\mathcal{O}_{p,X} = \mathcal{O}_{p,V_i} = k[V_i]_{m'_p}$, mit $m'_p = \mathcal{I}(p) \subset k[V_i]$. Mit $\overline{\alpha}$ wie oben gilt dann $\overline{\alpha}(m'_p) = m_p \cdot (k_+[X]_{x_i})_0$. Wegen $p \in V_i$ gilt $\overline{x_i} \notin m_p$, deshalb folgt

$$(k_+[X]_{m_p})_0 = \big((k_+[X]_{\overline{x_0}})_{m_p}\big)_0 \cong k[V_i]_{m'_p} \cong \mathcal{O}_{p,X}. \qquad \blacksquare$$

Übungen

Übung 4.12. Es sei V eine irreduzible quasiprojektive Varietät und seien $f, g \in \mathcal{O}(V)$. Zeigen Sie: Falls es eine nicht-leere offene Teilmenge $U \subset V$ gibt mit $f|_U = g|_U$, dann gilt $f = g$.

Übung 4.13. Sei V eine k-Varietät und $p \in V$ ein Punkt. Finden Sie eine Bijektion zwischen den Primidealen des lokalen Rings $\mathcal{O}_{p,V}$ und der Menge aller abgeschlossenen irreduziblen Untervarietäten von V, die p enthalten.

Übung 4.14. Es sei V eine k-Varietät mit irreduziblen Komponenten $V_1, \dots, V_r$. Zeigen Sie

(a) Falls $V_i \cap V_j = \varnothing$ für alle $i \neq j$ gilt, so ist die Abbildung

$$\mathcal{O}(V) \to \mathcal{O}(V_1) \times \cdots \times \mathcal{O}(V_r),\ f \mapsto \big(f|_{V_1}, \dots, f|_{V_r}\big)$$

ein Isomorphismus von k-Algebren.

(b) Ist V endlich, so ist die Voraussetzung $V_i \cap V_j = \varnothing$ für $i \neq j$ immer erfüllt.
(*Vorschlag:* Sei $V = W_1 \cup W_2$ mit W_i abgeschlossen in V. Wende Lemma 1.30 auf W_1 und W_2 an.)

4.4. Morphismen

Morphismen von affinen Varietäten haben wir schon im ersten Kapitel untersucht. Für projektive Varietäten haben wir uns dagegen bisher auf die sogenannten globalen und lokalen Polynomabbildungen beschränkt. Wir erweitern nun den Begriff des Morphismus auf beliebige (quasiprojektive oder quasiaffine) Varietäten.

Definition 4.33. Es seien X und Y zwei k-Varietäten. Ein **Morphismus** zwischen X und Y ist eine stetige Abbildung

$$\varphi\colon X \to Y$$

mit folgender Eigenschaft: Für jede offene Teilmenge $U \subset Y$ und jede reguläre Funktion $f \in \mathcal{O}(U)$ ist die Funktion $f \circ \varphi\colon \varphi^{-1}(U) \to K$ wieder regulär.

Aus der Definition ist klar, dass Kompositionen von Morphismen wieder welche sind. Der Morphismus φ heißt ein **Isomorphismus**, wenn es einen Morphismus $\psi\colon Y \to X$ gibt mit $\psi \circ \varphi = \mathrm{id}_X$ und $\varphi \circ \psi = \mathrm{id}_Y$. Die Varietäten X und Y heißen **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt, in Zeichen $X \cong Y$.

Lemma 4.34. *Es seien X und Y zwei k-Varietäten und $\varphi\colon X \to Y$ eine stetige Abbildung. Genau dann ist φ ein Morphismus, wenn jeder Punkt $p \in X$ eine offene Umgebung U in X besitzt derart, dass die Einschränkung $\varphi|_U\colon U \to Y$ ein Morphismus ist.*

Beweis. Übung 4.17. ∎

Korollar 4.35 (Verklebung)**.** *Es seien X und Y zwei k-Varietäten. Gegeben eine offene Überdeckung $X = \bigcup_{i\in I} U_i$ von X und Morphismen $\varphi_i\colon U_i \to Y$ für jedes $i \in I$ mit $\varphi_i|_{U_i\cap U_j} = \varphi_j|_{U_i\cap U_j}$ für alle $i, j \in I$, dann ist*

$$\varphi\colon X \to Y, p \mapsto \varphi_i(p) \text{ für } p \in U_i$$

ein Morphismus.

Beweis. Nach dem Lemma genügt es zu bemerken, dass φ stetig ist. Das ist klar, weil die U_i offen und die φ_i stetig sind. ∎

Schon vorher haben wir den Schnitt einer projektiven Varietät in $\mathbb{P}^n$ mit D_i als affine Varietät behandelt, durch 'Identifikation' $D_i \cong \mathbb{A}^n$. Das können wir jetzt präziser machen, indem wir die Definition einer affinen Varietät entsprechend erweitern.

Definition 4.36. Eine k-Varietät X heißt **affin**, wenn es $n \in \mathbb{N}$ und eine k-abgeschlossene Teilmenge $Y \subset \mathbb{A}^n$ gibt mit $X \cong Y$.

Proposition 4.37. *Der Homöomorphismus*

$$\rho_i\colon \begin{cases} \mathbb{A}^n & \to & D_i \\ (a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) & \mapsto & [a_0, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n] \end{cases}$$

zwischen $\mathbb{A}^n$ und $D_i = \mathcal{D}_+(x_i) \subset \mathbb{P}^n$ ist ein Isomorphismus von Varietäten.

Beweis. Betrachte ohne Einschränkung den Fall $i = 0$. Eine reguläre Funktion auf D_0 ist lokal durch einen Bruch f/g von homogenen Polynomen gleichen Gerades gegeben. Dann ist durch $(f/g) \circ \rho_0 = f(1, y_1, \dots, y_n)/g(1, y_1, \dots, y_n)$ entsprechend lokal eine reguläre Funktion auf $\mathbb{A}^n$ gegeben. Die Umkehrabbildung von ρ_0 ist $\rho_0^{-1}\colon [a_0, \dots, a_n] \mapsto (a_1/a_0, \dots, a_n/a_0)$. Eine reguläre Funktion auf $\mathbb{A}^n$ ist lokal durch einen Bruch f/g, $f, g \in k[y_1, \dots, y_n]$ gegeben. Sei $d = \max\{\deg(f), \deg(g)\}$, dann gilt

$$\frac{f}{g} \circ \rho_0^{-1} = \frac{f(x_1/x_0, \dots, x_n/x_0)}{g(x_1/x_0, \dots, x_n/x_0)} = \frac{x_0^d f(x_1/x_0, \dots, x_n/x_0)}{x_0^d g(x_1/x_0, \dots, x_n/x_0)} = \frac{x_0^{d-\deg(f)} f^*}{x_0^{d-\deg(g)} g^*},$$

wobei f^*, g^* die Homogenisierung von f, g bezüglich x_0 ist. Dadurch ist lokal eine reguläre Funktion auf D_0 definiert. ∎

Die Teilmengen $\mathcal{D}_+(x_i)$ sind also **offene affine Untervarietäten** von $\mathbb{P}^n$.

Lemma 4.38. *Es sei X eine k-Varietät, $Y \subset \mathbb{A}^n$ eine affine k-Varietät. Eine Abbildung $\varphi\colon X \to Y$ ist genau dann ein Morphismus, wenn $x_i \circ \varphi$ für jedes $i = 1, \dots, n$ eine reguläre Funktion auf X ist, wobei $x_i\colon \mathbb{A}^n \to K$ die i-te Koordinatenfunktion ist.*

Beweis. Ist φ ein Morphismus, so sind die $x_i \circ \varphi$ nach Definition regulär. Umgekehrt seien die $x_i \circ \varphi$ alle regulär. Dann ist auch $f \circ \varphi$ für jedes $f \in k[x_1, \dots, x_n]$ regulär. Da die abgeschlossenen

Teilmengen von $\mathbb{A}^n$ von der Form $\mathcal{V}(f_1) \cap \cdots \mathcal{V}(f_r)$ mit $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ sind und reguläre Funktionen stetig sind, folgt, dass auch φ stetig ist. Außerdem sind die regulären Funktionen auf Y lokal durch Quotienten von Polynomen definiert. Deshalb ist $g \circ \varphi$ für jede reguläre Funktion g auf Y wieder regulär. Also ist φ ein Morphismus. ∎

Aus dem Lemma folgt, dass die Morphismen $X \to \mathbb{A}^1$ von einer k-Varietät X in die affine Gerade genau die regulären Funktionen auf X sind. Außerdem folgt, dass die neue Definition von Morphismus für affine Varietäten mit der alten übereinstimmt, das heißt es gilt das Folgende:

Proposition 4.39. *Es seien $V \subset \mathbb{A}^m$ und $W \subset \mathbb{A}^n$ affine k-Varietäten. Genau dann ist eine Abbildung $\varphi\colon V \to W$ ein Morphismus, wenn es $f_1, \ldots, f_n \in k[V]$ gibt mit $\varphi = (f_1, \ldots, f_n)$.*

Beweis. Ist $\varphi = (f_1, \ldots, f_n)$ durch Elemente von $k[V]$ gegeben, so gilt $x_i \circ \varphi = f_i \in \mathcal{O}(V) = k[V]$. Also ist φ ein Morphimus nach Lemma 4.38. Die Umkehrung folgt entsprechend. ∎

Auch offene Untervarietäten von affinen Varietäten (also quasiaffine Varietäten) können wieder affin sein, wie die folgende Aussage zeigt.

Proposition 4.40. *Es sei V eine affine k-Varietät und $f \in k[V]$, $f \neq 0$. Dann ist auch $U = V \setminus \mathcal{V}(f)$ affin, mit Koordinatenring $k[U] = k[V]_f$.*

Beweis. Betrachte die affine Varietät

$$W = \{(p, t) \in V \times \mathbb{A}^1 \colon\ t \cdot f(p) = 1\}.$$

Per Definition ist $1/f \in \mathcal{O}(U)$. Also ist

$$\varphi\colon U \to W, p \mapsto (p, 1/f(p))$$

ein Morphismus. Die Projektion $\pi\colon W \to U$, $(p, t) \mapsto p$ ist ein Morphismus und erfüllt offenbar $\pi \circ \varphi = \mathrm{id}_U$ und $\varphi \circ \pi = \mathrm{id}_W$. Also ist φ ein Isomorphismus. Der Koordinatenring ist $k[W] = k[V][t]/(tf - 1)$ und damit isomorph zu $k[V_f]$ (siehe §4.1). ∎

Die Beschreibung der Primideale von $k[V]_f$ in Prop. 4.5 entspricht genau der Tatsache, dass die irreduziblen Untervarietäten von $V \setminus \mathcal{V}(f)$ in Bijektion sind mit den irreduziblen Untervarietäten von V, die nicht in $\mathcal{V}(f)$ enthalten sind.

Beispiele 4.41. (1) Es sei $V = \mathbb{A}^1$ und $f = x$. Die offene Untervarietät $V \setminus \mathcal{V}(f) = \mathbb{A}^1 \setminus \{0\}$ ist affin mit Koordinatenring $k[x]_x$. Dieser Ring ist, genauso wie oben im Beweis, isomorph zu $k[x, y]/(xy - 1)$. Also ist $\mathbb{A}^1 \setminus \{0\}$ zu einer Hyperbel isomorph.

(2) Dagegen ist $\mathbb{A}^n \setminus \{0\}$, der affine Raum ohne den Ursprung, für $n \geqslant 2$ nicht affin. Siehe dazu Übung 4.18.

Korollar 4.42. *Sei X eine k-Varietät. Jede offene Teilmenge von X ist eine endliche Vereinigung von affinen offenen Untervarietäten. Insbesondere besitzt jeder Punkt eine affine offene Umgebung.*

Beweis. Ist $X \subset \mathbb{P}^n$ quasiprojektiv, so gilt zunächst $X = \bigcup_{i=0}^n (X \cap \mathcal{D}_+(x_i))$ und diese Teilmengen von X sind offen und quasiaffin. Es reicht deshalb, die Behauptung für den Fall zu zeigen, dass X selbst quasiaffin ist. Sei also $Y \subset \mathbb{A}^n$ eine affine k-Varietät und $X \subset Y$ offen in Y. Dann ist jede offene Teilmenge von X auch offen in Y und damit von der Form $Y \setminus \mathcal{V}(f_1, \ldots, f_r)$ für $f_1, \ldots, f_r \in$

$k[Y]$. Nach Prop. 4.40 ist $Y \setminus \mathcal{V}(f_i)$ affin für jedes i und es gilt $Y \setminus \mathcal{V}(f_1, \ldots, f_r) = \bigcup_{i=1}^{r}(Y \setminus \mathcal{V}(f_i))$. Damit ist die Behauptung bewiesen. ∎

Proposition 4.43. *Es seien $X \subset \mathbb{P}^m$, $Y \subset \mathbb{P}^n$ quasiprojektive Varietäten, und $\varphi\colon X \to Y$ eine stetige Abbildung. Genau dann ist φ ein Morphismus, wenn zu jedem Punkt $p \in X$ eine offene Umgebung U und homogene Polynome $f_0, \ldots, f_n \in k[x_0, \ldots, x_m]$ vom selben Grad existieren, derart, dass*

$$\varphi(q) = \big[f_0(q), \ldots, f_n(q)\big]$$

für alle $q \in U$ gilt. Insbesondere ist jede globale Polynomabbildung (siehe §3.5) ein Morphismus.

Beweis. Es sei φ ein Morphismus und $p \in X$ ein Punkt. Wähle i mit $\varphi(p) \in D_i \subset \mathbb{P}^n$ und setze $V = \varphi^{-1}(D_i)$. Ohne Einschränkung sei $i = 0$. Betrachte die regulären Funktionen $y_j/y_0 \in \mathcal{O}(D_0)$ für $j = 1, \ldots, n$. Dann sind die Kompositionen $\psi_j = (y_j/y_0) \circ \varphi$ regulär auf V. Deshalb gibt es eine offene Umgebung U von p in V und homogene Polynome $g_1, \ldots, g_n, h_1, \ldots, h_n \in k[x_0, \ldots, x_m]$ mit $\deg(g_i) = \deg(h_i)$, $\mathcal{V}_+(h_i) \cap U = \varnothing$ und $\psi_j = g_j/h_j$ auf U. Es gilt deshalb für alle $q \in U$:

$$\begin{aligned}\varphi(q) &= \big[1, \psi_1(q), \ldots, \psi_n(q)\big] = \left[1, \frac{g_1(q)}{h_1(q)}, \ldots, \frac{g_n(q)}{h_n(q)}\right] \\ &= \big[(h_1 \cdots h_n)(q), (g_1 h_2 \cdots h_n)(q), \ldots, (h_1 \cdots h_{n-1} g_n)(q)\big].\end{aligned}$$

Diese Produkte sind alle homogen vom selben Grad. Die Umkehrung folgt wieder analog. ∎

Beispiel 4.44.

