

Algebraische Kurven

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Wintersemester 2008/2009

INHALTSVERZEICHNIS

1. Vorlesung	7
1.1. Algebraische Kurven - Einige Beispiele	7
1.2. Gleichungen der Form $Y^2 = G(X)$	11
1.3. Polynomringe	13
2. Vorlesung	15
2.1. Affin-algebraische Mengen	15
2.2. Ideale und Nullstellengebilde	18
3. Vorlesung	21
3.1. Die Zariski-Topologie	21
3.2. Das Verschwindungsideal	22
3.3. Das Radikal	24
4. Vorlesung	24
4.1. Irreduzible affin-algebraische Mengen	24
4.2. Zur Anzahl der Punkte auf Kurven	28
5. Vorlesung	29
5.1. Homogene Komponenten	29
5.2. Zur Anzahl der Punkte auf Kurven II	31
5.3. Polynomiale Abbildungen zwischen affinen Räumen	32
6. Vorlesung	35
6.1. Ebene polynomiale Parametrisierungen	35
6.2. Rationale Parametrisierungen	37
7. Vorlesung	41
7.1. Kegelschnitte und Quadriken	41
7.2. Klassifikation von reellen und komplexen Quadriken	44
7.3. Parametrisierung von Quadriken	46
8. Vorlesung	49
8.1. Mechanisch definierte algebraische Kurven	49
8.2. Zwei Geraden als Bahnen	51
8.3. Gerade und Kreis als Bahnen	53
9. Vorlesung	59
9.1. Noethersche Ringe	59

9.2.	Der Hilbertsche Basissatz	60
9.3.	Zerlegung in irreduzible Komponenten	62
9.4.	Moduln	64
10.	Vorlesung	65
10.1.	Noethersche Moduln	65
10.2.	Hilbertscher Nullstellensatz - algebraische Version	66
11.	Vorlesung	68
11.1.	Hilbertscher Nullstellensatz - geometrische Version	68
11.2.	Der Koordinatenring zu einer affin-algebraischen Menge	71
12.	Vorlesung	73
12.1.	Das K -Spektrum	73
12.2.	Das K -Spektrum als Funktor	77
12.3.	Weitere Eigenschaften des K -Spektrums	78
13.	Vorlesung	79
13.1.	Die offenen Mengen $D(f)$	79
13.2.	Zusammenhang und idempotente Elemente	81
14.	Vorlesung	84
14.1.	Algebraische Funktionen auf Varietäten	84
15.	Vorlesung	89
15.1.	Lokale Ringe	90
15.2.	Quotientenkörper und Funktionenkörper	90
15.3.	Topologische Filter und ihre Halme	91
16.	Vorlesung	95
16.1.	Irreduzible Filter	95
16.2.	Morphismen zwischen Varietäten	96
17.	Vorlesung	101
17.1.	Monoidringe	101
17.2.	Universelle Eigenschaft der Monoidringe	103
17.3.	Differenzengruppe zu einem Monoid	105
18.	Vorlesung	106
18.1.	Monomiale Kurven	106
19.	Vorlesung	111
19.1.	Restklassendarstellung für monomiale Kurven	111

19.2. Ganzheit	114
20. Vorlesung	116
20.1. Normale Ringe und Normalisierung	116
20.2. Normalisierung von Monoidringen	117
20.3. Monomiale Kurven und Normalisierung	119
21. Vorlesung	120
21.1. Diskrete Bewertungsringe	120
21.2. Das Lemma von Nakayama	124
22. Vorlesung	125
22.1. Die Einbettungsdimension	125
22.2. Glatte und singuläre Punkte	127
23. Vorlesung	130
23.1. Glatte und normale Punkte	131
23.2. Die Hilbert-Samuel Multiplizität	132
23.3. Monomiale Kurven und Multiplizität	134
24. Vorlesung	135
24.1. Tangenten bei Parametrisierungen	135
24.2. Tangenten bei Raumkurven	136
24.3. Potenzreihenringe	137
25. Vorlesung	139
25.1. Lösung in Potenzreihen für algebraische Kurven	139
26. Vorlesung	145
26.1. Die Schnittmultiplizität	145
27. Vorlesung	150
27.1. Der projektive Raum	150
27.2. Nullstellen von homogenen Polynomen	153
27.3. Der projektive Raum über \mathbb{R} und über \mathbb{C}	154
28. Vorlesung	156
28.1. Projektive Varietäten	156
28.2. Algebraische Funktionen und Morphismen	157
28.3. Homogenisierung und projektiver Abschluss	158
28.4. Projektive ebene Kurven	159
29. Vorlesung	162

29.1. Projektion weg von einem Punkt	162
29.2. Abbildungen nach \mathbb{P}_K^1	162
29.3. Parametrisierte projektive ebene Kurven	164
29.4. Monomiale projektive Kurven	166
30. Vorlesung	167
30.1. Der Satz von Bezout	167
Anhang 1: Bildlizenzen	173
Abbildungsverzeichnis	173
Anhang 2: GFDL-Lizenz	179

Vorwort

Dieses Skript gibt die Vorlesung über algebraische Kurven wieder, die ich im Wintersemester 2008/2009 an der Universität Osnabrück gehalten habe. Es handelt sich dabei im Wesentlichen um ausformulierte Manuskripttexte, die im direkten Anschluss an die einzelnen Vorlesungen öffentlich gemacht wurden. Ich habe diese Veranstaltung zum ersten Mal durchgeführt, bei einem zweiten Durchlauf werden sicher noch viele Korrekturen und Änderungen dazukommen. Dies bitte ich bei einer kritischen Durchsicht wohlwollend zu berücksichtigen.

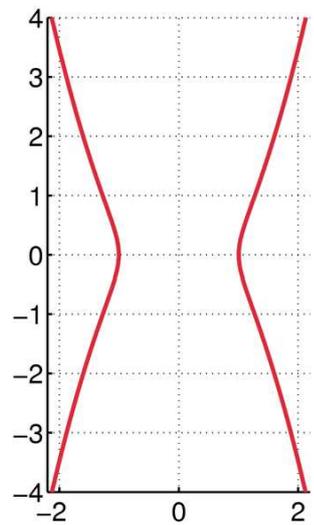
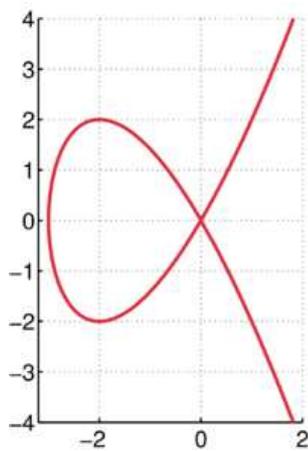
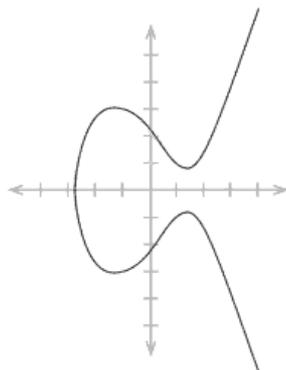
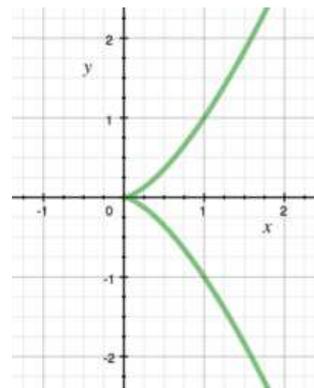
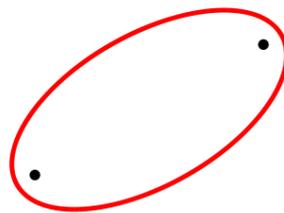
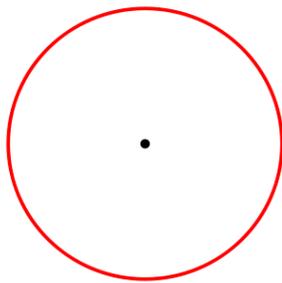
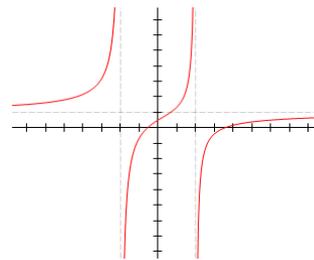
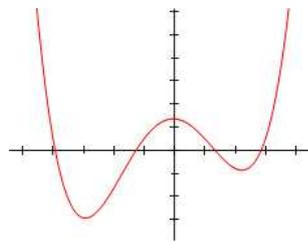
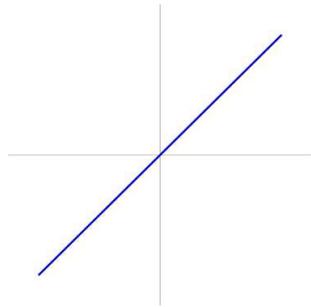
Der Text wurde auf Wikiversity geschrieben und steht unter der Creative-Commons-Attribution-ShareAlike 2.5, die Bilder wurden von Commons übernommen und unterliegen den dortigen freien Lizenzen. Die Lizenzen ermöglichen unter bestimmten Voraussetzungen, dass das Skript in seinen Einzelteilen verwendet, verändert und weiterentwickelt werden darf. Die Bildlizenzen im Einzelnen werden in einem Anhang aufgeführt. Ich bedanke mich bei der Wikiversity community und insbesondere bei Benutzer Exxu für die wichtigen Beiträge im Projekt semantische Vorlagen, die eine weitgehend automatische Erstellung des Latexcodes ermöglichen, bei den Studierenden für einzelne Korrekturen und erstellte Bilder und bei Frau Marianne Gausmann für die Erstellung des Pdf-Files. Bei Diplom-Math. Axel Stäbler bedanke ich mich für die Korrekturen der Aufgaben und bei Dr. Julio Moyano für die Vorführung der mechanischen Kurven.

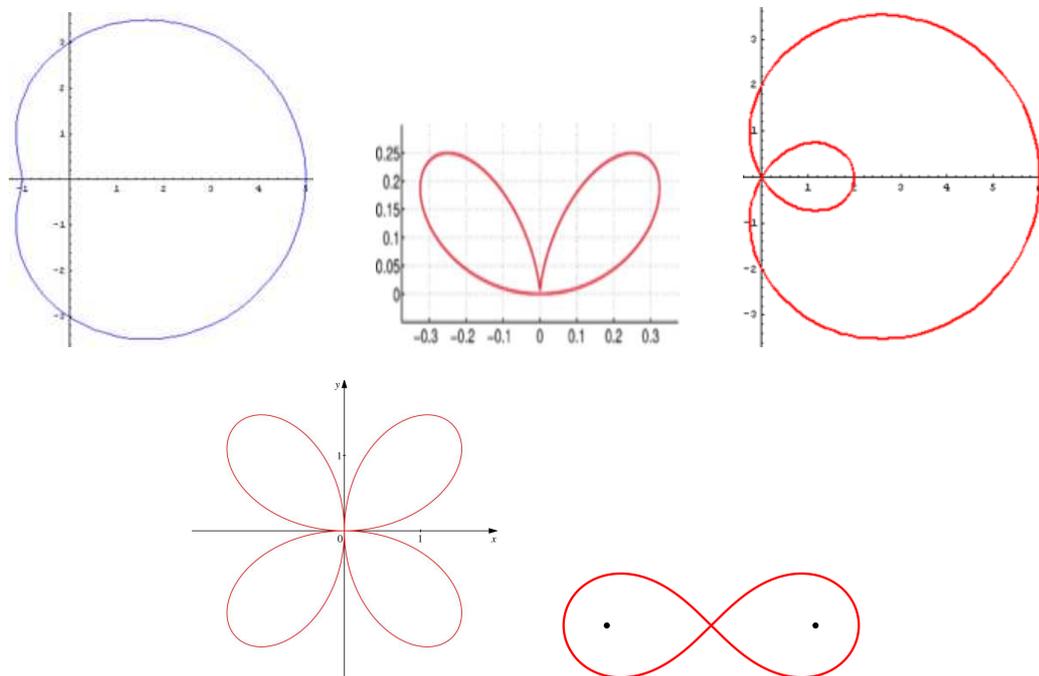
Holger Brenner

1. VORLESUNG

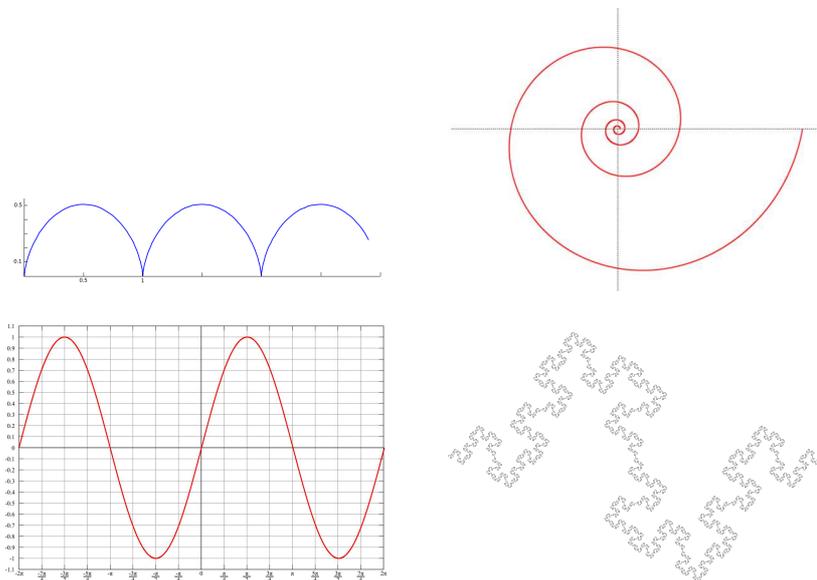
1.1. Algebraische Kurven - Einige Beispiele.