Es sei $C = \mathcal{V}(x^2 + y^2 - z^2) \subset \mathbb{P}^2$ und betrachte

$$\varphi\colon \begin{cases} C & \to & \mathbb{P}^1 \\ [x, y, z] & \mapsto & [x, y - z] \end{cases}$$

So wie es da steht, ist φ undefiniert, falls $x = 0$ and $y = z$, also im Punkt $p = [0, 1, 1]$. Diese Abbildung ist die **stereographische Projektion** vom Punkt p, die $r \in C$, $r \neq p$ auf den Schnittpunkt der Geraden $\overline{pr}$ mit $\{y = 0\}$ abbildet. Betrachte die offene Menge $D_0 = \{[s, t] \in \mathbb{P}^1 \colon s \neq 0\}$ und setze $U = \varphi^{-1}(D_0)$. Für $[x, y, z] \in U$ gilt dann

$$\varphi[x, y, z] = [x, y - z] = \left[1, \frac{y - z}{x}\right].$$

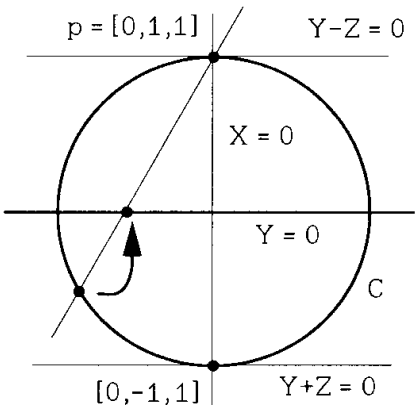


Bild in der affinen Ebene D_2

Bildquelle: [Harris], S. 20

Wegen $x^2 + y^2 = z^2$ folgt aber auch

$$\frac{y - z}{x} = \frac{y^2 - z^2}{x(y + z)} = \frac{-x^2}{x(y + z)} = \frac{-x}{y + z}.$$

Also ist die Einschränkung von φ auf U gegeben durch

$$\varphi[x, y, z] = \left[1, \frac{-x}{y + z}\right] = [y + z, -x],$$

und dieser Ausdruck *ist* definiert im Punkt $[0, 1, 1]$, nämlich $\varphi[0, 1, 1] = [1, 0]$, dafür aber nicht definiert in $[0, -1, 1]$. Also ist $\varphi\colon C \to \mathbb{P}^1$ ein Morphismus, lokal gegeben auf den offenen Mengen

$U_0 = C \setminus \{[0,1,1]\}$ und $U_1 = C \setminus \{[0,-1,1]\}$ durch

$$\varphi[x,y,z] = [x, y-z] \text{ für } [x,y,z] \in U_0 \quad \text{und} \quad \varphi[x,y,z] = [y+z, -x] \text{ für } [x,y,z] \in U_1.$$

Das war unser erstes Beispiel für einen Morphismus von projektiven Varietäten, der nicht durch eine globale Polynomabbildung gegeben ist. (Man kann beweisen, dass das in diesem Beispiel auch nicht möglich ist.) Wir diskutieren jetzt zwei allgemeinere Fälle: Die Projektion auf der Segre-Varietät sowie die Umkehrung der Veronese-Abbildung.

Satz 4.45. *Es sei $\sigma_{d,e}\colon \mathbb{P}^m \times \mathbb{P}^n \to \Sigma_{d,e}$ die Segre-Abbildung und $\pi\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^m$ die Projektion auf den ersten Faktor. Dann ist*

$$\pi \circ \sigma^{-1}\colon \Sigma_{m,n} \to \mathbb{P}^m$$

ein Morphismus.

Beweis. Per Definition ist $\sigma_{m,n}\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$ für $[u] \in \mathbb{P}^m$ und $[v] \in \mathbb{P}^n$ gegeben durch

$$\sigma_{m,n}([u],[v]) = [uv^T] = \left[u_0v_0, \dots, u_0v_n, u_1v_0, \dots, u_1v_n, \dots, u_mv_0, \dots, u_mv_n\right].$$

Wähle homogene Koordinaten z_{ij} auf $\mathbb{P}^{mn+m+n} = \mathbb{P}(\mathrm{Mat}_{(m+1)\times(n+1)}(K))$ und sei $U_i = \mathcal{D}_+(z_{i0})$ die offene Menge von Matrizen, in denen der erste Eintrag in der i-ten Spalte ungleich 0 ist. Ist $[uv^T] \in \Sigma_{m,n} \cap U_i$, dann muss $v_i \neq 0$ gelten. Es gilt deshalb $[uv^T] = [v_i^{-1} \cdot uv^T]$ und in dieser Matrix ist die i-te Spalte gleich u. Deshalb stimmt $\pi \circ \sigma^{-1}$ auf $U_i \cap \Sigma_{m,n}$ mit der Projektion

$$\pi_i\colon [a_{ij}] \mapsto [a_{i0}, \dots, a_{im}]$$

auf die i-te Spalte überein. Da $\pi \circ \sigma^{-1}$ stetig ist, ist es damit ein Morphismus nach Prop. 4.43. ∎

Satz 4.46. *Die Veronese-Abbildung $\nu_d\colon \mathbb{P}^n \to \mathbb{P}^{N-1}$, $N = \binom{n+d}{n}$, ist ein Isomorphismus $\mathbb{P}^n \xrightarrow{\sim} \nu_d(\mathbb{P}^n)$.*

Beweis. Da ν_d selbst eine globale Polynomabbildung ist, ist es ein Morphismus. Nach Prop. 3.36 ist ν_d außerdem injektiv. Sei $Z = \nu_d(\mathbb{P}^n)$. Dann müssen wir zeigen, dass die Umkehrabbildung $\nu_d^{-1}\colon Z \to \mathbb{P}^n$ ein Morphismus ist. Auf $\mathbb{P}^{N-1}$ arbeiten wir wieder mit homogenen Koordinaten z_α, $\alpha \in \Sigma$, $\Sigma = \{\alpha \in \mathbb{Z}_+^{n+1}\colon |\alpha| = d\}$. Wir haben gesehen, dass Z durch die quadratischen Gleichungen

$$Z = \mathcal{V}_+\left(z_\alpha z_\beta - z_\gamma z_\delta : \alpha + \beta = \gamma + \delta, \alpha, \beta, \gamma, \delta \in \Sigma\right)$$

gegeben ist. Betrachte für $i \in \{0, \dots, n\}$ und $\alpha \in \Sigma$ mit $\alpha_i \geqslant 1$ die Abbildung

$$\varphi_{\alpha,i}\colon Z \cap \mathcal{D}_+(z_\alpha) \to \mathbb{P}^n, z \mapsto [z_{\alpha - e_i + e_0}, z_{\alpha - e_i + e_1}, \dots, z_{\alpha - e_i + e_n}].$$

Diese Abbildung ist wohldefiniert, weil $z_\alpha \neq 0$ auf der rechten Seite vorkommt. Für $z \in Z \cap \mathcal{D}_+(z_\alpha z_\beta)$ mit $\alpha_i \geqslant 1$ und $\beta_j \geqslant 1$ gilt außerdem $\varphi_{\alpha,i}(z) = \varphi_{\beta,j}(z)$ wegen

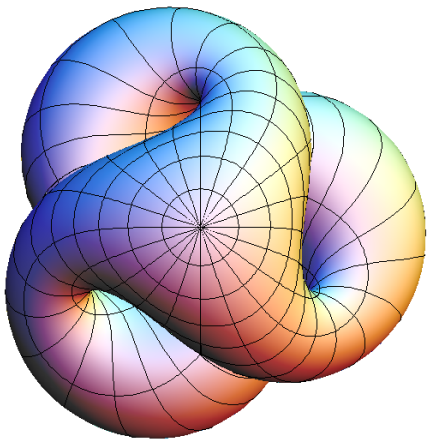
$$z_{\alpha - e_i + e_k} z_{\beta - e_j + e_l} = z_{\alpha - e_i + e_l} z_{\beta - e_j + e_k}.$$

Nach Kor. 4.35 verkleben die $\varphi_{\alpha,i}$ zu einem Morphismus $\varphi\colon Z \to \mathbb{P}^n$. Es gilt $\varphi \circ \nu_d = \mathrm{id}$, denn ist $x \in \mathbb{P}^n$ mit $x_i \neq 0$, so kann man $x = [a_0, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n]$ schreiben und sieht direkt $\varphi_{\alpha,i}(\nu_d(x)) = x$ für $\alpha = d \cdot e_d$. Also gilt $\varphi = \nu_d^{-1}$ und die Behauptung ist bewiesen. ∎

Korollar 4.47. *Es sei $f \in k[x_0, \dots, x_n]$ ein homogenes Polynom vom Grad d. Dann ist die offene Untervarietät $\mathcal{D}_+(f) \subset \mathbb{P}^n$ affin.*

Beweis. Sei $f = \sum_{|\alpha|=d} c_\alpha x^\alpha$. Unter der Veronese-Abbildung $\nu_d\colon \mathbb{P}^n \to \mathbb{P}^{N-1}$ gilt dann $\nu_d(\mathcal{D}_+(f)) = \nu_d(\mathbb{P}^n) \cap \mathcal{D}_+(\ell)$ mit $\ell = \sum_{|\alpha|=d} c_\alpha z_\alpha$ (vgl. Kor.3.38). Diese Varietät ist affin nach Prop. 4.37 (denn durch einen Koordinatenwechsel auf $\mathbb{P}^{N-1}$ können wir zum Beispiel $\ell = z_{e_0}$ erreichen). ∎

Beispiel 4.48. Es sei $k = \mathbb{R}$ und $f = x_0^2 + \cdots + x_n^2$. Nach dem vorangehenden Korollar ist $V = \mathbb{P}^n \smallsetminus \mathcal{V}_+(f)$ eine affine Varietät. Andererseits hat die Quadrik $\mathcal{V}_+(f)$ keine reellen Punkte. Deshalb haben V und $\mathbb{P}^n$ dieselben reellen Punkte. Für $n = 2$ gibt es also zum Beispiel eine affine Fläche $V \subset \mathbb{A}^n$ derart, dass $V \cap \mathbb{R}^n$ zum reellen projektiven Raum homöomorph ist. Allerdings besitzt V keine Einbettung in $\mathbb{A}^3$. Als reelle Mannigfaltigkeit erlaubt $\mathbb{P}^2_{\mathbb{R}}$ nur eine Immersion in $\mathbb{R}^3$ (mit Selbstdurchdringung). Eine solche Immersion ist zum Beispiel die sogenannte Boysche Fläche.



Boysche Fläche (*Bildquelle:* virtualmathmuseum.org)

Schließlich können wir den Hauptsatz der Eliminationstheorie auf die allgemeinere Situation von Morphismen zwischen projektiven Varietäten übertragen.

Satz 4.49. *Es sei X eine projektive k-Varietät und $\varphi\colon X \to \mathbb{P}^n$ ein Morphismus. Dann ist $\varphi(X)$ abgeschlossen.*

Beweis. Es gelte $X \subset \mathbb{P}^m$. Betrachte den Graph

$$\Gamma_\varphi = \{(p, q) \in \mathbb{P}^m \times \mathbb{P}^n \colon f(p) = q\}.$$

Dann ist Γ_φ eine abgeschlossene Teilmenge von $\mathbb{P}^m \times \mathbb{P}^n$. Um das zu sehen, sei U eine offene Teilmenge von X, auf der $\varphi|_U = (f_0, \ldots, f_n)$ durch homogene Polynome $f_0, \ldots, f_n \in k[x_0, \ldots, x_m]$ gleichen Grades gegeben ist. In homogenen Koordinaten $y_0, \ldots, y_n$ auf $\mathbb{P}^n$ gilt dann

$$\Gamma_\varphi \cap (U \times \mathbb{P}^n) = \mathcal{V}(y_i f_j - y_j f_i \colon i < j, i, j = 0, \ldots, n).$$

Denn ist $(p, q) = ([u], [v])$ in der linken Seite, so bedeutet $\varphi(p) = q$ gerade, dass die Vektoren $(f_0(u), \ldots, f_n(u))$ und $(v_1, \ldots, v_n)$ bis auf Skalierung übereinstimmen, was genau dann der Fall ist, wenn sie die angegebenen bihomogenen Gleichungen erfüllen. Also ist $\Gamma_\varphi \cap (U \times \mathbb{P}^n)$ abgeschlossen in $U \times \mathbb{P}^n$. Da X von solchen offenen Mengen U überdeckt wird, zeigt dies, dass Γ_φ abgeschlossen ist. (Unter der Projektion auf den ersten Faktor ist Γ_φ zu X isomorph).

Nach dem Hauptsatz der Eliminationstheorie wie in Kor. 3.41 ist die Projektion von Γ_φ auf $\mathbb{P}^n$ abgeschlossen. Das ist gerade $\varphi(X)$. ∎

Das zeigt einen ganz wesentlichen Unterschied zwischen projektiven und affinen Varietäten. Affine Varietäten, die zunächst als abgeschlossene Teilmengen von $\mathbb{A}^n$ definiert sind, können auch zu nicht-abgeschlossenen Untervarietäten von affinen oder projektiven Räumen isomorph sein (so wie die offenen affinen Untervarietäten $D_i \subset \mathbb{P}^n$). Dagegen kann eine projektive Varietät immer nur als abgeschlossene Teilmenge eines projektiven Raums auftreten.

Beispiel 4.50. Im Unterschied zu projektiven Varietäten ist das Bild einer quasiprojektiven Varietät unter einem Morphismus im allgemeinen nicht nur nicht abgeschlossen, sondern noch nicht einmal wieder eine quasiprojektive Varietät. Betrachte zum Beispiel den Morphismus

$$\varphi\colon \mathbb{A}^2 \to \mathbb{A}^2,\ (x_1, x_2) \mapsto (x_1, x_1x_2).$$

Das Bild von φ in Koordinaten y_1, y_2 ist die die Menge

$$W = (\mathbb{A}^2 \setminus \mathcal{V}(y_1)) \cup \{(0,0)\}.$$

Dies ist keine quasiprojektive Varietät, denn W ist nicht offen in seinem Abschluss $\mathbb{A}^2$.

Allzu wild können die Bilder von Morphismen dann allerdings doch nicht werden. Eine Teilmenge von $\mathbb{P}^n$ heißt **konstruierbar**, wenn sie eine endliche Vereinigung von quasiprojektiven Varietäten ist.[3] Es gilt dann der folgende allgemeine Satz, der auf Chevalley[4] zurückgeht, den wir allerdings weder beweisen noch verwenden.

Satz 4.51. *Das Bild einer konstruierbaren Menge unter einem Morphismus ist konstruierbar.*

Beweis. Siehe zum Beispiel [Harris], Satz 3.16. ∎

Als Folgerung aus Satz 4.49 bekommen wir auch eine Charakterisierung des Rings $\mathcal{O}(X)$ der regulären Funktionen auf einer irreduziblen projektiven Varietät.

Korollar 4.52. *Es sei $X \subset \mathbb{P}^n$ eine irreduzible projektive k-Varietät.*

(1) Der Ring $\mathcal{O}(X)$ ist isomorph zu einer endlichen Körpererweiterung von k.

(2) Falls $X \cap \mathbb{P}^n_k \neq \varnothing$, so gilt $\mathcal{O}(X) = k$. Insbesondere gilt $\mathcal{O}(X) = k$, falls k algebraisch abgeschlossen ist.

Beweis. (1) Da X irreduzibel ist, ist X nicht-leer. Es sei $p \in X$ ein Punkt. Dann gibt es eine endliche Körpererweiterung L/k mit $p \in \mathbb{P}^n_L$ (nämlich $L = k(a_0, \ldots, a_n)$, $p = [a_0, \ldots, a_n]$). Es sei

$$\mu_p\colon \mathcal{O}(X) \to L, f \mapsto f(p)$$

der Auswertungshomomorphismus im Punkt p. Jedes $f \in \mathcal{O}(X)$ ist ein Morphismus $X \to \mathbb{A}^1$ und durch Komposition mit der Inklusion $\mathbb{A}_1 \cong D_0 \subset \mathbb{P}^1$ können wir f als Morphismus $X \to \mathbb{P}^1$ auffassen. Nach Satz 4.49 ist $f(X)$ abgeschlossen in $\mathbb{P}^1$. Wegen $f(X) \subset D_0 \subsetneq \mathbb{P}^1$ muss $f(X)$ endlich sein. Da X irreduzibel ist, ist außerdem $f(X)$ irreduzibel. Ist also $\mu_p(f) = f(p) = 0$, so folgt bereits $f(X) = \{0\}$, also $f = 0$. Dies zeigt, dass μ_p injektiv ist. Also ist $\mathcal{O}(X)$ ein Teilring der endlichen Körpererweiterung L/k und damit selbst eine endliche Körpererweiterung, was (1) beweist. (2) folgt mit dem gleichen Argument, indem wir $p \in X \cap \mathbb{P}^n_k$ und $L = k$ wählen. ∎

[3] Äquivalent ist dies die kleinste Menge von Teilmengen von $\mathbb{P}^n$, die die projektiven Varietäten enthält und unter endlichen booleschen Operationen (also Vereinigung, Durchschnitt und Komplementbildung) abgeschlossen ist.