Was ist eine algebraische Kurve? Na zum Beispiel die folgenden schönen Bilder:





Nun kann man natürlich viel malen. Schön sind auch die folgenden Kurven, doch das sind keine algebraischen Kurven:



Das „algebraisch“ in algebraische Kurve kommt daher, dass zu ihrer Definition nur algebraische Operationen verwendet werden dürfen, d.h. Addition und Multiplikation, nicht aber analytische Prozesse wie Limes nehmen, unendliche Summen, Approximieren, Differenzieren und Integrieren. Die erlaubten Abbildungen in unserem Kontext sind durch Polynome in mehreren Variablen gegeben. In den obigen Bildern geht es um ebene algebraische Kurven, die durch ein Polynom in zwei Variablen definiert werden. Die beiden ersten

Bilder sind *Graphen* zu einer polynomialen Funktion in einer Variablen, sie werden beschrieben durch

$$Y = P(X)$$

wobei im ersten Bild $P(X) = X$ ist (es liegt also ein lineares Polynom vor) und im zweiten Bild etwas wie

$$P(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$$

mit gewissen Koeffizienten a_i aus einem Körper K vorliegt. In der algebraischen Geometrie fixiert man einen *Grundkörper* K . Wichtige Körper sind für uns die *reellen Zahlen* (insbesondere sind die Bilder so zu verstehen!) oder die *komplexen Zahlen* \mathbb{C} . Ein solcher Graph ist insofern ein einfaches Gebilde, dass es zu jedem Wert für X genau einen Wert für Y (den Funktionswert) gibt, und den man auch noch einfach ausrechnen kann, wenn man im gegebenen Körper rechnen kann. Der Graph ist in gewissem Sinne eine „gebogene“ Kopie der Grundlinie, der X -Achse.

Betrachten wir das dritte Bild. Das ist der Graph einer *rationalen Abbildung*, d.h. man hat zwei Polynome P, Q in einer Variablen X und schaut sich den Quotienten $\frac{P(X)}{Q(X)}$ an. Dieser Ausdruck macht nur dort Sinn, wo der Nenner nicht null ist. An den Nullstellen des Nennerpolynoms ist die rationale Funktion nicht definiert (wenn Nenner und Zähler an der gleichen Stelle beide null sind, so kann man durch kürzen manchmal erreichen, dass der Quotient auch an dieser Stelle einen Sinn bekommt). Wenn der Nenner null ist, der Zähler aber nicht, so ist die undefiniertheitsstelle ein „Pol“ - der reelle Graph strebt nach $+\infty$ bzw. $-\infty$. Es ist verlockend zu sagen, dass der Wert der rationalen Funktion an diesen undefinierten Stellen „unendlich“ ist, und im Kontext der projektiven Geometrie macht das durchaus Sinn, wie wir später sehen werden. Die „Graphengleichung“ $Y = \frac{P(X)}{Q(X)}$ ist jedenfalls wegen den undefiniertheitsstellen keine optimale Beschreibung für die Kurve. Wenn man sie hingegen mit dem Nenner multipliziert, so erhält man die Bedingung (oder *Gleichung*)

$$YQ(X) = P(X) \text{ bzw. genauer } \{(x, y) \in K^2 : yQ(x) = P(x)\},$$

in der links und rechts wohldefinierte Polynome stehen. Die *Erfüllungsmenge* (oder *Lösungsmenge*) ist eindeutig definiert (wobei bei $Q(x) = 0$ für ein bestimmtes x die linke Seite null ist, und es dann dort bei $P(x) \neq 0$ keine Lösung gibt (wie im Bild) und bei $P(x) = 0$ jeder Y -Wert erlaubt ist. In letzterem Fall gehört also eine zur X -Achse senkrechte Gerade durch $(x, 0)$ zu dem Gebilde).

Beispiel 1.1. (Hyperbel) Ein typisches und wichtiges Beispiel für eine rationale Funktion ist $Y = 1/X$. Den zugehörigen Graph nennt man *Hyperbel* H . Nennerfrei geschrieben ergibt sich die Gleichung

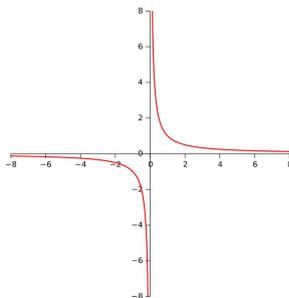
$$XY = 1 \text{ bzw. } H = \{(x, y) : xy = 1\}.$$

Diese rationale Funktion ist auf $K^\times = K - \{0\}$ eine echte Funktion (mit H als Graph) und stiftet eine „natürliche“ Bijektion

$$K^\times \longrightarrow H, x \longmapsto \left(x, \frac{1}{x}\right).$$

K^\times und H sind also in einem zu präzisierenden Sinn „äquivalent“ oder „isomorph“.

Beide Beschreibungen haben etwas für sich. Die Beschreibung als $K^\times \subset K$ spielt sich auf einer Geraden ab (wenn man an $K = \mathbb{R}$ denkt), dafür gehört der Punkt 0, der ein *Häufungspunkt* von K^\times ist, nicht zu K^\times . D.h., K^\times ist nicht *abgeschlossen*. Dagegen ist die Hyperbel in \mathbb{R}^2 abgeschlossen, für die abgeschlossene Realisierung muss man also in eine höhere Dimension gehen. Die Frage, was eine gute Beschreibung für ein Objekt der algebraischen Geometrie ist, wird immer wieder auftauchen.



Im reellen Fall, also bei $K = \mathbb{R}$, besteht \mathbb{R}^\times (und entsprechend $H_{\mathbb{R}}$) aus zwei disjunkten „Zweigen“, ist also nicht *zusammenhängend*. Im komplexen Fall, also bei $K = \mathbb{C}$, ist \mathbb{C}^\times (und entsprechend $H_{\mathbb{C}}$) eine punktierte reelle Ebene, also *zusammenhängend*. Dies ist ein typisches Phänomen der algebraischen Geometrie, dass wichtige Eigenschaften vom Grundkörper abhängen. Besonders wichtig sind dann aber Eigenschaften, die nur von den beschreibenden Gleichungen abhängen und für die Lösungsmengen zu allen Körpern gelten.

Das vierte Bild ist ein *Kreis*, seine Gleichung ist

$$K = \{(x, y) : x^2 + y^2 = r^2\},$$

wobei r den Radius des Kreises bezeichnet. Schon das Bild zeigt, dass dieses Gebilde nicht der Graph einer Funktion (Abbildung) sein kann, da bei einem Graphen zu einem x -Wert stets genau ein y -Wert gehört. Man kann aber keine Funktion finden mit $y = \varphi(x)$ und $K = \{(x, \varphi(x)) : x \in \mathbb{R}\}$.

Die Frage, ob man ein algebraisches Lösungsgebilde als einen Graphen realisieren kann, ist äquivalent dazu, ob man die definierende Gleichung nach y „auflösen“ kann. Im Beispiel kann man $y^2 = r^2 - x^2$ und damit

$$y = \sqrt{r^2 - x^2} = \sqrt{(r - x)(r + x)}$$

schreiben. Ist es also doch ein Graph? Hier gibt es zwei Interpretationen:

- Wenn man sich auf reelle Zahlen und auf positive Wurzeln beschränkt, so hat man im letzten Schritt keine Äquivalenzumformung durchgeführt, und Information „hinzugefügt“, die in der ursprünglichen Gleichung nicht vorhanden war. Die positive Wurzel zu nehmen bedeutet, sich auf den oberen Halbkreis zu beschränken (Information, also Bedingungen hinzufügen, bewirkt, dass die Lösungsmenge verkleinert wird).
- Wenn man stattdessen unter $\sqrt{\quad}$ alle Lösungen berücksichtigt (d.h. im Reellen die positive und die negative Quadratwurzel, was man häufig als $\pm\sqrt{\quad}$ schreibt), so hat man keine Information dazugetan, aber auch nicht nach einer Funktion aufgelöst (sondern nur, wie man manchmal sagt, nach einer „mehrwertigen Funktion“).

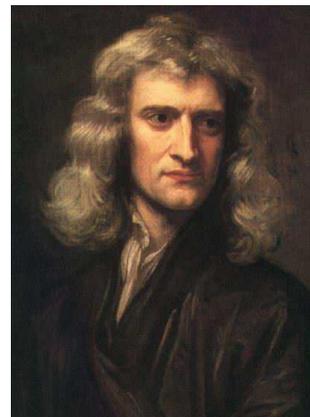
Beide Standpunkte haben etwas für sich. Dass man für einen Teil des geometrischen Objektes (dem oberen Halbbogen) versucht, eine einfache Beschreibung als Graph zu finden, kehrt im Satz über implizite Funktionen, im Potenzreihenansatz, in Parametrisierungen und in der lokalen Theorie wieder.

1.2. Gleichungen der Form $Y^2 = G(X)$.

Eine Kreisgleichung kann man auffassen als eine Gleichung der Form

$$Y^2 = G(X),$$

wobei G ein Polynom in der einen Variablen X bezeichnet (im Fall eines Kreises ist $G = -X^2 + 1$). Das ist kein Graph, aber die „Wurzel“ eines Graphen. Betrachten wir generell eine solche Situation, wo $G(X)$ komplizierter sein darf. Das Nullstellengebilde repräsentiert hier die Quadratwurzel $\sqrt{G(X)}$.



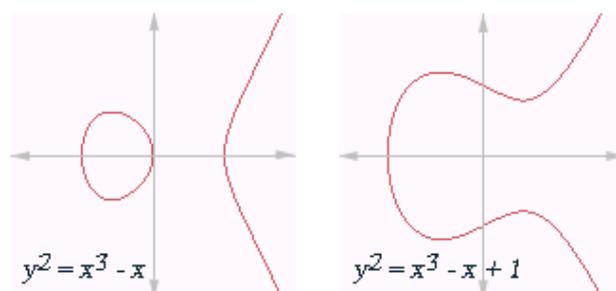
Wenn man sich für X einen beliebigen Wert x vorgibt, so gibt es (im Reellen) drei Möglichkeiten für zugehörige Lösungen:

- Wenn $G(x)$ negativ ist, so gibt es keine Lösung.
- Wenn $G(x) = 0$ ist, so gibt es genau die Lösung $y = 0$.
- Wenn $G(x)$ positiv ist, so gibt es die zwei Lösungen $y = \pm\sqrt{G(x)}$.

Das gibt auch einen Ansatz, wie das reelle Bild aussieht: Für jedes x berechnet man $G(x)$ und markiert bei $(x, \sqrt{G(x)})$ (falls die Wurzel nichtnegativ ist) einen Punkt.

Im Komplexen sind nur die Fälle $G(x) = 0$ oder $G(x) \neq 0$ zu unterscheiden. Wenn G selbst nur den Grad zwei besitzt, so handelt es sich um einen

Kegelschnitt, die schon in der Antike betrachtet wurden. Mit dem Fall, dass $G(X)$ ein kubisches (reelles) Polynom ist (also den Grad drei besitzt), hat sich Isaac Newton intensiv beschäftigt. Dieses Beispielmateriale ist schon sehr reichhaltig.



Betrachten wir den Fall $G(X) = X^3$, also das durch

$$\{(x, y) : y^2 = x^3\}$$

beschriebene Gebilde. Dieses Gebilde nennt man die *Neilsche Parabel*. Hier tritt ein neues Phänomen auf, nämlich, dass der Nullpunkt anders ist als alle anderen Punkte. Man spricht von einer *Singularität*; im Gegensatz dazu nennt man die anderen Punkte *glatt* oder *nicht-singulär*. Eine genaue Definition zu geben ist Teil dieses Kurses, als erste ungenaue Formulierung kann man sagen, dass eine Kurve in einem glatten Punkt lokal und in geeigneten Koordinaten so aussieht wie der (gedrehte) Graph einer differenzierbaren Funktion. Die Singularität in der Neilschen Parabel nennt man auch eine *Spitze* (oder eine *Kuspe*, was einfach Spitze bedeutet). Dagegen ist die Singularität im Bild 8 ein *Kreuzungspunkt* oder *Doppelpunkt*.

Im Bild 7 vom Anfang und oben sieht man ebenfalls Nullstellengebilde der Form $Y^2 = G(X)$, wobei $G(X)$ ein Polynom vom Grad drei ist. Wie sieht $G(X)$ aus, damit sich solch eine Kurve ergibt? Die zuletzt genannten Beispiele zeigen auch, dass es von der genauen Gestalt von $G(X)$ abhängt, ob die Kurve eine Singularität besitzt oder nicht.