[4] Claude Chevalley (1909–1984), französisch-amerikanischer Mathematiker

Bemerkung 4.53. In der komplexen Geometrie gilt die Aussage, dass jede holomorphe Funktion auf einer zusammenhängenden kompakten komplexen Mannigfaltigkeit konstant ist (eine Verallgemeinerung des Satzes von Liouville über beschränkte holomorphe Funktionen auf $\mathbb{C}$). Wir haben gerade bewiesen, dass die entsprechende Aussage für reguläre Funktionen auf einer komplexen projektiven Varietät gilt. Diese Tatsache ist einer der Ausgangspunkte für eine äußerst weitgehende Analogie zwischen (glatten) projektiven Varietäten über $\mathbb{C}$ und kompakten komplexen Mannigfaltigkeiten, die historisch weit zurückreicht und in ihrer modernen Form häufig unter dem Stichwort 'GAGA' läuft (nach einer einflussreichen Arbeit von J.P. Serre mit dem Titel 'Géométrie Algébrique et Géométrie Analytique').

Korollar 4.54. *Eine k-Varietät ist genau dann gleichzeitig affin und projektiv, wenn sie endlich ist.*

Beweis. Ist X eine projektive Varietät, so ist $\mathcal{O}(X)$ eine endliche Körpererweiterung von k. Ist X auch affin, so gilt dasselbe für den Koordinatenring $k[X]$. Dann muss X endlich sein (siehe Übung 4.20 oder Kor. 4.80). Umgekehrt ist jede endliche projektive Varietät bis auf Koordinatenwechsel in einer der affinen offenen Untervarieäten D_i enthalten und damit affin. Jede endliche affine Varietät ist isomorph zu ihrem projektiven Abschluss. ∎

Als Anwendung der vorangehenden Resultate bekommen wir eine Verallgemeinerung von Kor. 3.27, mit einem überraschend einfachen Beweis.

Korollar 4.55. *Es sei $X \subset \mathbb{P}^n$ eine unendliche projektive k-Varietät und $Y \subset \mathbb{P}^n$ eine Hyperfläche. Dann gilt $X \cap Y \neq \emptyset$.*

Beweis. Wenn Y eine Hyperfläche ist, dann ist das Komplement $U = \mathbb{P}^n \setminus Y$ affin nach Kor. 4.47. Falls $X \cap Y = \emptyset$, dann ist die projektive Varietät X also in U enthalten und damit auch affin. Nach dem vorangehenden Korollar ist das nur möglich, wenn X endlich ist. ∎

Übungen

Übung 4.15. Betrachte den Morphismus $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^2$, $\varphi(t) = (t^2, t^3)$. Das Bild von φ ist die Neilsche Parabel $C = \mathcal{V}(y^2 - x^3)$. Zeigen Sie, dass φ ein Homöomorphismus von $\mathbb{A}^1$ auf C ist. (Andererseits wissen wir nach Beispiel 1.53, dass φ kein Isomorphismus ist, weil $k[C] \not\cong k[t]$ gilt.)

Übung 4.16. Beweisen Sie die folgende Verallgemeinerung von Prop. 1.51 und Prop. 4.39. Es sei X eine k-Varietät, Y eine affine k-Varietät. Dann gibt es eine natürliche (funktorielle) Bijektion zwischen den Morphismen $X \to Y$ und den Homomorphismen $k[Y] \to \mathcal{O}(X)$ von k-Algebren.

Übung 4.17. Beweisen Sie Lemma 4.34

Übung 4.18*. Es sei $W = \mathbb{A}^2 \setminus \{(0,0)\}$ die affine Ebene ohne den Ursprung. Zeigen Sie:

(a) Die Abbildung $k[x,y] = \mathcal{O}(\mathbb{A}^2) \to \mathcal{O}(W)$, $f \mapsto f|_W$ ist ein Isomorphismus.
(*Hinweise:* Sei $f \in \mathcal{O}(W)$ und U eine offene Teilmenge von W mit $f|_U = g/h$, $g, h \in k[x,y]$, mit $\mathrm{ggT}(g,h) = 1$ und $\deg(h) > 0$. Zeigen Sie, dass U echt in W enthalten sein muss. Überlegen Sie, was gelten muss, wenn f auf zwei verschiedenen offenen Mengen durch solche Darstellungen gegeben ist.)

(b) Folgern Sie, dass W keine affine Varietät sein kann.

Übung 4.19. Es sei $C \subset \mathbb{P}^3$ die verdrehte Kubik. Unter der Veronese-Abbildung ist C isomorph zu $\mathbb{P}^1$. Zeigen Sie, dass $k_+[C]$ und $k_+[\mathbb{P}^1]$ jedoch nicht-isomorphe k-Algebren sind. Dies zeigt, dass Kor. 1.52 sich nicht auf affine Varietäten überträgt. (*Vorschlag:* Sei $\widehat{C} \subset \mathbb{A}^4$ der affine Kegel über C, $p = (0,0,0,0)$ und $m = \mathcal{I}(p) \subset k[\widehat{C}]$. Bestimmen Sie die Dimension des k-Vektorraums m/m^2.)

Übung 4.20. Es sei V eine affine k-Varietät. Zeigen Sie: Falls $\dim_k(k[V]) < \infty$, so ist V endlich. (Siehe Übung 1.35 für die Umkehrung.) (*Vorschlag:* Nehmen Sie $k = K$ an und zeigen Sie, dass V nicht mehr als $\dim(k[V])$ Punkte enthalten kann. Für den allgemeinen Fall muss man etwas Körpertheorie benutzen.)

Übung 4.21. Es seien $X, Y \subset \mathbb{A}^n$ affine k-Varietäten und sei

$$\Delta = \{(p,p) \subset \mathbb{A}^n \times \mathbb{A}^n = \mathbb{A}^{2n} : p \in \mathbb{A}^n\}$$

die **Diagonale** in $\mathbb{A}^n \times \mathbb{A}^n$. Zeigen Sie, dass die Abbildung

$$\varphi: \begin{cases} X \cap Y & \to & (X \times Y) \cap \Delta \\ p & \mapsto & (p,p) \end{cases}$$

ein Isomorphismus von k-Varietäten ist.

Übung 4.22. Es sei X eine quasiprojektive k-Varietät und seien $U, V \subset X$ offene affine Untervarietäten. Zeigen Sie, dass $U \cap V$ wieder affin ist. (*Hinweis:* Verwenden Sie Übung 4.21).

Übung 4.23. Es sei k ein Körper, der nicht algebraisch abgeschlossen ist. Zeigen Sie:
(a) Für jedes $n \geqslant 2$ gibt es ein homogenes Polynom $f \in k[x_0, \ldots, x_n]$, $f \notin k$, mit $\mathcal{V}_+(f) \cap \mathbb{P}^n_k = \varnothing$. (*Vorschlag:* Induktion nach n.)
(b) Zu jeder projektiven k-Varietät X existiert eine offene affine Untervarietät $V \subset X$ mit $X \cap \mathbb{P}^n_k \subset V$.

4.5. Rationale Abbildungen und Varietäten

In der projektiven Geometrie haben wir schon die Bedeutung von Abbildungen gesehen, die nicht überall definiert sind, wie zum Beispiel Projektionen. Solche Abbildungen untersuchen wir jetzt allgemein und stellen die Beziehung zum Funktionenkörper her.

Definition 4.56. Seien X und Y zwei irreduzible k-Varietäten. Eine **rationale Abbildung** von X nach Y ist eine Äquivalenzklasse $[\varphi]$ von Paaren (φ, U) bestehend aus einer nicht-leeren offenen Teilmenge U von X und einem Morphismus $\varphi: U \to Y$. Dabei ist die Äquivalenz wieder definiert durch $(\varphi_1, U_1) \sim (\varphi_2, U_2)$, falls

$$\varphi_1|_{U_1 \cap U_2} = \varphi_2|_{U_1 \cap U_2}$$

gilt. Wir schreiben kurz

$$\varphi: X \dashrightarrow Y.$$

Beispiele 4.57. Sei $X \subset \mathbb{P}^m$ eine irreduzible quasiprojektive k-Varietät.

(1) Jede rationale Funktion $f \in k(X)$ definiert eine rationale Abbildung $X \dashrightarrow \mathbb{A}^1$. Denn per Definition ist f regulär auf einer nicht-leeren offenen Teilmenge U von X und $f: U \to \mathbb{A}^1$ ist ein Morphismus.

(2) Ist $p \in X$ ein Punkt, so ist durch die Projektion $\pi_p: X \setminus \{p\} \to \mathbb{P}^{m-1}$ mit Zentrum p eine rationale Abbildung $X \dashrightarrow \mathbb{P}^{m-1}$ gegeben.

(3) Allgemeiner definiert jede lokale Polynomabbildung von X nach $\mathbb{P}^n$, gegeben durch homogene Polynome $f_0, \dots, f_n \in k[x_0, \dots, x_m]$ gleichen Grades mit $X \not\subset \mathcal{V}(f_0, \dots, f_n)$, eine rationale Abbildung $X \dashrightarrow \mathbb{P}^n$, repräsentiert durch den Morphismus

$$X \setminus \mathcal{V}(f_0, \dots, f_n) \to \mathbb{P}^n, p \mapsto [f_0(p), \dots, f_n(p)].$$

Tatsächlich hat jede rationale Abbildung $\varphi\colon X \dashrightarrow \mathbb{P}^n$ einen Repräsentanten von dieser Form. Denn ist $\psi\colon U \to \mathbb{P}^n$ ein Morphismus auf einer nichtleeren offenen Teilmenge $U \subset X$, der φ repräsentiert, so gibt es nach Prop. 4.43 eine nichtleere offene Teilmenge $V \subset U$, so dass $\psi|_U$ wie oben durch homogene Polynome vom selben Grad gegeben ist. Per Definition repräsentiert $\psi|_U$ dieselbe rationale Abbildung wie ψ.

Ist $\varphi\colon X \dashrightarrow Y$ eine rationale Abbildung zwischen irreduziblen k-Varietäten, dann gibt es eine maximale offene Teilmenge U von X derart, dass φ durch einen Morphismus $U \to Y$ repräsentiert wird, nämlich die Vereinigung

$$\operatorname{dom}(\varphi) = \bigcup_{(\psi, U) \in [\varphi]} U$$

aller Definitionsbereiche von Repränsentaten von φ. Die offene Teilmenge $\operatorname{dom}(\varphi)$ heißt der **Definitionsbereich** von φ. Das **Bild** $\operatorname{im}(\varphi)$ von φ ist definiert als $\varphi(\operatorname{dom}(\varphi))$.

Beispiel 4.58. Sei $\pi_p\colon X \to \mathbb{P}^{n-1}$ die Projektion von einem Punkt wie oben. Dann gilt $X \setminus \{p\} \subset \operatorname{dom}(\pi_p)$ per Definition. Das Zentrum der Projektion p kann ebenfalls in $\operatorname{dom}(\pi_p)$ liegen, womit π_p dann ein Morphismus ist wie die stereographische Projektion in Beispiel 4.44, oder auch nicht, wie zum Beispiel im Fall $X = \mathbb{P}^n$.

Eine rationale Abbildung $\varphi\colon X \dashrightarrow Y$ zwischen irreduziblen Varietäten heißt **dominant**, wenn $\operatorname{im}(\varphi)$ dicht in Y ist (äquivalent: wenn $\operatorname{im}(\varphi)$ eine offene Teilmenge enthält). Ist φ dominant und $\psi\colon Y \to Z$ eine weitere rationale Abbildung, so ist die Komposition

$$\psi \circ \varphi\colon X \dashrightarrow Z$$

wohldefiniert, nämlich durch die Einschränkung von $\psi \circ \varphi$ auf $\operatorname{dom}(\varphi) \cap \varphi^{-1}\big(\operatorname{dom}(\psi)\big)$.

Nicht-dominante rationale Abbildungen lassen sich dagegen im allgemeinen nicht komponieren. Ist zum Beispiel $\varphi\colon X \dashrightarrow \mathbb{P}^n$ die konstante Abbildung, die X auf einen Punkt $p \in \mathbb{P}^n$ abbildet und ist $\psi\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$ die Projektion mit Zentrum p, so ist $\psi \circ \varphi$ nicht definiert.

Definition 4.59. Eine rationale Abbildung $\varphi\colon X \dashrightarrow Y$ heißt **birational**, wenn es eine rationale Abbildung $\psi\colon Y \dashrightarrow X$ mit $\psi \circ \varphi = \mathrm{id}_X$ und $\varphi \circ \psi = \mathrm{id}_Y$ gibt. Die irreduziblen k-Varietäten X und Y heißen **birational äquivalent**, wenn es eine birationale Abbildung zwischen ihnen gibt.

Per Definition sind X und Y birational äquivalent, wenn es offene Untervarietäten $U \subset X$ und $W \subset Y$ gibt mit $U \cong W$. Insbesondere ist eine irreduzible Varietät birational äquivalent zu jeder nicht-leeren offenen Untervarietät. Damit sind zum Beispiel der projektive und der affine Raum derselben Dimension birational äquivalent.

Beispiel 4.60. Die Parabel $C = \mathcal{V}(y - x^2)$ und die Hyperbel $C' = \mathcal{V}(1 - xy)$ in der affinen Ebene sind nicht isomorph (siehe Übung 1.38), denn es gilt $C \cong \mathbb{A}^1$ aber $C' \cong \mathbb{A}^1 \setminus \{0\}$ (Beispiel 4.41). Parabel und Hyperbel sind also nicht isomorph, aber birational äquivalent.

Proposition 4.61. *Jede dominante rationale Abbildung $\varphi\colon X \dashrightarrow Y$ zwischen zwei irreduziblen k-Varietäten induziert eine Inklusion*

$$\varphi^{\#}\colon k(Y) \hookrightarrow k(X),\ f \mapsto f \circ \varphi$$

der Funktionenkörper. Umgekehrt kommt jede auf k konstante Inklusion $k(Y) \hookrightarrow k(X)$ in dieser Weise von einer dominanten rationalen Abbildung $X \dashrightarrow Y$.