Bleiben wir noch bei der Neilschen Parabel C . Wenn t irgendeine reelle oder komplexe Zahl ist, so liegt der Punkt mit den Koordinaten $(x, y) = (t^2, t^3)$ stets auf der Neilschen Parabel, da ja $(t^2)^3 = t^6 = (t^3)^2$ ist. Man kann auch umgekehrt zeigen, dass jeder Punkt der Neilschen Parabel eine solche Gestalt besitzt, dass es also zu (x, y) mit $y^2 = x^3$ ein (und zwar genau ein) t gibt mit $(x, y) = (t^2, t^3)$. Man sagt, dass die Abbildung

$$\mathbb{R} \longrightarrow C, t \longmapsto (t^2, t^3),$$

eine (bijektive polynomiale) *Parametrisierung* der Neilschen Parabel ist. Es ist eine nicht-triviale Frage, welche algebraischen Kurven eine polynomiale Parametrisierung besitzen. Eine Kurve der Form $Y^2 = G(X)$, die glatt ist

und wo G den Grad drei hat, besitzt keine solche Parametrisierung. In der elementaren Zahlentheorie lernt man, dass alle *pythagoreischen Tripel* auf eine einfache übersichtliche Gestalt gebracht werden können. Äquivalent dazu ist eine (rationale) Parametrisierung des rationalen Einheitskreises. Siehe Zahlentheorie (Osnabrück 2008)/Vorlesung 10.

Wir kommen zur ersten allgemeinen Definition.

Definition 1.2. Sei K ein Körper. Eine *ebene affin-algebraische Kurve* über K ist das Nullstellengebilde $V(F) \subseteq K^2$ eines nicht-konstanten Polynoms F in zwei Variablen, also

$$F = \sum_{0 \leq i, j \leq m} a_{ij} X^i Y^j \quad (\text{mit } a_{ij} \in K).$$

D.h. es ist

$$V(F) = \{(x, y) \in K^2 : F(x, y) = \sum_{0 \leq i, j \leq m} a_{ij} x^i y^j = 0\}.$$

Noch ein Lemma, aus dem folgt, dass die oben zuletzt angeführten Kurven nicht algebraisch sind.

Lemma 1.3. *Sei C eine ebene affin-algebraische Kurve und sei L eine Gerade in K^2 . Dann ist der Durchschnitt $C \cap L$ die ganze Gerade, oder er besteht nur aus endlich vielen Punkten.*

Beweis. Eine ebene algebraische Kurve $C = V(F)$ ist nach Definition immer die Nullstelle eines Polynoms F in zwei Variablen. Die Gerade L sei durch die Gleichung $aX + bY + c = 0$ gegeben. Ohne Einschränkung sei $a \neq 0$, dann kann man nach X auflösen und erhält die Geradengleichung $X = \alpha Y + \beta$. Ein Schnittpunkt $P \in C \cap L$ muss also sowohl $F(P) = 0$ erfüllen als auch die Geradengleichung. Mit der Geradengleichung kann man X in F durch $\alpha Y + \beta$ ersetzen. Dadurch wird F zu einem Polynom in der einen Variablen Y , das wir \tilde{F} nennen. Dann ist $P \in C \cap L$ äquivalent dazu, dass $P \in L$ und $\tilde{F}(P) = 0$ ist. D.h. die Schnittmenge wird durch das Polynom \tilde{F} beschrieben. Bei $\tilde{F} = 0$ ist die ganze Gerade der Schnitt. Bei $\tilde{F} \neq 0$ gibt es nur endlich viele Nullstellen. \square

In den obigen Beispielen gibt es aber Geraden, die die Kurven in unendlich vielen Punkten schneiden - deshalb sind sie nicht algebraisch.

1.3. Polynomringe.

Nach diesen einführenden Beispielen fixieren wir ein paar Begrifflichkeiten, die wahrscheinlich schon bekannt sind.

Definition 1.4. Der *Polynomring* über einem kommutativen Ring R besteht aus allen Polynomen

$$P = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$$

mit $a_i \in R$, $n \in \mathbb{N}$, und mit komponentenweiser Addition und einer Multiplikation, die durch distributive Fortsetzung der Regel

$$X^n \cdot X^m := X^{n+m}$$

definiert ist.

Darauf aufbauend kann man auch Polynomringe in mehreren Variablen definieren. Man setzt

$$R[X, Y] := (K[X])[Y], \quad R[X, Y, Z] := (K[X, Y])[Z],$$

etc. Ein Polynom in n Variablen hat die Gestalt

$$F = \sum_{(\nu_1, \dots, \nu_n)} a_{(\nu_1, \dots, \nu_n)} X_1^{\nu_1} \cdots X_n^{\nu_n}.$$

Es wird dabei summiert über eine endliche Summe von *Exponententupel* (ν_1, \dots, ν_n) . Die Ausdrücke $X_1^{\nu_1} \cdots X_n^{\nu_n}$ nennt man auch *Monome*. Ein Polynom schreibt man zumeist abkürzend als $F = \sum_{\nu} a_{\nu} X^{\nu}$. Das Produkt von zwei Monomen bedeutet Addition der Exponententupel, also

$$(X_1^{\nu_1} \cdots X_n^{\nu_n}) \cdot (X_1^{\mu_1} \cdots X_n^{\mu_n}) := X_1^{\nu_1 + \mu_1} \cdots X_n^{\nu_n + \mu_n}.$$

Für uns, im Kontext der algebraischen Geometrie, ist hauptsächlich der Fall interessant, wo der Grundring R ein Körper ist. In der algebraischen Geometrie interessiert man sich für die Gestalt von Nullstellengebilden von Polynomen in mehreren Variablen. Wir werden später sehen, dass die Beziehung zwischen algebraischen und geometrischen Eigenschaften besonders stark ist, wenn der Grundkörper algebraisch abgeschlossen ist.

Definition 1.5. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $F \in K[X]$ eine Nullstelle besitzt.

Definition 1.6. Ein Körper heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $F \in K[X]$ eine Nullstelle besitzt.

Satz 1.7. (*Fundamentalsatz der Algebra*) *Der Körper \mathbb{C} der komplexen Zahlen ist algebraisch abgeschlossen.*

Beweis. Wir werden den Satz hier nicht beweisen. Die Beweise dafür benutzen topologische oder analytische Mittel. \square

Der Fundamentalsatz der Algebra wurde erstmals von Gauss bewiesen.



Carl Friedrich Gauss
(1777-1855)

2. VORLESUNG

2.1. Affin-algebraische Mengen.

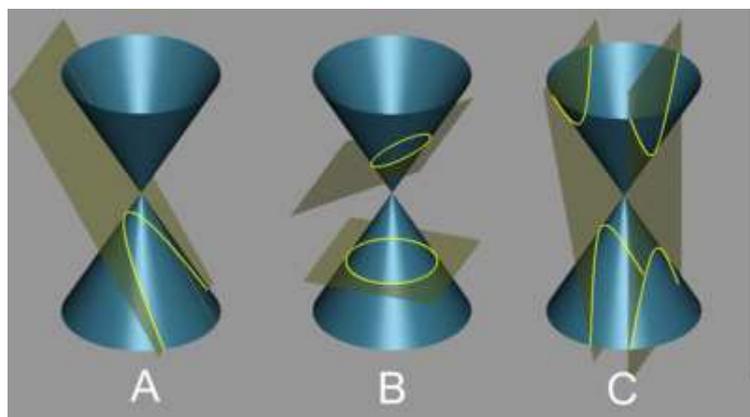
Definition 2.1. Sei K ein Körper. Dann nennt man $\mathbb{A}_K^n = K^n$ den *affinen Raum* über K der Dimension n .