Beweis. Weil φ dominant ist, ist $\varphi^{\#}(f) = f \circ \varphi$ für jedes $f \in k(Y)$ eine rationale Abbildung $X \dashrightarrow \mathbb{A}^1$ und damit ein Element von $k(X)$. Es ist klar, dass $\varphi^{\#}$ ein Ringhomomorphismus ist und 1 auf 1 abbildet. Also ist $\varphi^{\#}$ Homomorphismus von Körpern und damit injektiv. Sei umgekehrt $\alpha\colon k(Y) \hookrightarrow k(X)$ irgendein solcher Homomorphismus. Sei $V \subset Y$ eine nichtleere offene affine Untervarietät von Y. Dann gibt eine abgeschlossene Teilmenge $W \subset \mathbb{A}^n$ mit $V \cong W$ und es gilt $\mathcal{O}(V) \cong k[W] = k[x_1, \dots, x_n]/\mathcal{I}(W)$ und damit $k(Y) \cong k(V) \cong k(W) \cong \mathrm{Quot}(k[x_1, \dots, x_n]/\mathcal{I}(W))$. Setze $f_i = \alpha(\overline{x_i}) \in k(X)$. Dann ist $\varphi = (f_1, \dots, f_n)\colon X \dashrightarrow \mathbb{A}^n$ die gesuchte rationale Abbildung mit $\varphi^{\#} = \alpha$ (vgl. Beweis von Prop. 1.51(3)). ∎

Korollar 4.62. *Genau dann sind zwei Varietäten X und Y birational, wenn ihre Funktionenkörper isomorph sind.* ∎

Definition 4.63. Eine Varietät heißt **rational**, wenn sie birational zu einem projektiven (oder affinen) Raum ist. Der Funktionenkörper

$$k(\mathbb{P}^n) \cong k(\mathbb{A}^n) = k(x_1, \dots, x_n)$$

heißt der **rationale Funktionenkörper** in n Variablen über k.

Nach Prop. 4.61 ist eine Varietät also genau dann k-rational, wenn ihr Funktionenkörper zu einem rationalen Funktionenkörper isomorph ist.

Proposition 4.64. *Ist k ein unendlicher Körper und $X \subset \mathbb{P}^n$ eine rationale irreduzible k-Varietät, dann ist die Menge der k-rationalen Punkte $X \cap \mathbb{P}^n_k$ Zariski-dicht in X.*

Beweis. Da X rational ist, gibt es nicht-leere offene Teilmengen $U \subset \mathbb{A}^m$ für ein $m \geqslant 0$ und $W \subset X$ und einen Isomorphismus $\varphi\colon U \xrightarrow{\sim} W$. Da φ ein Isomorphismus von k-Varietäten ist, gilt $\varphi(U \cap k^n) \subset \mathbb{P}^n_k$. Da k^m Zariski-dicht in $\mathbb{A}^m$ ist (weil k unendlich ist), ist $U \cap k^m$ Zariski-dicht in U. Deshalb ist $\varphi(U \cap k^m)$ Zariski-dicht in W und damit in X. ∎

Die Bezeichnung *rationale Punkte* kommt dabei vom Fall $k = \mathbb{Q}$, der für die Zahlentheorie besonders relevant ist. Zum Beispiel benutzt man eine rationale Parametrisierung des Einheitskreises $\mathcal{V}(x^2 + y^2 - 1)$ (siehe Übung 4.25), um alle pythagoräischen Zahlentripel aufzulisten (also alle Tripel $a, b, c \in \mathbb{Z}$ mit $a^2 + b^2 = c^2$; teilen durch c^2 in einer solchen Gleichung gibt einen rationalen Punkt auf der Einheitskreislinie). Die berühmte Fermatsche Vermutung[5], bewiesen im Jahr 1995 von A. Wiles und R. Taylor, besagt, dass die Kurve $\mathcal{V}(x^n + y^n - 1)$ für $n \geqslant 3$ keine rationalen Punkte mit $x, y \neq 0$ besitzt. Diese Kurve kann also insbesondere nicht rational sein (was im Unterschied zur Fermatschen Vermutung lange bekannt und nicht besonders schwer

[5]aufgestellt von Pierre de Fermat (1607–1665)

zu beweisen ist; den Fall $n = 3$ diskutieren wir gleich). Der Teil der Zahlentheorie, der sich mit rationalen Punkten auf algebraischen Varietäten beschäftigt, ist die *arithmetische Geometrie*.

Beispiel 4.65. Im Fall von Quadriken hat Prop. 4.64 auch eine einfache Umkehrung: Es sei $\operatorname{char}(k) \neq 2$ und $f \in k[x_0, \dots, x_n]$ eine nicht-ausgeartete quadratische Form. Genau dann ist die Quadrik $X = \mathcal{V}_+(f) \subset \mathbb{P}^n$ rational, wenn $\mathcal{V}(f) \cap \mathbb{P}^n_k \neq \varnothing$ gilt. Die eine Richtung ist klar aus Prop. 4.64. Umgekehrt sei $p \in X \cap \mathbb{P}^n_k$ ein k-rationaler Punkt. Wir können durch Koordinatenwechsel $p = [1, 0, \dots, 0]$ annehmen. Betrachte die Projektion π_p mit Zentrum p auf die Hyperebene $H = \mathcal{V}_+(x_0) \cong \mathbb{P}^{n-1}$, gegeben durch $q \mapsto \overline{pq} \cap H$. Diese Projektion ist birational. Der anschauliche Grund ist folgender: Für jedes $r \in H$ ist die Gerade $\overline{pr}$ entweder in X enthalten oder hat zwei Schnittpunkte mit X. Einer davon ist p, der andere das eindeutige Urbild von r unter π_p; die genaue Umsetzung dieser Beweisidee ist Übung 4.28.

Zum Abschluss diskutieren wir noch den Fall kubischer Kurven in der Ebene. Diese sind im allgemeinen nicht rational. Deshalb kann man ihre rationalen Punkte nicht durch Parametrisierung finden, was in der Zahlentheorie eine wichtige Rolle spielt (Stichwort: Elliptische Kurven).

Satz 4.66. *Es gelte* $\operatorname{char}(k) \neq 2, 3$ *und sei* $f \in k[x]$ *mit* $\deg(f) = 3$. *Genau dann ist die ebene kubische Kurve* $\mathcal{V}(y^2 - f) \subset \mathbb{A}^2$ *rational, wenn* f *eine doppelte Nullstelle hat.*

Diese Aussage wird meistens mit etwas mehr Theorie bewiesen. Den folgenden direkten Beweis habe ich von [Reid] kopiert. Zur Vorbereitung ein Lemma, das auf Fermat zurückgeht.

Lemma 4.67 (Fermats unendlicher Abstieg)**.** *Es gelte* $\operatorname{char}(k) \neq 2$ *und seien* $f, g \in k[t]$ *zwei teilerfremde Polynome. Angenommen es gibt vier verschiedene Punkte* $[\lambda, \mu] \in \mathbb{P}^1_k$ *derart, dass*

$$\lambda f + \mu g$$

bis auf Skalierung ein Quadrat in $k[t]$ *ist. Dann folgt* $f, g \in k$.

Beweis. Wir beweisen die Behauptung für Polynome f, g vom Grad höchstens d durch Induktion nach d. Für $d = 0$ ist nichts zu zeigen. Sei also $d \geqslant 1$. Wir können den Körper k durch seinen algebraischen Abschluss ersetzten, ohne dass das an Voraussetzung oder Behauptung etwas ändert. Es gelte also $k = \overline{k}$. Ist $T \in \mathrm{GL}_2(k)$, so gilt

$$\begin{pmatrix} \lambda & \mu \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} \lambda & \mu \end{pmatrix} T^{-1} \cdot T \begin{pmatrix} f \\ g \end{pmatrix}.$$

und offenbar gilt $(f, g)^t \in k^2$ genau dann, wenn $T(f, g)^t \in k^2$. Wir können deshalb auf die vier Punkte in $\mathbb{P}^1$ aus der Voraussetzung eine Projektivität anwenden und (nach Kor. 3.3) annehmen, dass diese gerade $[0, 1], [1, 0], [1, -1], [1, -\lambda] \in \mathbb{P}^1_k$ sind, mit $\lambda \in k \smallsetminus \{0, 1\}$. Also sind

$$f, g, f - g, f - \lambda g$$

Quadrate. Es gibt also zwei teilerfremde Polynome $u, v \in k[t]$ mit $f = u^2$ und $g = v^2$. Da

$$\begin{aligned} f - g &= u^2 - v^2 = (u + v)(u - v) \\ f - \lambda g &= u^2 - \lambda v^2 = (u + \sqrt{\lambda} v)(u - \sqrt{\lambda} v). \end{aligned}$$

ebenfalls Quadrate sind und u und v teilerfremd sind, sind die $u+v, u-v, u+\sqrt{\lambda}v, u-\sqrt{\lambda}v$ ebenfalls Quadrate. Nach Induktionsvoraussetzung folgt $u, v \in k$ und damit auch $f, g \in k$. ∎

Beweis von Thm. 4.66. Es sei $C = \mathcal{V}(f)$. Falls f eine doppelte Nullstelle hat, dann muss diese in k liegen. Durch Koordinatenwechsel können wir dann annehmen, dass $f = x^2(c-x)$ für $c \in k$ gilt. Eine Parametrisierung dieser Kubik haben wir schon ziemlich zu Anfang in Übung 1.17 konstruiert: Sie ist das Bild des Morphismus $\varphi\colon t \mapsto (c-t^2, t(c-t^2))$. Die Umkehrung ist die Abbildung $\psi\colon (x,y) \mapsto y/x$; denn es gilt $\psi(\varphi(t)) = t$ für $t^2 \neq c$ und aus $y^2 = x^2(c-x)$ folgt $(y/x)^2 = c-x$ und deshalb $\varphi(\psi(x,y)) = (c-(y/x)^2, y/x(c-(y/x)^2)) = (x,y)$ für $x \neq 0$.

Angenommen f hat keine doppelte Nullstelle. Wir können $k = \overline{k}$ annehmen, denn wenn C über $\overline{k}$ schon keine rationale Parametrisierung hat, dann erst recht nicht über k. Durch Koordinatenwechsel können wir dann erreichen, dass $f = x(x-1)(x-c)$ für $c \in k \setminus \{0,1\}$ gilt. Es sei $\varphi\colon \mathbb{A}^1 \dashrightarrow C$ eine rationale Abbildung, gegeben durch ein Paar $(p/q, r/s)$ von rationalen Funktionen. Das heißt also $p, q, r, s \in k[t]$ sind Polynome mit $\mathrm{ggT}(p,q) = 1$, $\mathrm{ggT}(r,s) = 1$ und

$$\left(\frac{r}{s}\right)^2 = \left(\frac{p}{q}\right)\left(\frac{p}{q}-1\right)\left(\frac{p}{q}-c\right).$$

Bereinigen der Nenner gibt

$$r^2q^3 = s^2p(p-q)(p-cq).$$

Weil p, q sowie r, s teilerfremd sind, folgt $s^2 | q^3$ und $q^3 | s^2$, also $s^2 = aq^3$ für $a \in k^\times$. Dann ist

$$aq = \left(\frac{s}{q}\right)^2$$

ein Quadrat in $k[t]$. Außerdem folgt durch Einsetzen von $s^2 = aq^3$ in die obige Gleichung

$$r^2 \sim p(p-q)(p-cq).$$

Es folgt, dass $p, q, p-q, p-cq$ bis auf Skalierung Quadrate in $k[t]$ sind. Nach dem Lemma von Fermat folgt daraus $p, q \in k$ und aus den obigen Gleichungen dann auch $r, s \in k$. Also ist die rationale Abbildung φ konstant und damit nicht birational. ∎

Bemerkung 4.68. Eine irreduzible k-Varietät X heißt **unirational**, wenn es eine dominante rationale Abbildung $\mathbb{P}^n \dashrightarrow X$ (über k) für ein $n \in \mathbb{Z}_+$ gibt. Äquivalent ist nach Prop. 4.61, dass der Funktionenkörper $k(X)$ in einem rationalen Funktionenkörper $k(x_1, \ldots, x_n)$ enthalten ist.

Nach einem klassischen Satz von Lüroth[6] ist jede unirationale Kurve rational. Entsprechendes gilt nach einem Satz von Castelnuovo[7] für Flächen, falls $\mathrm{char}(k) = 0$. In Primzahlcharakteristik ist dies dagegen falsch, Gegenbeispiele sind die sogenannten *Zariski-Flächen*. Schließlich zeigten Clemens und Griffiths[8] sowie (unabhängig) Iskowskich und Manin[9] in den Jahren 1971-72 die Existenz von unirationalen komplexen Varietäten der Dimension 3, die nicht rational sind. Diese Sätze sind ziemlich kompliziert.

[6] Jacob Lüroth (1844–1910)
[7] Guido Castelnuovo (1865–1952)
[8] C. H. Clemens und P. A. Griffiths, „The Intermediate Jacobian of the cubic threefold", *Annals of Mathematics*, Vol. 95, No. 2 (1972)
[9] V. A. Iskowskich und Ju. I. Manin, „Three-dimensional quartics and counterexamples to the Lüroth problem", *Matematicheskii Sbornik* Novaya Seriya 86 (1971)

Elementar betrachtet sind die unirationalen Varietäten per Definition genau die „parametrisierbaren“ Varietäten. Unirationalität ist etwas besser fassbar als Rationalität. Zum Beispiel kann man verhältnismäßig leicht beweisen, dass jede kubische Hyperfläche in $\mathbb{P}^n$ für $n \geqslant 3$ unirational ist. Welche kubischen Hyperflächen rational sind, ist dagegen im allgemeinen unbekannt.

Übungen

Übung 4.24. Betrachten Sie die **quadratische Cremona-Transformation**

$$\varphi\colon \begin{cases} \mathbb{P}^2 & \dashrightarrow & \mathbb{P}^2 \\ [x_0, x_1, x_2] & \mapsto & [x_1x_2, x_0x_2, x_0x_1] \end{cases}.$$

Zeigen Sie, dass φ birational ist mit $\varphi^{-1} = \varphi$. Bestimmen Sie Definitionsbereich und Bild. Beschreiben Sie die Einschränkung von φ auf die drei Geraden $\mathcal{V}_+(x_0x_1x_2)$.

Übung 4.25. Es gelte $\operatorname{char}(k) \neq 2$ und sei $C = \mathcal{V}(x^2 + y^2 - 1) \subset \mathbb{A}^2$. Zeigen Sie, dass durch

$$\varphi\colon \begin{cases} \mathbb{A}^1 & \dashrightarrow & C \\ t & \mapsto & \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right) \end{cases}.$$

eine birationale Abbildung gegeben ist. Bestimmen Sie Umkehrabbildung, Definitionsbereich und Bild.

Übung 4.26. Es seien V und W zwei irreduzible k-Varietäten und $\varphi\colon V \to W$ eine rationale Abbildung. Zeigen Sie, dass $\overline{\varphi(V)}$ irreduzibel ist.

Übung 4.27. Es sei $\varphi\colon \mathbb{P}^1 \dashrightarrow \mathbb{P}^n$ eine rationale Abbildung. Zeigen Sie, dass $\operatorname{dom}(\varphi) = \mathbb{P}^1$ gilt, mit anderen Worten, dass φ ein Morphismus ist. (Das erklärt die Beobachtung in Übung 3.36.)

Übung 4.28. Es gelte $\operatorname{char}(k) \neq 2$ und es sei $f \in k[x_0, \ldots, x_n]$ eine nicht-ausgeartete quadratische Form. Beweisen Sie die folgenden Aussagen:

(a) Gibt es $a \in k^{n+1} \smallsetminus \{0\}$ mit $f(a) = 0$, so lässt sich f durch linearen Koordinatenwechsel in die Form

$$x_0x_1 + \widetilde{f}(x_2, \ldots, x_n)$$

bringen, wobei $\widetilde{f} \in k[x_2, \ldots, x_n]$ eine nicht-ausgeartete quadratische Form ist.

(b) Ist $p \in \mathcal{V}_+(f) \subset \mathbb{P}^n_k$, so ist die Projektion $\pi_p\colon \mathcal{V}_+(f) \dashrightarrow \mathbb{P}^{n-1}$ mit Zentrum p birational.

(c) Die Quadrik $\mathcal{V}_+(f)$ ist genau dann rational, wenn sie einen k-rationalen Punkt besitzt.