Der affine Raum ist also zunächst einfach eine Menge aus Punkten. Ein Punkt im affinen Raum ist einfach ein n -Tupel (a_1, \dots, a_n) mit Koordinaten aus K . Warum dann ein neuer Begriff? Mit dem Begriff „affiner Raum“ wird angedeutet, dass wir den K^n als Objekt der algebraischen Geometrie verstehen wollen. D.h. wir betrachten den affinen n -dimensionalen Raum als das natürliche geometrische Objekt, auf dem Polynome in n Variablen (als Funktionen) operieren. Wir werden zunehmend den affinen Raum um weitere Strukturen (Zariski-Topologie, Strukturgarbe) ergänzen, die deutlich machen, dass er „mehr“ ist als „nur“ ein K^n . Für $n = 1$ spricht man von der *affinen Geraden* und für $n = 2$ von der *affinen Ebene*.

Ein Polynom $F \in K[X_1, \dots, X_n]$ fasst man in natürlicher Weise als Funktion auf dem affinen Raum auf: einem Punkt $P \in \mathbb{A}_K^n$ mit $P = (a_1, \dots, a_n)$ wird der Wert $F(P) = F(a_1, \dots, a_n)$ zugeordnet, indem die Variable X_i durch a_i ersetzt wird und alles in K ausgerechnet wird. Zu einem Polynom $F \in K[X_1, \dots, X_n]$ kann man insbesondere fragen, ob $F(P) = 0$ ist oder nicht. Zu F rückt dann insbesondere das dadurch definierte „Nullstellengebilde“ ins Interesse, nämlich

$$V(F) = \{P \in \mathbb{A}_K^n : F(P) = 0\}.$$

Davon haben wir schon einige in der ersten Vorlesung kennengelernt. Es ist aber auch sinnvoll, zu untersuchen, wie das gemeinsame (simultane) Nullstellengebilde zu mehreren Polynomen aussieht. Dieses beschreibt den Durchschnitt der einzelnen beteiligten Nullstellengebilde (wie bspw. bei Kegelschnitten, wo man einen Kegel im dreidimensionalen Raum mit verschiedenen Ebenen schneidet).



Daher definieren wir allgemein.

Definition 2.2. Sei K ein Körper und sei $F_j \in K[X_1, \dots, X_n]$, $j \in J$, eine Familie von Polynomen in n Variablen. Dann nennt man

$$\{P \in \mathbb{A}_K^n : F_j(P) = 0 \text{ für alle } j \in J\}$$

das durch die Familie definierte *Nullstellengebilde* (oder *Nullstellenmenge*). Es wird mit $V(F_j, j \in J)$ bezeichnet.

Diejenigen Teilmengen des affinen Raumes, die als Nullstellenmengen auftreten, verdienen einen eigenen Namen.

Definition 2.3. Sei K ein Körper und sei $K[X_1, \dots, X_n]$ der Polynomring in n Variablen. Dann heißt eine Teilmenge $V \subseteq \mathbb{A}_K^n$ im affinen Raum *affin-algebraisch*, wenn sie die Nullstellenmenge zu einer Familie F_j , $j \in J$, von Polynomen $F_j \in K[X_1, \dots, X_n]$ ist, wenn also $V = V(F_j, j \in J)$ gilt.

Beispiel 2.4. Wir betrachten die affine Ebene \mathbb{A}_K^2 und darin einige affin-algebraische Teilmengen, die durch die Variablen X und Y definiert sind. Das Nullstellengebilde $V(X, Y)$ besteht einfach aus dem *Nullpunkt* $(0, 0)$. Die Bedingung sagt ja hier, dass beide Variablen null sein müssen. Die Menge $V(X)$ ist die *Y-Achse* (alle Punkte der Form $(0, y)$) und $V(Y)$ ist die *X-Achse*. Die Menge $V(X + Y)$ besteht aus allen Punkten (x, y) mit $y = -x$. Das ist also die *Gegendiagonale*. Die Menge $V(XY)$ besteht aus den Punkten (x, y) , wo das Produkt $xy = 0$ sein muss. Über einem Körper kann ein Produkt aber nur dann null sein, wenn einer der Faktoren null ist. D.h. es ist $V(XY) = V(X) \cup V(Y)$ und es liegt das *Achsenkreuz* vor.

Die Punkte in einem affinen Raum oder auf einer affin-algebraischen Menge interpretiert man häufig so, dass sie selbst ein gewisses komplizierteres mathematisches Objekt repräsentieren. Eigenschaften der Objekte werden dann dadurch reflektiert, dass die repräsentierenden Punkte gewisse algebraische Gleichungen erfüllen oder nicht, oder, was äquivalent ist, auf gewissen affin-algebraischen Mengen liegen oder nicht. Dies soll durch das nächste Beispiel illustriert werden.

Beispiel 2.5. (Matrizen) Eine 2×2 -Matrix

$$\begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$$

ist durch die vier Zahlen $a_{11}, a_{21}, a_{12}, a_{22} \in K$ eindeutig festgelegt. Man kann eine Matrix also mit einem Punkt im \mathbb{A}_K^4 identifizieren. Bei dieser Interpretation ist es sinnvoll, die Variablen mit $X_{11}, X_{21}, X_{12}, X_{22}$ zu bezeichnen. Man kann sich dann fragen, welche Eigenschaften von Matrizen sich durch algebraische Gleichungen beschreiben lassen.

Eine *obere Dreiecksmatrix* liegt vor, wenn $a_{12} = 0$ ist. Die Menge der oberen Dreiecksmatrizen ist also die Nullstellenmenge von X_{12} .

Eine *invertierbare Matrix* liegt vor, wenn $a_{11}a_{22} - a_{12}a_{21} \neq 0$ ist. Die Menge der nicht invertierbaren Matrizen wird also durch die algebraische *Determinantenbedingung* $X_{11}X_{22} - X_{12}X_{21} = 0$ beschrieben.

Eine Matrix beschreibt die Multiplikation mit einem Skalar, wenn sie eine Diagonalmatrix mit konstantem Diagonaleintrag ist. Diese Menge wird durch die drei Gleichungen $X_{12} = 0$, $X_{21} = 0$ und $X_{11} - X_{22} = 0$ beschrieben.

Ein Element $\lambda \in K$ ist ein *Eigenwert* einer Matrix genau dann, wenn λ eine Nullstelle des *charakteristischen Polynoms* der Matrix ist, d.h. wenn

$$\det \begin{pmatrix} \lambda - a_{11} & -a_{21} \\ -a_{12} & \lambda - a_{22} \end{pmatrix} = \lambda^2 - \lambda(a_{11} + a_{22}) + a_{11}a_{22} - a_{12}a_{21} = 0$$

ist. In der linearen Algebra ist normalerweise die Matrix vorgegeben und man sucht nach Nullstellen λ dieses Polynoms in einer Variablen. Man kann es aber auch umgekehrt sehen und λ vorgeben, und das Nullstellengebilde

$$\lambda^2 - \lambda(X_{11} + X_{22}) + X_{11}X_{22} - X_{12}X_{21} = 0$$

in den vier Variablen untersuchen. Diese Gleichung beschreibt also die Menge aller Matrizen, die λ als Eigenwert besitzen.

Entsprechend besitzt eine Matrix genau dann die beiden Eigenwerte $\lambda \neq \delta$, wenn

$$\lambda^2 - \lambda(X_{11} + X_{22}) + X_{11}X_{22} - X_{12}X_{21} = 0$$

und

$$\delta^2 - \delta(X_{11} + X_{22}) + X_{11}X_{22} - X_{12}X_{21} = 0$$

ist. Die Differenz der beiden Gleichungen ist

$$\lambda^2 - \delta^2 - (\lambda - \delta)(X_{11} + X_{22}) = 0,$$

die eine solche Matrix erst recht erfüllen muss. Wegen $\lambda \neq \delta$ kann man das schreiben als

$$X_{11} + X_{22} = \lambda + \delta.$$

Für eine Matrix nennt man die Summe der Diagonaleinträge die *Spur* der Matrix. Die zuletzt hingeschriebene Gleichung besagt also, dass für eine Matrix mit Eigenwerten $\lambda \neq \delta$ die Spur die Summe dieser Eigenwerte sein muss.

Das charakteristische Polynom einer Matrix kann man auch schreiben als

$$\lambda^2 - \lambda \cdot \text{Spur}(M) + \text{Det}(M),$$

mit

$$\text{Spur}(M) = X_{11} + X_{22} \text{ und } \text{Det}(M) = X_{11}X_{22} - X_{12}X_{21}.$$

Insbesondere haben Matrizen genau dann das gleiche charakteristische Polynom, wenn ihre Spur und ihre Determinante übereinstimmt. Damit kann man auch sagen, dass die Menge der Matrizen mit einem vorgegebenen charakteristischen Polynom die *Faser* unter der Abbildung

$$\mathbb{A}_K^4 \longrightarrow \mathbb{A}_K^2, M \longmapsto (\text{Spur}(M), \text{Det}(M)),$$

ist. Diese Abbildung ist durch einfache polynomiale Ausdrücke gegeben. Ist diese Abbildung surjektiv? Sehen die Fasern immer gleich aus, d.h., besitzt die Menge der Matrizen mit vorgegebener Spur und Determinante immer die gleiche Struktur, oder gibt es da Unterschiede. Sei s und d vorgegeben. Dann geht es um die Lösungsmenge zu

$$X_{11} + X_{22} = s \text{ und } X_{11}X_{22} - X_{12}X_{21} = d.$$

Hierbei ist X_{11} durch X_{22} eindeutig festgelegt, und umgekehrt. Man kann daher eine Variable *eliminieren*, indem man $X_{22} = s - X_{11}$ setzt. Dann ergibt sich das „äquivalente“ System in den drei Variablen X_{11}, X_{12}, X_{21} , mit der einzigen Gleichung

$$X_{11}(s - X_{11}) - X_{12}X_{21} = d \text{ bzw. } X_{11}^2 - sX_{11} + X_{12}X_{21} + d = 0.$$

Unter „äquivalent“ verstehen wir hier, dass die Lösungen des einen System mit den Lösungen des anderen Systems in einer Bijektion stehen, die durch Polynome gegeben ist. An dieser letzten Umformung sieht man, dass es bei $K = \mathbb{R}$ stets eine Lösung geben muss: man wählt x_{12} negativ und x_{21} hinreichend groß, so dass $+x_{12}x_{21} + d$ negativ ist. Dann liegt ein quadratisches Polynom in der einen Variablen X_{11} vor, und für $x_{11} = 0$ ergibt sich ein negativer Wert. Da der Leitkoeffizient positiv ist, muss dieses Polynom auch Nullstellen haben.

Durch eine *Variablentransformation* kann man die Gleichung noch weiter vereinfachen. Sie vorausgesetzt, dass 2 in K invertierbar ist (dass also die Charakteristik von K nicht 2 ist). Dann kann man mit $X = X_{11} - s/2$ (und mit $Y = X_{12}, Z = X_{21}$) schreiben

$$X^2 + YZ + c$$

mit $c = -\frac{s^2}{4} + d$. Daraus sieht man, dass die Gestalt der Matrizenmenge mit vorgegebener Spur und Determinante nur von $-\frac{s^2}{4} + d$ abhängt. In der Tat ist nun, wenn dieser Term null ist oder nicht, das Nullstellengebilde verschieden. Im ersten Fall hat es eine Singularität, im zweiten Fall nicht, wie wir später sehen werden.

2.2. Ideale und Nullstellengebilde.

Da wir zunächst beliebige Familien von Polynomen zulassen, die Nullstellengebilde und damit affin-algebraische Mengen definieren, erscheinen diese zunächst sehr unübersichtlich. Es gelten hier aber drei wichtige Aussagen, die wir nach und nach beweisen werden, nämlich:

- (1) Das Nullstellengebilde zu einer Polynom-Familie ist gleich dem Nullstellengebilde des Ideals, das von der Familie erzeugt wird.
- (2) Zu jedem Ideal gibt es ein endliches Ideal-Erzeugendensystem, so dass jedes Nullstellengebilde durch endlich viele Polynome beschrieben werden kann (Hilbertscher Basissatz).

- (3) Über einem algebraisch abgeschlossenen Körper stehen die Nullstellengebilde in Bijektion mit den sogenannten Radikalen (das sind spezielle Ideale) (Hilbertscher Nullstellensatz).

Die erste dieser Aussagen können wir sofort beweisen, die anderen beiden verlangen einige algebraische Vorbereitungen, die wir in den nächsten Vorlesungen entwickeln werden.