(d)* Zeigen Sie, dass (a)–(c) nicht notwendig richtig sind, wenn f ausgeartet ist.

Übung 4.29. (*Cayley-Transformation*) Es sei $\operatorname{char}(k) \neq 2$ und sei $M = \operatorname{Mat}_{n\times n}(K)$ der affine Raum der $n \times n$-Matrizen. Betrachte die Abbildung

$$\varphi\colon \begin{cases} M & \dashrightarrow & M \\ A & \mapsto & \frac{I-A}{I+A} \end{cases},$$

wobei I die Einheitsmatrix ist. (Die Notation als Bruch ist gerechtfertigt, denn ist $I + A$ invertiebar, so gilt $(I + A)^{-1}(I - A) = (I - A)(I + A)^{-1}$.) Zeigen Sie:

(a) Die Abbildung φ ist eine rationale Abbildung mit $\varphi^2 = \mathrm{id}_M$.

(b) Die Einschränkung von φ auf den Raum $S \subset M$ der schiefsymmetrischen Matrizen in M induziert eine birationale Abbildung $S \dashrightarrow \mathrm{SO}_n(K)$. (*Hinweis:* Aus $A = -A^T$ folgt $\det(I + A) = \det(I - A)$.)

4.6. Dimension

Wir haben die Diskussion des Dimensionsbegriffs lange aufgeschoben. In Kapitel 3 wurde die Dimension einer projektiven Varietät mit Hilfe des Hilbert-Polynoms definiert. Jetzt diskutieren wir den allgemeinen Fall, wobei allerdings einiges unbewiesen bleiben wird. Tatsächlich gibt es mehrere äquivalente Möglichkeiten die Dimension zu definieren. Die erste ist rein topologisch:

Definition 4.69. Es sei X ein topologischer Raum. Die **(kombinatorische) Dimension** von X ist definiert als das Supremum aller $n \in \mathbb{Z}_+$ derart, dass eine Kette

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$$

von irreduziblen abgeschlossenen Teilmengen von X existiert. Sie wird mit $\dim(X)$ bezeichnet. Die Dimension der leeren Menge ist als $-\infty$ definiert. Die Dimension einer Teilmenge von $\mathbb{A}^n$ oder $\mathbb{P}^n$ definieren wir als ihre Dimension als topologischer Raum, mit der durch die k-Zariski-Topologie gegebenen Teilraumtopologie. Insbesondere ist die Dimension einer quasiprojektiven Varietät in dieser Weise definiert.

Diese Definition der Dimension passt intuitiv zur Dimension in der linearen Algebra: Die Dimension eines Vektorraums ist die maximale Länge einer strikt aufsteigenden Kette von linearen Unterräumen (also einer sogenannten *Fahne*).

Der kombinatorische Dimensionsbegriff ist intuitiv, aber seine formale Behandlung ist nicht ganz einfach. Um die grundlegenden Aussagen der Dimensionstheorie zu beweisen, braucht man eine ganze Menge kommutative Algebra. Die Dimension hat die folgenden Eigenschaften:

(D1) Der affine Raum $\mathbb{A}^n$ und der projektive Raum $\mathbb{P}^n$ haben die Dimension n.

(D2) Sind X und Y Varietäten, so gilt $\dim(X \times Y) = \dim(X) + \dim(Y)$.

(D3) Ist X eine Varietät mit irreduziblen Komponenten $X_1, \ldots, X_r$, so gilt

$$\dim(X) = \max\{\dim(X_i) \colon i = 1, \ldots, r\}.$$

(D4) Für jede quasiprojektive (bzw. quasiaffine) Varietät U in $\mathbb{P}^n$ (bzw. $\mathbb{A}^n$) gilt

$$\dim(U) = \dim(\overline{U}).$$

(D5) Sind X und Y Varietäten mit $Y \subset X$, so gilt $\dim(Y) \leqslant \dim(X)$. Ist zusätzlich X irreduzibel und $Y \neq X$ abgeschlossen in X, so folgt $\dim(Y) < \dim(X)$.

(D6a) Ist $V \subset \mathbb{A}^n$ eine irreduzible affine Varietät und $f \in k[x_1, \ldots, x_n]$ ein nicht-konstantes Polynom mit $V \not\subset \mathcal{V}(f)$, dann gilt

$$\dim(V \cap \mathcal{V}(f)) = \dim(V) - 1.$$

(D6p) Ist $X \subset \mathbb{P}^n$ eine irreduzible projektive Varietät und $f \in k[x_0, \ldots, x_n]$ ein nicht-konstantes homogenes Polynom mit $X \not\subset \mathcal{V}_+(f)$, dann gilt

$$\dim(X \cap \mathcal{V}_+(f)) = \dim(X) - 1.$$

(D7) Eine Varietät ist genau dann nulldimensional, wenn sie endlich ist.

Hinter einigen dieser Aussagen verbergen sich dicke Sätze der kommutativen Algebra. Sie werden deshalb in dieser Vorlesung nicht bewiesen. Wir werden aber die Eigenschaften (D1)–(D7), ihre Folgerungen und ihre algebraischen Grundlagen diskutieren.

(D1) Die Fahne

$$\{0\} = \mathcal{V}(x_1, \ldots, x_n) \subsetneq \mathcal{V}(x_2, \ldots, x_n) \subsetneq \cdots \subsetneq \mathcal{V}(x_n) \subsetneq \mathbb{A}^n.$$

zeigt sofort, dass die Dimension von $\mathbb{A}^n$ mindestens n ist. Sie übersetzt sich in eine gleichlange Kette von Primidealen

$$\langle 0\rangle \subsetneq \langle x_n\rangle \subsetneq \langle x_n, x_{n-1}\rangle \subsetneq \cdots \subsetneq \langle x_1, \ldots, x_n\rangle \qquad (*)$$

in $k[x_1, \ldots, x_n]$, die Verschwindungsideale der betreffenden irreduziblen Mengen.

Frage 4.70. Wie sieht eine entsprechende Kette von Untervarietäten und homogenen Idealen aus, die $\dim(\mathbb{P}^n) \geqslant n$ zeigt?

Definition 4.71. Es sei R ein Ring. Die **Krull**[10]**-Dimension von** R ist die größte Zahl n derart, dass eine Kette

$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n \subsetneq R$$

von Primidealen in R existiert.

Proposition 4.72. *Die Dimension einer affinen k-Varietät stimmt mit der Krull-Dimension ihres Koordinatenrings überein.*

Beweis. Eine Inklusion $Z_1 \subsetneq Z_2$ von irreduziblen abgeschlossenen Untervarietäten einer affinen Varietät V entspricht der Inklusion von Primidealen $\mathcal{I}(Z_2) \subsetneq \mathcal{I}(Z_1)$ in $k[V]$, und umgekehrt. Außerdem gilt $P = \mathcal{I}(\mathcal{V}(P))$ für jedes Primideal $P \subset k[V]$. Daraus folgt die Behauptung. ∎

Eigenschaft (D1) sagt also für den affinen Raum gerade, dass sich die Kette $(*)$ von Primidealen im Polynomring nicht weiter verfeinern lässt und es auch sonst keine längere Kette gibt[11].

(D2) Die Dimensionsformel für das Produkt $\dim(X \times Y) = \dim(X) + \dim(Y)$ ist klar aus (D1) für affine Räume $X = \mathbb{A}^m$, $Y = \mathbb{A}^n$. Mit (D3) folgt sie auch leicht für $X = \mathbb{P}^m$ und $Y = \mathbb{P}^n$, indem man bemerkt, dass $\mathbb{A}^m \times \mathbb{A}^n \cong D_+(x_0) \times D_+(y_0)$ eine dichte Teilmenge von $\mathbb{P}^m \times \mathbb{P}^n$ ist.

Für den allgemeinen Fall kann man genauso darauf reduzieren, dass X und Y affin sind. Dann verwendet man, dass der Koordatenring $k[X \times Y]$ isomorph ist zum *Tensorprodukt* $k[X] \otimes_k k[Y]$, was wir nicht diskutiert haben. Dann beweist man die Dimensionsaussage für das Tensorprodukt (zum Beispiel mit Hilfe der Noether-Normalisierung).

(D3) Das ist nun zur Abwechslung eine leichte Folgerung der Definition. Denn jede Kette von irreduziblen Teilmengen von X muss in einer der irreduziblen Komponenten enthalten sein, woraus die Behauptung sofort folgt.

[10] Wolfgang Krull (1899–1971)

[11] Die Frage, ob sich jede Kette von Primidealen zu einer Kette maximaler Länge verfeinern lässt, ist eine weitere ringtheoretische Frage, die wir nicht vertiefen wollen. Tatsächlich gibt es noethersche Ringe, in denen das nicht der Fall ist. Allerdings sind solche Ringe ziemlich exotisch und tauchen kaum in der algebraischen Geometrie auf.

(D4) Diese Aussage ist dagegen nicht rein topologisch. (Man kann exotische Beispiele von topologischen Räumen konstruieren, in denen (D4) für die kombinatorische Dimension nicht gilt.) Der Beweis benutzt die algebraische Charakterisierung über Primidealketten.

(D5) Das folgt wieder leicht aus der Definition. Denn in einer Kette $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ von irreduziblen abgeschlossenen Teilmengen von Y hat jedes Z_i die Form $Z_i = \widetilde{Z}_i \cap Y$ mit $\widetilde{Z}_i$ abgeschlossen und irreduzibel in X. Daraus folgt sofort $\dim(Y) \leqslant \dim(X)$. Ist Y abgeschlossen mit $Y \subsetneq X$ und ist X irreduzibel, dann kann man $\widetilde{Z}_i = Z_i$ setzen und außerdem die Kette in X mit $Z_{n+1} = X$ verlängern, so dass $\dim(Y) < \dim(X)$ gelten muss.

(D6) Aus (D5) folgt sofort $\dim(V \cap \mathcal{V}(f)) < \dim(V)$, aber es nicht klar, dass die Dimension nicht um mehr als 1 sinken kann. Von Anfang an haben wir *Hyperflächen* definiert als Varietäten, die durch eine einzige Gleichung gegeben sind. Eigenschaft (D6) sagt für $V = \mathbb{A}^n$ oder $X = \mathbb{P}^n$ gerade, dass jede Hyperfläche die Dimension $n-1$ hat. Tatsächlich gilt auch die Umkehrung:

Satz 4.73. *Eine irreduzible affine Varietät $V \subset \mathbb{A}^n$ hat genau dann die Dimension $n-1$, wenn es ein irreduzibles Polynom $f \in k[x_1, \ldots, x_n]$ mit $V = \mathcal{V}(f)$ gibt.* ∎

Das projektive Analogon gilt ebenfalls und folgt relativ leicht aus der affinen Version durch Übergang zum projektiven Abschluss. Der algebraische Hintergrund ist der **Krullsche Hauptidealsatz**, ein weiteres Ergebnis der kommutativen Algebra, das wir nicht beweisen; siehe dazu [Eisenbud], Kapitel 10.

Aus (D6) folgt durch Induktion:

Proposition 4.74. *Für jedes $r \geqslant 0$ und Polynome $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ bzw. homogene Polynome $f_1, \ldots, f_r \in k[x_0, \ldots, x_n]$ gilt*

$$\dim(\mathcal{V}(f_1, \ldots, f_r)) \geqslant n - r \qquad \textit{bzw.} \qquad \dim(\mathcal{V}_+(f_1, \ldots, f_r)) \geqslant n - r$$ ∎

Im Unterschied zum Fall $r = 1$ ist es aber weit schwieriger, die Gleichheit in dieser Aussage zu charakterisieren. In der linearen Algebra kann man die Dimension des Lösungsraums eines linearen Gleichungssystems leicht bestimmen, indem man den Rang der Koeffizientenmatrix ausrechnet, also die Abhängigkeiten zwischen den Gleichungen bestimmt. Insbesondere lässt sich jeder lineare Unterraum der Dimension $n-r$ in $\mathbb{A}^n$ durch genau r Gleichungen beschreiben.

Für nicht-lineare Gleichungssysteme ist das nicht wahr, sobald mehr als eine Gleichung im Spiel ist. Wir betrachten die Situation im projektiven Raum. Eine projektive Varietät $X \subset \mathbb{P}^n$ der Dimension $n-r$ heißt ein **mengentheoretisch vollständiger Durchschnitt**, wenn es homogene Polynome $f_1, \ldots, f_r \in k[x_0, \ldots, x_n]$ gibt derart, dass

$$X = \mathcal{V}_+(f_1, \ldots, f_r)$$

gilt. Mit anderen Worten, X ist der Durchschnitt von r Hyperflächen. Die Varietät X heißt ein **vollständiger Durchschnitt**, wenn es $f_1, \ldots, f_r$ mit der stärkeren Eigenschaft

$$\mathcal{I}_+(X) = \langle f_1, \ldots, f_r \rangle$$

gibt. Meistens ist man eher an dieser stärkeren Eigenschaft interessiert als an der mengentheoretischen. Aus Satz 4.73 folgt, dass jede Hyperfläche in $\mathbb{P}^n$ ein vollständiger Durchschnitt ist.

Beispiel 4.75. Das einfachste Beispiel für eine Varietät, die *kein* vollständiger Durchschnitt ist, ist die verdrehte Kubik in $\mathbb{P}^3$:

$$C = \mathcal{V}_+(f_0, f_1, f_2), \quad \text{mit} \quad \begin{cases} f_0 = x_0x_2 - x_1^2, \\ f_1 = x_0x_3 - x_1x_2, \\ f_2 = x_1x_3 - x_2^2. \end{cases}$$

Per Definition liegen die drei quadratischen Formen f_0, f_1, f_2 im homogenen Verschwindungsideal $\mathcal{I}_+(C)$, und sie sind linear unabhängig. Da C nicht in einer Ebene liegt, enthält $\mathcal{I}_+(C)$ keine Linearformen. Deshalb muss jedes homogene Erzeugendensystem von $\mathcal{I}_+(C)$ die Polynome f_0, f_1, f_2 enthalten. Andererseits ist C ein mengentheoretisch vollständiger Durchschnitt. Man kann zwar keine der drei Gleichungen weglassen (wenn man das tut, erhält man immer die Kurve C und zusätzlich noch eine Gerade). Es gilt aber

$$C = \mathcal{V}_+\big(x_0x_2 - x_1^2, x_2(x_1x_3 - x_2^2) - x_3(x_0x_3 - x_1x_2)\big).$$

Das alles haben wir in Übung 3.24 gezeigt. Es ist ein *ungelöstes Problem*, ob jede Kurve in $\mathbb{P}^3$ der Durschnitt von zwei Flächen, also ein mengentheoretisch vollständiger Durchschnitt ist.

Im affinen Raum oder in lokalen Ringen wird die Sache etwas einfacher. (Zum Beispiel ist die verdrehte Kubik in $\mathbb{A}^3$ ein vollständiger Durchschnitt.) Auch hier kann es allerdings Probleme geben, wenn Singularitäten ins Spiel kommen (siehe Übung 4.32).

(D7) Das ist leicht zu sehen, wenn $k = K$ gilt. Denn in diesem Fall ist eine endliche Teilmenge einer Varietät genau dann irreduzibel, wenn sie aus einem einzigen Punkt besteht. Deshalb ist jede endliche Varietät nach (D3) nulldimensional. Ist umgekehrt V eine nulldimensionale Varietät, dann kann V keine irreduzible Komponente mit mehr als einem Punkt haben (denn die hätte Dimension $\geqslant 1$). Da eine Varietät nur endlich viele irreduzible Komponenten hat, muss V dann endlich sein. Im Fall $k \subsetneq K$ braucht man etwas mehr Körpertheorie, um (D7) zu beweisen. Siehe dazu Übung 1.35, Übung 4.20 und Kor. 4.80.

Damit ist unsere Diskussion der Eigenschaften (D1)-(D7) abgeschlossen.

Der Befehl `dim` berechnet in Macaulay2 die Dimension eines Rings oder einer affinen Varietät. Für ein Ideal I in einem Ring R ist $\dim(I)$ dabei die kombinatorische Dimension des Restklassenrings R/I, im Fall des Polynomrings also die Dimension der zugehörigen affinen Varietät.

```
i1 : R=QQ[x,y,z];
i2 : I=ideal(1-x^3-y^3-z^3);
i3 : dim(I)
o3 = 2

i4 : V=Spec(R/I)
o4 = V
o4 : AffineVariety

i5 : dim(V)
o5 = 2
```

Die Dimension einer projektiven Varietät, definiert durch ein homogenes Ideal, ist dagegen bekanntlich um eins kleiner als die Dimension des affinen Kegels. Man kann Macaulay2 explizit mitteilen, dass man eine projektive Varietät betrachten möchte, mit dem Befehl `Proj`.

```
i6 : S=QQ[x0,x1,x2,x3];
i7 : I=ideal(x0^3-x1^3-x2^3-x3^3);
i8 : dim(I)
o8 = 3

i9 : X=Proj(S/I)
o9 = X
o9 : ProjectiveVariety

i10 : dim(X)
o10 = 2
```

Es gibt noch eine andere algebraische Charakterisierung der Dimension, nämlich über den Transzendenzgrad des Funktionenkörpers. Dazu etwas Terminologie aus der Algebra.

Definition 4.76. Es sei K/k eine Körpererweiterung. Eine Familie $(a_i : i \in I)$ von Elementen aus K heißt **algebraisch unabhängig** über k, wenn der k-Algebren-Homomorphismus

$$k[t_i : i \in I] \to K, t_i \mapsto a_i$$

injektiv ist, andernfalls **algebraisch abhängig**. Jede maximale algebraisch unabhängige Familie heißt eine **Transzendenzbasis** von K über k. Der **Transzendenzgrad** von K über k ist die Mächtigkeit einer Transzendenzbasis, geschrieben $\operatorname{trdeg}_k(K)$.

Eine Familie von Elementen aus K ist also genau dann algebraisch unabhängig, wenn es zwischen ihren Elementen keine nicht-triviale polynomiale Identitität mit Koeffizienten in k gibt. Natürlich muss man die Existenz von maximalen algebraisch unabhängigen Familien und die Wohldefiniertheit des Transzendenzgrads beweisen. Im wesentlichen zeigt man dazu, dass sich algebraische Unabhängigkeit formal genauso verhält, wie lineare Unabhängigkeit. Der entscheidende Schritt ist dabei, wie in der linearen Algebra, der *Austauschsatz*:

Lemma 4.77. *Es seien B und B' zwei endliche Transzendenzbasen von K/k und sei $b \in B$. Dann gibt es $b' \in B'$, so dass auch $(B \setminus \{b\}) \cup \{b'\}$ eine Transzendenzbasis ist.*

Für den Beweis und alle weiteren Details siehe [Bosch], Kapitel 7. Der Zusammenhang mit der Dimension steckt in der folgenden algebraischen Aussage.

Satz 4.78. *Es sei A eine endlich erzeugte, nullteilerfreie k-Algebra. Dann gilt*

$$\dim(A) = \operatorname{trdeg}_k\big(\operatorname{Quot}(A)\big).$$

Beweis. siehe [Eisenbud], Kapitel 13, Thm. A. ∎

Aus Satz 4.78 folgt sofort die Dimensionseigenschaft (D1) für den affinen Raum, da der Quotientenkörper des Polynomrings der rationale Funktionenkörper $k(x_1, \ldots, x_n)$ vom Transzendenzgrad n ist. Außerdem folgt:

Korollar 4.79. *Die Dimension einer irreduziblen k-Varietät X stimmt mit dem Transzendenzgrad des Funktionenkörpers $k(X)$ über k überein.*

Beweis. Wegen Eigenschaft (D3) der Dimension gilt $\dim(X) = \dim(U)$ für jede nicht-leere offene affine Untervarietät U von X, außerdem $k(X) \cong k(U)$. Mit Satz 4.78 folgt $\dim(X) = \dim(U) = \mathrm{trdeg}_k(k(U)) = \mathrm{trdeg}_k(k(X))$. ∎

Korollar 4.80. *Eine affine Varietät $V \subset \mathbb{A}^n$ ist genau dann endlich, wenn $\dim_k(k[V])) < \infty$ gilt.*

Beweis. Es sei V endlich und seien $V_1, \ldots, V_r$ die irreduziblen Komponenten von V. (Das sind die einzelnen Punkte von V, wenn $k = K$ gilt.) Nach Übung 4.14 gilt dann

$$k[V] = k[V_1] \times \cdots \times k[V_r].$$

Weil jedes V_i endlich ist, hat $k(V_i)$ den Transzendenzgrad 0. Also ist $k(V_i)/k$ endlich und algebraisch. Damit ist auch $k[V_i] \subset k(V_i)$ endlich dimensional über k. Ist umgekehrt $k[V]$ endlich dimensional, so auch alle $k[V_i]$ und damit haben alle $k(V_i)$ den Transzendenzgrad 0. Also haben alle V_i die Dimension 0 und sind damit endlich. ∎

Die Charakterisierung der Dimension über den Funktionenkörper zeigt auch, dass sich die Dimension unter birationaler Äquivalenz nicht ändert. Für später halten wir fest:

Satz 4.81. *Jede irreduzible k-Varietät ist birational zu einer affinen Hyperfläche.*

Beweisskizze. Wir beschränken uns im Beweis auf den Fall $\mathrm{char}(k) = 0$. Es seien $x_1, \ldots, x_n \in k(X)$ eine Transzendenzbasis über k. Die Körpererweiterung $k(X)/k(x_1, \ldots, x_n)$ ist dann also endlich und algebraisch. Weil k die Charakteristik 0 hat, ist sie außerdem separabel und es greift der Satz vom primitiven Element (siehe [Bosch], §3.6, Satz 12): Es gibt also ein Element $x_{n+1} \in k(X)$ mit $k(X) = k(x_1, \ldots, x_n)(x_{n+1})$, das eine Polynomgleichung

$$F(x_{n+1}) = a_d x_{n+1}^d + a_{d-1} x_{n+1}^{d-1} + \cdots + a_0$$

mit $a_0, \ldots, a_d \in k(x_1, \ldots, x_n)$ erfüllt. Bereinigen der Nenner liefert ein irreduzibles Polynom $f \in k[x_1, \ldots, x_n]$. Nach Konstruktion gilt dann $k(X) = k(\mathcal{V}(f))$, so dass X nach Kor. 4.62 zur Hyperfläche $\mathcal{V}(f)$ birational äquivalent ist.

Falls k positive Charakteristik hat, geht der Beweis im Prinzip genauso. Man muss aber $x_1, \ldots, x_n$ geschickt so wählen, dass die Körpererweiterung $k(X)/k(x_1, \ldots, x_n)$ separabel ist. (Siehe dazu zum Beispiel [Hulek], §1.1.5.) ∎

Zum Schluß dieses Abschnitts zeigen wir, dass die Dimension einer projektiven Varietät mit dem Grad des Hilbert-Polynoms übereinstimmt, was ja unsere erste Definition war. Zur Vorbereitung brauchen wir eine Hilfsaussage, die die Primärzerlegung eines Ideals aus §3.9 benutzt.

Lemma 4.82. *Es sei $I \subset k[x_0, \ldots, x_n]$ ein homogenes Ideal mit homogener Primärzerlegung*

$$I = I_1 \cap \cdots \cap I_r.$$

Sei $S = k[x_0, \dots, x_n]/I$ der graduierte Restklassenring und $X = \mathcal{V}_+(I) \subset \mathbb{P}^n$. Angenommen $f \in k[x_0, \dots, x_n]$ ist homogen vom Grad e mit der Eigenschaft, dass $\mathcal{V}_+(f)$ keine der irreduziblen Varietäten $\mathcal{V}_+(I_j)$ enthält, es sei denn $\mathcal{V}_+(I_j) = \varnothing$. Dann gibt es $e' \geqslant e$ so, dass die lineare Abbildung

$$\alpha_d \colon \begin{cases} S_{d-e} & \to & S_d \\ \overline{g} & \mapsto & \overline{fg} \end{cases}$$

für alle $d \geqslant e'$ injektiv ist.

Beweis. Für die Ideale I_j in der Primärzerlegung müssen wir zwei Fälle unterscheiden. Falls $\mathcal{V}_+(I_j) = \varnothing$ gilt, so gibt es $d_j \geqslant 0$ mit $S_{d_j} \subset I_j$ nach dem projektiven Nullstellensatz (Kor. 3.13). Falls keine solche Komponente existiert, setze $e' = e$, andernfalls setze $e' = \max\{e, d_j \colon \mathcal{V}_+(I_j) = \varnothing\}$. Ist nun $\overline{g} \in S_{d-e}$ mit $d \geqslant e'$ und $\overline{fg} = 0$ in S_d, dann also $fg \in I$ und damit $fg \in I_j$ für $j = 1, \dots, r$. Falls $\mathcal{V}(I_j) \neq \varnothing$, so folgt $f \notin \sqrt{I_j}$ aus der Voraussetzung an f und deshalb $g \in I_j$. Falls $\mathcal{V}(I_j) = \varnothing$, so folgt ebenfalls $g \in I_j$ wegen $\deg(g) \geqslant d_j$. Es folgt also $g \in I$ und damit $\overline{g} = 0$, wie behauptet. ∎

Beispiel 4.83. Es sei $I = \langle x_0x_1, x_1^2 \rangle \subset k[x_0, x_1]$ und $X = \mathcal{V}_+(I)$. Dann gilt $X = \{[1, 0]\} \subset \mathbb{P}^1$, so dass x_0 auf keiner irreduziblen Komponenten von X verschwindet. Es ist aber $I \subsetneq \mathcal{I}_+(X)$ wegen $x_1 \in \mathcal{I}_+(X) \setminus I$. Betrachte wie im Beweis des Lemmas die lineare Abbildung

$$\alpha_d \colon \begin{cases} (k[x_0, x_1]/I)_{d-1} & \to & (k[x_0, x_1]/I)_d \\ \overline{g} & \mapsto & \overline{g \cdot x_0} \end{cases}.$$

Dann ist α_1 nicht injektiv, denn es gilt $\alpha_1(\overline{x_1}) = \overline{x_0x_1} = 0$, aber $\overline{x_1} \neq 0$. Aber α_2 ist injektiv, da I_2 jede quadratische Form enthält, die in $[1, 0]$ verschwindet.

Satz 4.84. *Es sei $I \subset k[x_0, \dots, x_n]$ ein homogenes Ideal und $X = \mathcal{V}_+(I) \subset \mathbb{P}^n$. Die Dimension von X ist äquivalent gegeben durch die folgenden Größen:*

(i) die kombinatorische Dimension von X;
(ii) den Transzendenzgrad des Funktionenkörpers $k(X)$ über k, falls X irreduzibel ist;
(iii) den Grad des Hilbert-Polynoms P_I.

Beweis. Es sei $m = \dim(X)$. Die Gleichheit von (i) und (ii) haben wir bereits diskutiert. Wir zeigen die Gleichheit mit dem Grad des Hilbert-Polynoms durch Induktion nach m. Als Induktionsanfang nehmen wir den Fall $X = \varnothing$. Nach dem projektiven Nullstellensatz (Kor. 3.13) gilt dann $I_d = k[x_0, \dots, x_n]_d$ für alle hinreichend großen d. Also gilt für die Hilbert-Funktion $h_I(d) = 0$ für hinreichend großes d und damit $P_I = 0$. Es ist also $\dim(X) = \deg(P_I) = -\infty$, wie gewünscht[12]. Sei nun $m \geqslant 0$. Dann können wir durch Koordinatenwechsel ohne Einschränkung annehmen, dass die Voraussetzungen des vorangehenden Lemmas für $f = x_0$ erfüllt sind (siehe Übung 4.33). Es sei also $S = k[x_0, \dots, x_n]/I$. Nach dem Lemma ist die lineare Abbildung

$$\alpha_d \colon S_{d-1} \to S_d, \overline{g} \mapsto \overline{g \cdot x_0}.$$

[12]Wenn man sich an dem seltsamen Induktionsanfang bei $-\infty$ stört, kann man formal auch die Dimension der leeren Menge und den Grad des Nullpolynoms als -1 definieren. Es spielt keine Rolle, so lange man sich überzeugt, dass im Induktionsschritt alles in Ordnung ist.

injektiv für alle hinreichend großen d. Das Bild von α_d ist gerade das Ideal $\langle \overline{x_0} \rangle_d$. Für die Hilbert-Funktionen gilt $H_I(d) = \dim S_d$ und

$$\begin{aligned} H_{I+\langle x_0 \rangle}(d) &= \dim(S/\langle \overline{x_0} \rangle)_d = \dim(S_d) - \dim(\langle \overline{x_0} \rangle_d) = \dim S_d - \dim S_{d-1} \\ &= H_I(d) - H_I(d-1) \end{aligned}$$

für alle hinreichend großen d. Also gilt dieselbe Gleichheit auch für die Hilbert-Polynome. Nach Induktionsvoraussetzung und dem nachfolgenden Lemma folgt

$$m - 1 = \dim\big(X \cap \mathcal{V}(x_0)\big) = \deg(P_{I+\langle x_0 \rangle}) = \deg(P_X) - 1$$

(falls $m \geqslant 1$; für $m = 0$ entsprechend). Die letzte Gleichheit benutzt folgende Beobachtung: Ist $P \in \mathbb{Q}[t]$ ein normiertes Polynom, dann ist $P(t) - P(t-1)$ ein normiertes Polynom vom Grad genau $\deg(P) - 1$, wie man durch Koeffizientenvergleich sieht. Damit ist die Behauptung bewiesen. ■

Da wir Hilbert-Polynome mit dem Algorithmus aus Satz 3.61 konkret ausrechnen können, haben wir damit auch eine gute Möglichkeit, die Dimension einer projektiven Varietät zu bestimmen. Man beachte, dass man dafür nach Satz 4.84 direkt mit definierenden Gleichungen rechnen kann und es nicht nötig ist, das homogene Verschwindungsideal der Varietät, also das Radikal, zu bestimmen.

Übungen

Übung 4.30. Es seien $X, Y \subset \mathbb{A}^n$ irreduzible affine k-Varietäten. Es gelte $\dim(X) = n - 1$ und $Y \not\subset X$. Zeigen Sie, dass jede irreduzible Komponente von $X \cap Y$ die Dimension $\dim(Y) - 1$ hat.

Übung 4.31. Für jeden Morphismus $\varphi\colon X \to Y$ von Varietäten gilt $\dim(\varphi(X)) \leqslant \dim(X)$.

Übung 4.32. Es sei $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^3$, $t \mapsto (t^3, t^4, t^5)$. Zeigen Sie:
(a) Das Bild $C = \varphi(\mathbb{A}^1)$ ist abgeschlossen und 1-dimensional.
(b) Das Ideal $\mathcal{I}(C)$ wird nicht von zwei Elementen erzeugt.

Übung 4.33. Es seien $P_1, \ldots, P_r \subset k[x_0, \ldots, x_n]$ homogene Primideale mit $\varnothing \subsetneq \mathcal{V}_+(P_i) \subsetneq \mathbb{P}^n$ für $i = 1, \ldots, r$. Zeigen Sie, dass es eine Linearform $\ell \in k[x_0, \ldots, x_n]_1$ gibt mit $\mathcal{V}_+(P_i) \not\subset \mathcal{V}_+(\ell)$ für $i = 1, \ldots, r$. (*Vorschlag:* Lemma 3.57).

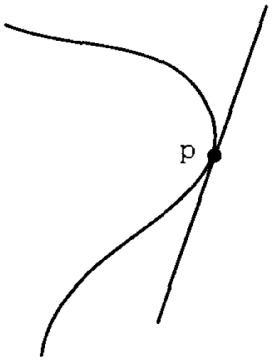
Übung 4.34*. Verfeinern Sie das Argument im Beweis von Satz 4.84 im Induktionsschritt, um einen neuen Beweis von Satz 3.61 (Existenz des Hilbert-Polynoms) zu geben. (*Hinweis:* Verwenden Sie Übung 3.48).

4.7. Tangentialraum und Glattheit

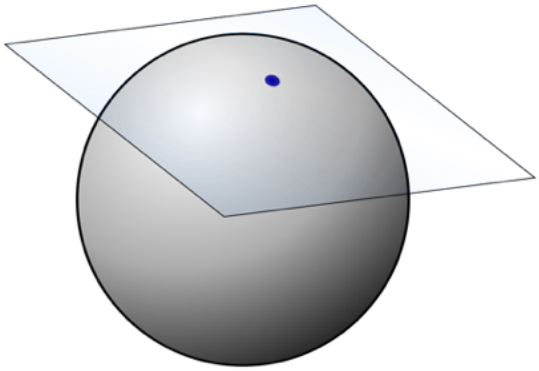
Tangentialraum und Glattheit sind geometrische Begriffe, die aus der Analysis und der Differentialgeometrie entlehnt sind. Ihre Bedeutung ist auch in der algebraischen Geometrie immens. Da es sich aber um punktweise Definitionen handelt, setzen wir in diesem Abschnitt $k = K$ voraus, so dass alle Punkte von Varietäten über dem Grundkörper definiert sind.

Sei im folgenden immer $k = K$ ein algebraisch abgeschlossener Körper.

Definition 4.85. Es sei $f \in k[x_1, \ldots, x_n]$ ein irreduzibles Polynom und $V = \mathcal{V}(f)$ die zugehörige Hyperfläche. Ein Punkt $p \in V$ heißt **regulär**, wenn der Gradient $(\nabla f)(p)$ nicht der Nullvektor ist. Der **Tangentialraum** an V in einem regulären Punkt p ist die Hyperebene $(\nabla f)(p)^{\perp}$.

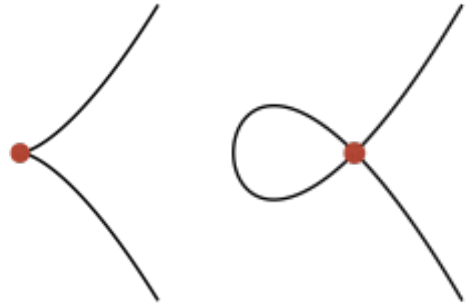


Tangentialraum an eine Kurve



Tangentialraum an eine Sphäre (*Bildquelle:* Wikimedia Commons)

Beispiele 4.86. Der Nullpunkt ist genau dann ein regulärer Punkt von $\mathcal{V}(f)$, wenn der konstante Term von f gleich 0 ist und der lineare Term ungleich 0.



$x^3 - y^2 = 0$ $\qquad$ $x^3 + x^2 - y^2 = 0$ $\qquad$ $4x^3 + 5x^2 - 4y^2 + x = 0$

Definition 4.87. Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät mit Verschwindungsideal $\mathcal{I}(V) \subset k[x_1, \ldots, x_n]$. Für $v \in k^n$, betrachte den Richtungsableitungs-Operator

$$D_v = \sum_{i=1}^{n} v_i \frac{\partial}{\partial x_i}.$$

Der **Tangentialraum an** V in einem Punkt $p \in V$ ist der lineare Raum

$$T_p(V) = \left\{ v \in k^n : (D_v f)(p) = 0 \text{ für alle } f \in \mathcal{I}(V) \right\}.$$

Die Ableitungen von Polynomen sind dabei wie üblich formal durch die Ableitungsregeln gegeben (was über $\mathbb{C}$ mit der Grenzwert-Definition übereinstimmt). Aus der Linearität der Ableitung ist klar, dass $T_p(V)$ ein linearer Raum ist, genauer gesagt ein Untervektorraum des Raums $T_p(\mathbb{A}^n) = k^n$ aller Richtungsableitungen. Für eine Hyperfläche $V = \mathcal{V}(f)$, mit f reduziert, stimmt diese Definition wegen $\mathcal{I}(V) = \langle f \rangle$ mit der vorigen überein (nach der Produktregel):

$$T_p(V) = \{v \in k^n : D_v(f)(p) = 0\} = \left\{(v_1, \dots, v_n) \in k^n : \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p) \cdot v_i = 0\right\} = \{(\nabla f)(p)\}^\perp.$$

Per Definition ist der Tangentialraum ein linearer Unterraum von $T_P(\mathbb{A}^n)$ und geht damit durch den Ursprung. Für unsere geometrische Anschauung ist es dagegen oft besser, den **affinen Tangentialraum** $p + T_p(V)$ zu betrachten, der durch den Punkt p geht. Für die Hyperfläche $V = \mathcal{V}(f)$ bedeutet das explizit

$$p + T_p(V) = \left\{v \in k^n : \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p) \cdot (v_i - p_i) = 0\right\}.$$

Ist zum Beispiel $n = 2$, $f \in k[x, y]$ ein irreduzibles Polynom und $p = (a, b)$ ein regulärer Punkt auf der ebenen affinen Kurve $\mathcal{V}(f)$, so ist der affine Tangentialraum also die Gerade

$$\frac{\partial f}{\partial x}(a)(x - a) + \frac{\partial f}{\partial y}(b)(y - b) = 0$$

Proposition 4.88. *Es sei $V \subset \mathbb{A}^n$ eine affine Varietät. Seien $f_1, \dots, f_\ell \in k[x_1, \dots, x_n]$ Erzeuger des Ideals $\mathcal{I}(V)$ und sei J die $\ell \times n$-Matrix mit Einträgen*

$$J_{ij} = (\partial f_i / \partial x_j)_{i,j}.$$

Dann ist $T_p(V)$ der Kern von $J(p)$.

Beweis. Gegeben $f \in \mathcal{I}(V)$, schreibe $f = \sum_{j=1}^\ell g_j f_j$. Dann gilt

$$D_v(f)(p) = \sum_{j=1}^\ell g_j(p) D_v(f_j)(p)$$

nach der Produktregel und wegen $f_j(p) = 0$. Ist also v im Kern von $J(p)$, so folgt $D_v(f)(p) = \sum_{j=1}^\ell g_j(p)\big(\sum_{i=1}^n v_i(\partial f_j/\partial x_i)(p)\big) = 0$. Also enthält $T_p(V)$ den Kern von $J(p)$. Ist umgekehrt $v \in T_p(V)$, so gilt $D_v(f_j)(p) = 0$ für alle $j = 1, \dots, \ell$ und damit $v \in \ker(J(p))$. ∎

Die Definition des Tangentialraums über Richtungsableitungen führt zu zwei technischen Problemen: (1) Es ist nicht klar, wie sie sich auf nicht-affine Varietäten verallgemeinern lässt. (2) Es ist nicht klar, wie sie sich unter Isomorphismen von Varietäten verhält. Um diese Probleme zu beheben, verwenden wir die folgende abstraktere Beschreibung des Tangentialraums.

Satz 4.89. *Es sei $V \subset \mathbb{A}^n$ eine affine Varietät, $p \in V$ ein Punkt und $m_p = \{f \in k[V] : f(p) = 0\}$ das zugehörige maximale Ideal von $k[V]$. Dann gibt es einen natürlichen Isomorphismus*

$$T_p(V) \xrightarrow{\sim} (m_p/m_p^2)^*$$

von k-Vektorräumen, wobei $(m_p/m_p^2)^*$ den Dualraum des Vektorraums m_p/m_p^2 bezeichnet.

Beweis. Zuerst etwas Erinnerung aus der linearen Algebra. Seien V und W zwei endlich-dimensionale k-Vektorräume und

$$\alpha : V \times W \to k$$

eine bilineare Abbildung. Dann induziert α die beiden linearen Abbildungen

$$\alpha_1: \begin{cases} V & \to & W^* \\ v & \mapsto & \alpha(v,-) \end{cases} \qquad \text{und} \qquad \alpha_2: \begin{cases} W & \to & V^* \\ w & \mapsto & \alpha(-,w) \end{cases}.$$

(Dabei ist $\alpha(v,-)\colon W \to k$ die lineare Abbildung $w \mapsto \alpha(v,w)$ und entsprechend $\alpha(-,w)$.) Wenn α_1 und α_2 injektiv sind, dann sind sie auch surjektiv. Denn ist α_1 injektiv, so impliziert das $\dim(V) \leqslant \dim(W^*) = \dim(W)$ und umgekehrt für α_2, also $\dim(V) = \dim(W)$. Damit sind α_1 und α_2 injektive lineare Abbildungen zwischen Vektorräumen der gleichen endlichen Dimension und damit Isomorphismen. In diesem Fall wird α eine *perfekte Paarung* genannt.

Sei nun $p = (p_1, \dots, p_n)$ und $M_p = \langle x_1 - p_1, \dots, x_n - p_n \rangle \subset k[x_1, \dots, x_n]$ das maximale Ideal zum Punkt p, so dass also $m_p = M_p/\mathcal{I}(V)$ gilt.

Bemerke zunächst, dass für $f \in M_p$ genau dann $D_v(f)(p) = 0$ für alle $v \in T_p(\mathbb{A}^n)$ gilt, wenn f in M_p^2 enthalten ist. (Taylor-Formel; Übung 4.35). Es folgt, dass die bilineare Abbildung

$$\alpha: \begin{cases} T_p(\mathbb{A}^n) \times M_p/M_p^2 & \to & k \\ (v, f) & \mapsto & D_v(f)(p) \end{cases}$$

eine perfekte Paarung ist. Die Behauptung ist also richtig für $V = \mathbb{A}^n$.

Wir behaupten, dass α auch modulo $\mathcal{I}(V)$ eine perfekte Paarung

$$\overline{\alpha}\colon T_p(V) \times (m_p/m_p)^2 \to k, (v, \overline{f}) \mapsto D_v(f)(p)$$

induziert. Dafür müssen wir als erstes zeigen, dass $\overline{\alpha}$ wohldefiniert ist. Gegeben $v \in T_p(X)$ und $f \in \mathcal{I}(V)$, dann gilt $D_v(f)(p) = 0$ nach Definition. Sind also f und g in M mit $f - g \in \mathcal{I}(X) + M_p^2$ und $v \in T_p(X)$, so folgt $D_v(f)(p) = D_v(g)(p)$. Also ist $\overline{\alpha}$ wohldefiniert.

Um zu zeigen, dass $\overline{\alpha}$ perfekt ist, müssen wir zeigen, dass die Kerne auf beiden Seiten (also von α_1 und α_2) Null sind. Auf der linken Seite ist das klar, denn wir haben lediglich von $T_p(\mathbb{A}^n)$ auf $T_p(V)$ eingeschränkt.

Auf der rechten Seite arbeiten wir im Vektorraum M_p/M_p^2. Dieser wird von den Restklassen $\overline{x_i - p_i}$ aufgespannt und ist deshalb endlich-dimensional. Seien $f_1, \dots, f_\ell$ Erzeugende von $\mathcal{I}(V)$ und sei U der in M_p/M_p^2 von $\overline{f_1}, \dots, \overline{f_\ell}$ aufgespannte Unterraum. Sei U' ein Komplement von U, also $M_p/M_p^2 = U \oplus U'$ und seien $g_1, \dots, g_r \in M_p$ so gewählt, dass $\overline{g_1}, \dots, \overline{g_r}$ eine Basis von U' bilden. Da α eine perfekte Paarung ist, gibt es eine duale Basis, also Elemente $v_1, \dots, v_r \in T_p(\mathbb{A}^n)$ mit $D_{v_i}(g_j)(p) = \delta_{ij}$ und für den von $v_1, \dots, v_r$ aufgespannten Unterraum W von $T_p(\mathbb{A}^n)$ gilt $T_p(\mathbb{A}^n) = T_p(V) \oplus W$. Nun ist W gerade der Kern der Abbildung

$$T_p(\mathbb{A}^n) \to (U')^*, v \mapsto \alpha(v,-).$$

Wegen $m_p/m_p^2 \cong (M_p/M_p^2)/U \cong U'$ zeigt das, dass die Abbildung $T_p(V) \to (m_p/m_p^2)^*$, $v \mapsto \alpha(v,-)$ injektiv ist, wie behauptet. Damit ist alles bewiesen. ∎

Korollar 4.90. *Es sei $V \subset \mathbb{A}^n$ eine affine k-Varietät und $p \in V$ ein Punkt. Sei $\mathcal{O}_{p,V}$ der lokale Ring von V im Punkt p und $m_{p,V}$ sein maximales Ideal. Dann gibt es einen natürlichen Isomorphismus $T_p(X) \xrightarrow{\sim} (m_{p,V}/m_{p,V}^2)^*$ von k-Vektorräumen.*

Beweis. Es gilt $\mathcal{O}_{p,V} = k[V]_{m_p}$ (wobei $m_p = \{f \in k[V]\colon f(p) = 0\}$). Nach dem Satz gilt also

$$T_p(V) \cong (m_p/m_p^2)^* \cong (m_{p,V}/m_{p,V}^2)^*,$$

wobei die letzte Isomorphie darauf beruht, dass Lokalisierung und Quotientenbildung miteinander vertauschen (siehe Übung 4.5). ■

Definition 4.91. Es sei X eine quasiprojektive Varietät und $p \in X$ ein Punkt. Sei $m_{p,X}$ das maximale Ideal des lokalen Rings $\mathcal{O}_{p,X}$ von X in p. Der **Tangentialraum an** X **im Punkt** p ist der k-Vektorraum $(m_{p,X}/m_{p,X}^2)^*$. Der Punkt p heißt **regulär**, wenn

$$\dim(T(X)) = \dim(X)$$

gilt. Ein Punkt von X, der nicht regulär ist, heißt ein **singulärer Punkt** oder eine **Singularität**.

Ist $p \in X$ ein regulärer Punkt, dann sagt man auch, dass X **glatt** im Punkt p ist. Die Varietät X heißt insgesamt **glatt** (oder **regulär**[13]), wenn sie in jedem ihrer Punkte glatt ist.

Die Menge aller regulären Punkte von X heißt der **reguläre Ort** und wird mit X_{reg} bezeichnet. Die Menge der singulären Punkte von X heißt der **singuläre Ort** und wird mit X_{sing} bezeichnet.

Aufgrund der neuen Definition mithilfe von lokalen Ringen, ist klar, dass sich Regularität unter Isomorphismen überträgt: Sind X und Y zwei Varietäten, $\varphi\colon X \to Y$ ein Isomorphismus, dann ist $p \in X$ genau dann ein regulärer Punkt, wenn $\varphi(p) \in Y$ ein regulärer Punkt ist.

Beispiele 4.92. Die Veronese-Varietäten $v_d(\mathbb{P}^n)$ sind glatt, da sie zu $\mathbb{P}^n$ isomorph sind. Insbesondere sind die verdrehte Kubik und die rationalen Normalkurven glatt. Die Segre-Varietäten $\Sigma_{m,n}$ sind ebenfalls glatt. (Allgemein ist das kartesische Produkt glatter Varietäten glatt.)

In Macaulay2 kann man den singulären Ort mit dem Befehl `singularLocus` berechnen lassen.

```
i1 : S=QQ[x0,x1,x2,x3];
i2 : I=ideal(x0^3-x1^3-x2^3-x3^3);
i3 : V=Spec(S/I);
i4 : W=singularLocus(V)
o4 : AffineVariety
i5 : dim(W)
o5 = 0
```

Die Varietät V hat also nur endlich-viele singuläre Punkte.

```
i6 : decompose(ideal(W))
o6 = {ideal (x3, x2, x1, x0)}
```

Genauer besteht der singuläre Ort nur aus dem Nullpunkt. Da I ein homogenes Ideal ist, ist diese Singularität auf der zugehörigen projektiven Varietät nicht zu sehen.

```
i7 : X=Proj(S/I);
i8 : dim(singularLocus(X))
o8 = -infinity
```

Die projektive Varietät X ist also glatt.

[13] In der modernen algebraischen Geometrie wird 'glatt' häufig nur als eine Eigenschaft von Morphismen verwendet bzw. ist für Varietäten anders definiert. Der Unterschied ist nur in Charakteristik p relevant. In vielen Büchern werden die Begriffe 'glatt' und 'regulär' synonoym verwendet, aber in Charakteristik p ist Vorsicht geboten.

Satz 4.93. *In jeder quasiprojektiven Varietät ist der reguläre Ort offen und dicht. Insbesondere besitzt jede Varietät einen regulären Punkt.*

Beweis. Es sei V eine quasi-projektive Varietät. Zunächst bemerken wir, dass die Menge der Punkte von V, die nur in einer einzigen irreduziblen Komponenten von V enthalten sind, offen und dicht in V ist (siehe Übung 4.36). Deshalb können wir für den Beweis ohne Einschränkung annehmen, dass V irreduzibel ist. Außerdem wird V von offenen affinen Untervarietäten überdeckt (Kor. 4.42). Deshalb können wir weiter auf den Fall reduzieren, dass V affin ist.

Wir zeigen die Behauptung nun zunächst für eine irreduzible affine Hyperfläche. Es sei $f \in k[x_1, \dots, x_n]$ irreduzibel und $V = \mathcal{V}(f)$. Per Definition sind die singulären Punkte genau die Punkte von V, in denen der Gradient ∇f verschwindet. Es gilt also

$$V_{\text{sing}} = \mathcal{V}(f, \partial f/\partial x_1, \dots, \partial f/\partial x_n).$$

Das ist eine abgeschlossene Untervarietät von V, also ist $V_{\text{reg}} = V \setminus V_{\text{sing}}$ offen. Wir müssen nur noch zeigen, dass $V_{\text{sing}} \neq V$ gilt. Da das Polynom $\partial f/\partial x_i$ in der Variablen x_i kleineren Grad als f hat, kann es nicht durch f teilbar sein, es sei denn, es ist (identisch) Null. In Charakteristik 0 geschieht das genau dann, wenn die Variable x_i in f nicht vorkommt. Da eine der Variablen $x_1, \dots, x_n$ in f vorkommen muss, kann ∇f also nicht überall auf V verschwinden. Falls $\text{char}(k) = p > 0$, so gilt $\partial f/\partial x_i = 0$ genau dann, wenn f ein Polynom in x_i^p ist. Wäre dies für alle $i = 1, \dots, n$ der Fall, dann könnten wir aus jedem Koeffizienten von f die p-te Wurzel ziehen (da k algebraisch abgeschlossen ist) und $f = g^p$ für ein $g \in k[x_1, \dots, x_n]$ folgern, im Widerspruch zur Irreduzibilität von f. Damit ist die Behauptung im Fall von affinen Hyperflächen bewiesen.

Wenn V keine Hyperfläche ist, dann können wir Satz 4.81 anwenden: Da V birational zu einer affinen Hyperfläche ist, gibt es eine offene dichte Teilmenge U von V die isomorph zu einer offenen dichten Teilmenge einer Hyperfläche ist. Daher enthält U eine offene dichte Teilmenge von regulären Punkten.

Es bleibt zu zeigen, dass V_{sing} abgeschlossen in V ist. Es sei $V \subset \mathbb{A}^n$ abgeschlossen mit Verschwindunsideal $\mathcal{I}(V) = \langle f_1, \dots, f_r \rangle$. Sei J die Matrix mit Einträgen $(\partial f_i/\partial x_j)$ wie zuvor. Nach Prop. 4.88 sind die regulären Punkte von V genau die Punkte $p \in V$, in denen $J(p)$ den Rang $n - \dim(V)$ hat. Da V_{reg} dicht in V ist, kann $J(p)$ niemals größeren Rang als $n - \dim(V)$ haben. Denn angenommen es gäbe $p \in V$ mit $\text{Rang}(J(p)) > n - \dim(V)$, dann gäbe es einen Minor von J der Größe $r > n - \dim(V) + 1$, der in p nicht verschwindet (siehe Aufgabe 1.14). Dann besitzt p aber eine offene Umgebung, in der dieser Minor nicht verschwindet, im Widerspruch zur Dichtheit von V_{reg}. Also ist die Menge der singulären Punkte von V genau die Menge der Punkte $p \in V$, in denen $J(p)$ kleineren Rang als $n - \dim(V)$ hat. Das ist die abgeschlossene Menge von V, die durch das Verschwinden aller Minoren der Größe $n - \dim(V)$ gegeben ist. ∎

Der Beweis hat zusätzlich folgendes gezeigt:

Korollar 4.94. *Ist X eine k-Varietät der Dimension d, dann gilt*

$$\dim T_p(X) \geqslant d$$

für alle $p \in X$, mit Gleichheit auf der offenen dichten Menge X_{reg}. ∎

Bemerkung 4.95. Im Beweis von Satz 4.93 haben wir auf den irreduziblen Fall reduziert. Tatsächlich ist die Menge aller Punkte $p \in X$, die in mehr als einer irreduziblen Komponenten von X liegen, immer im singulären Ort von X enthalten. Für Hyperflächen ist das klar: Ist $f = f_1 f_2$ mit f_1 und f_2 reduziert und ohne gemeinsame Faktoren, dann gilt also $\mathcal{V}(f)_{\text{sing}} = \mathcal{V}(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$. Für $p \in \mathcal{V}(f_1) \cap \mathcal{V}(f_2)$ ist dann $\frac{\partial f}{x_i}(p) = \frac{\partial f_1}{x_i}(p) f_2(p) + \frac{\partial f_2}{x_i}(p) f_1(p) = 0$ nach der Produktregel, also $p \in \mathcal{V}(f)_{\text{sing}}$. Für den allgemeinen Fall siehe etwa [Shafarevich], II.2, Thm. 6.

Tangentialräume sind zunächst affin definiert. Der Tangentialraum an eine projektive Varietät sollte aber auch ein projektiver Unterraum sein: Sei $X \subset \mathbb{P}^n$ eine projektive Varietät und $p \in X$. Dann ist p in einer offenen affinen Teilmenge $D_i \cong \mathbb{A}^n$ enthalten. Wir definieren den **projektiven Tangentialraum** $\mathbb{T}_p(X)$ an X in P als den projektiven Abschluss des affinen Tangentialraums

$$p + T_p(X \cap D_i) \subset D_i \subset \mathbb{P}^n.$$

Diese Definition hängt nicht von der Wahl von D_i ab, ist aber technisch nicht sehr bequem.

Wir betrachten zunächst wieder den Fall einer Hyperfläche $X = \mathcal{V}_+(f)$, mit $f \in k[x_0, \ldots, x_n]$ homogen und irreduzibel. Betrachte die affine offene Teilmenge D_0 mit affinen Koordinaten $y_i = x_i/x_0$. Dann ist $X \cap D_0$ beschrieben durch $\widetilde{f}(y_1, \ldots, y_n) = f(1, y_1, \ldots, y_n)$. Für einen Punkt $p = (w_1, \ldots, w_n) \in X \cap D_0$ ist der affine Tangentialraum gegeben durch

$$p + T_p(X) = \left\{ (y_1, \ldots, y_n) \colon \sum_{i=1}^{n} \frac{\partial f}{\partial y_i}(p) \cdot (y_i - w_i) = 0 \right\}.$$

Der projektive Tangentialraum wird durch die homogenisierte Gleichung beschrieben:

$$\mathbb{T}_p(X) = \left\{ [x_0, x_1, \ldots, x_n] \colon \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(1, w_1, \ldots, w_n) \cdot (x_i - w_i x_0) = 0 \right\}.$$

Das können wir weiter vereinfachen, indem wir die **Euler-Identität**

$$\sum_{i=0}^{n} \frac{\partial f}{\partial x_i} \cdot x_i = d \cdot f,$$

mit $d = \deg(f)$, benutzen. Wegen $f(1, w_1, \ldots, w_n) = 0$ folgt

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(1, w_1, \ldots, w_n) \cdot (-w_i \cdot x_0) = \frac{\partial f}{\partial x_0}(1, w_1, \ldots, w_n) \cdot x_0.$$

Daraus folgt

$$\mathbb{T}_p(X) = \left\{ [x_0, \ldots, x_n] \in \mathbb{P}^n \colon \sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p) \cdot x_i = 0 \right\}.$$

Der Punkt p ist genau dann singulär, wenn die partiellen Ableitungen von f in p verschwinden, also genau dann, wenn $\mathbb{T}_p(X) = \mathbb{P}^n$ gilt. Wegen der Euler-Identität impliziert das Verschwinden aller partieller Ableitungen auch das Verschwinden von f (es sei denn, die Charakteristik von k teilt d). Der singuläre Ort von $\mathcal{V}_+(f)$ wird also genau von den partiellen Ableitungen definiert.

Ist $X \subset \mathbb{P}^n$ eine projektive Varietät, nicht notwendig eine Hyperfläche, dann ist $\mathbb{T}_p(X)$ der Durchschnitt aller Tangentialräume in p an alle Hyperflächen, die X enthalten. Wenn also das homogene Verschwindungsideal $\mathcal{I}_+(X)$ von $f_1, \ldots, f_\ell$ erzeugt wird, dann gilt

$$\mathbb{T}_p(X) = \bigcap_{i=1}^{\ell} \mathbb{T}_p(\mathcal{V}_+(f_i)) = \left\{ [x_0, \ldots, x_n] \in \mathbb{P}^n \colon \sum_{i=0}^{n} \frac{\partial f_j}{\partial x_i}(p) \cdot x_i = 0, j = 1, \ldots, \ell \right\} = \mathbb{P}(\ker J),$$

wobei J die $\ell \times n$-Matrix mit Einträgen $J_{ij} = (\partial f_i/\partial x_j)(p)$ ist.

Eine projektive Hyperfläche $\mathcal{V}_+(f)$ in $\mathbb{P}^n$ ist genau dann glatt, wenn $\mathcal{V}_+(\frac{\partial f}{\partial x_0}, \dots, \frac{\partial f}{\partial x_n}) = \varnothing$ gilt (wenn wir der Einfachheit halber $\operatorname{char}(k) \nmid d$ annehmen). Wie sieht die Menge aller homogenen Polynome mit dieser Eigenschaft aus? Sei dazu $V_d = k[x_0, \dots, x_n]_d$ $(d \geqslant 0)$ und betrachte

$$\Theta_d = \big\{(p, [F]) \in \mathbb{P}^n \times \mathbb{P}V_d \colon (\nabla f)(p) = 0\big\}.$$

Die Menge Θ_d ist abgeschlossen in $\mathbb{P}^n \times \mathbb{P}V_d$, denn $(\nabla f)(p) = 0$ ist ein System von Polynomgleichungen in p und den Koeffizienten von f. Es folgt aus dem Hauptsatz der Eliminationstheorie, dass die Projektion $\Delta_d = \pi_2(\Theta_d)$ von Θ_d auf den zweiten Faktor abgeschlossen in $\mathbb{P}V_d$ ist.

Die Varietät Δ_d besteht aus allen $f \in k[x_0, \dots, x_n]_d$, für die $\mathcal{V}_+(f)_{\text{sing}} \neq \varnothing$, sowie allen f, die einen mehrfachen irreduziblen Faktor haben. Es gilt $\Delta_d \subsetneq \mathbb{P}V_d$, denn für jeden Grad d und jeden Körper k gibt es glatte projektive k-Hyperflächen. (Falls $\operatorname{char}(k) \nmid d$ gilt, so ist zum Beispiel $\mathcal{V}_+(x_0^d + \dots + x_n^d)_d$ eine glatte Hyperfläche). Tatsächlich ist Δ_d eine Hyperfläche, genannt die **Diskriminante**. Sie ist also durch ein einziges Polynom in den Koeffizienten von f definiert.

Für $d = 1$ gilt offenbar $\Delta_1 = \varnothing$. Der Fall $d = 2$, quadratische Formen, ist ebenfalls elementar: Beschreibt man eine quadratische Form $f \in k[x_0, \dots, x_n]_d$ durch eine symmetrische $(n+1) \times (n+1)$-Matrix A als $f = x^t A x$ (mit $x = (x_0, \dots, x_n)$, $\operatorname{char}(k) \neq 2$), so gilt $\mathcal{V}_+(\nabla f) = \varnothing$ genau dann, wenn A invertierbar ist (siehe Übung 4.37). Die Diskriminante ist also $\Delta_2 = \mathcal{V}_+(\det)$, wobei $\det$ die Determinante als Polynom vom Grad $n+1$ in den $\binom{n+2}{2}$ Einträgen von A ist.

Im allgemeinen hat die Diskriminante den Grad $(n+1)(d-1)^n$ und über die Struktur dieses Riesen-Polynoms ist nicht allzu viel bekannt.

Übungen

Übung 4.35. (k=K) Es sei $p = (a_1, \dots, a_n) \in \mathbb{A}^n$ ein Punkt, $M_p = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ und $f \in M_p$. Zeigen Sie: Genau dann gilt $D_v(f)(p) = 0$ für alle $v \in k^n$, wenn $f \in M_p^2$ gilt.

Übung 4.36. Es sei X eine quasiprojektive Varietät. Zeigen Sie, dass die Menge der Punkte von X, die nur in einer einzigen irreduziblen Komponenten von X enthalten sind, offen und dicht in X ist.

Übung 4.37. Es gelte $\operatorname{char}(k) \neq 2$. Sei A eine symmetrische $(n+1) \times (n+1)$-Matrix mit Einträgen in k und $f = x^t A x \in k[x_0, \dots, x_n]$ die zugehörige quadratische Form. Zeigen Sie: Genau dann gilt $\mathcal{V}_+(\frac{\partial f}{\partial x_0}, \dots, \frac{\partial f}{\partial x_n}) = \varnothing$, wenn A invertierbar ist.

Übung 4.38. Zeigen Sie: Wenn eine projektive Hyperfläche vom Grad 3 zwei singuläre Punkte enthält, dann auch die Verbindungsgerade dieser beiden Punkte.

Übung 4.39. Bestimmen Sie für $\alpha \in k$ die singulären Punkte der Kurve $\mathcal{V}_+(f) \subset \mathbb{P}^2$ gegeben durch

$$f = x_0^3 + x_1^3 + x_2^3 + \alpha(x_0 + x_1 + x_2)^3.$$

Übung 4.40. Bestimmen Sie die singulären Punkte der *Steiner-Fläche*

$$\mathcal{V}_+(x_1^2 x_2^2 + x_0^2 x_2^2 + x_0^2 x_1^2 - x_0 x_1 x_2 x_3) \subset \mathbb{P}^3.$$

Plotten Sie das reelle Bild dieser Fläche (mit $x_0 = 1$).