Lemma 2.6. *Sei K ein Körper und sei $F_j \in K[X_1, \dots, X_n]$, $j \in J$, eine Familie von Polynomen in n Variablen. Es sei \mathfrak{a} das von den F_j erzeugte Ideal in $K[X_1, \dots, X_n]$. Dann ist*

$$V(F_j, j \in J) = V(\mathfrak{a}).$$

Beweis. Das Ideal \mathfrak{a} besteht aus allen Linearkombinationen der F_j und enthält insbesondere alle F_j . Daher ist die Inklusion $V(F_j, j \in J) \supseteq V(\mathfrak{a})$ klar. Für die umgekehrte Inklusion sei $P \in V(F_j, j \in J)$ und sei $H \in \mathfrak{a}$. Dann ist $H = \sum_{i=1}^k A_i F_{j_i}$ (mit $A_i \in K[X_1, \dots, X_n]$) und somit ist

$$H(P) = \sum_{i=1}^k A_i(P) F_{j_i}(P) = 0,$$

also verschwindet jedes Element aus dem Ideal im Punkt P . Daher ist $P \in V(\mathfrak{a})$. \square

Wir können also im Folgenden bei jeder Nullstellenmenge davon ausgehen, dass sie durch ein Ideal gegeben ist.

Lemma 2.7. *Für Ideale $\mathfrak{a} \subseteq \mathfrak{b}$ in $K[X_1, \dots, X_n]$ gilt $V(\mathfrak{a}) \supseteq V(\mathfrak{b})$ für die zugehörigen Nullstellengebilde.*

Beweis. Sei $P \in V(\mathfrak{b})$. D.h. für jedes $F \in \mathfrak{b}$ ist $F(P) = 0$. Dann ist erst recht $F(P) = 0$ für jedes $F \in \mathfrak{a}$. \square

Affin-algebraische Teilmengen des affinen Raumes erfüllen einige wichtige strukturelle Eigenschaften.

Proposition 2.8. *Sei K ein Körper, $K[X_1, \dots, X_n]$ der Polynomring in n Variablen und sei \mathbb{A}_K^n der zugehörige affine Raum. Dann gelten folgende Eigenschaften*

- (1) $V(0) = \mathbb{A}_K^n$, d.h. der ganze affine Raum ist eine affin-algebraische Menge.
- (2) $V(1) = \emptyset$, d.h. die leere Menge ist eine affin-algebraische Menge.
- (3) Es seien V_1, \dots, V_k affin-algebraische Mengen mit $V_i = V(\mathfrak{a}_i)$. Dann gilt

$$V_1 \cup V_2 \cup \dots \cup V_k = V(\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_k).$$

Insbesondere ist die Vereinigung von endlich vielen affin-algebraischen Mengen wieder eine affin-algebraische Menge.

- (4) Es seien V_i , $i \in I$, affin-algebraische Mengen mit $V_i = V(\mathfrak{a}_i)$. Dann gilt

$$\bigcap_{i \in I} V_i = V\left(\sum_{i \in I} \mathfrak{a}_i\right).$$

Insbesondere ist der Durchschnitt von beliebig vielen affin-algebraischen Mengen wieder eine affin-algebraische Menge.

Beweis. (1) und (2) sind klar, da das konstante Polynom 0 überall und das konstante Polynom 1 nirgendwo verschwindet.

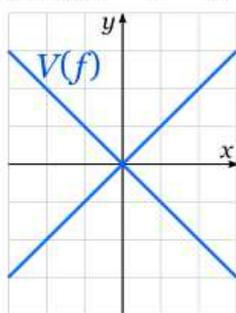
(3). Sei P ein Punkt in der Vereinigung, sagen wir $P \in V(\mathfrak{a}_1)$. D.h. $f(P) = 0$ für jedes Polynom $f \in \mathfrak{a}_1$. Ein beliebiges Element aus dem Produktideal $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_k$ hat die Gestalt

$$h = \sum_{j=1}^m r_j f_{1j} \cdot f_{2j} \cdots f_{kj}$$

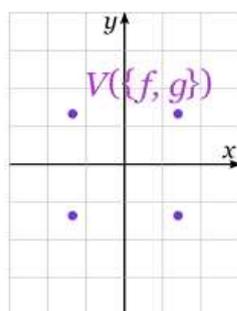
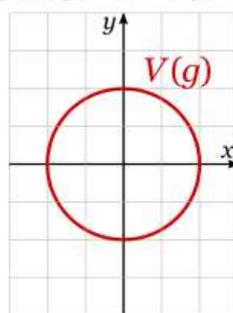
mit $f_{ij} \in \mathfrak{a}_i$. Damit ist $h(P) = 0$, da stets $f_{1j}(P) = 0$ gilt, also gehört P zum rechten Nullstellengebilde. Gehört hingegen P nicht zu der Vereinigung links, so ist $P \notin V(\mathfrak{a}_i)$ für alle $i = 1, \dots, k$. D.h. es gibt $f_i \in \mathfrak{a}_i$ mit $f_i(P) \neq 0$. Dann ist aber $(f_1 f_2 \cdots f_k)(P) \neq 0$ und $f_1 f_2 \cdots f_k \in \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_k$, so dass P nicht zur Nullstellenmenge rechts gehören kann.

(4). Sei $P \in \mathbb{A}_K^n$. Dann ist $P \in V(\mathfrak{a}_i)$ für alle $i \in I$ genau dann, wenn $f(P) = 0$ ist für alle $f \in \mathfrak{a}_i$ und für alle $i \in I$. Dies ist genau dann der Fall, wenn $f(P) = 0$ ist für alle f aus der Summe dieser Ideale. \square

$$f(x, y) = x^2 - y^2$$



$$g(x, y) = x^2 + y^2 - 4$$



3. VORLESUNG

3.1. Die Zariski-Topologie.

In Proposition 2.8 haben wir gezeigt, dass die affin-algebraischen Teilmengen eines affinen Raumes die Axiome für abgeschlossene Mengen einer Topologie erfüllen. Diese Topologie nennt man die Zariski-Topologie.

Definition 3.1. In einem affinen Raum \mathbb{A}_K^n versteht man unter der *Zariski-Topologie* diejenige Topologie, bei der die affin-algebraischen Mengen als abgeschlossen erklärt werden. Die offenen Mengen der Zariski-Topologie sind also die Komplemente der affin-algebraischen Mengen.

Die Zariski-Topologie weicht sehr stark von anderen Topologien ab, insbesondere von solchen, die durch eine Metrik gegeben sind. Insbesondere ist die Zariski-Topologie nicht *Haussdorfsch*. Generell kann man sagen, dass die offenen Mengen (außer der leeren Menge) in der Zariski-Topologie sehr groß sind (siehe Aufgabe 3.8), während die abgeschlossenen (also die affin-algebraischen Mengen) sehr dünn sind (außer dem ganzen Raum selbst).

Beispiel 3.2. (Affine Gerade) Die Zariski-Topologie auf der affinen Geraden \mathbb{A}_K^1 lässt sich einfach beschreiben. Als (Zariski-)abgeschlossene Teilmengen haben wir zunächst einmal die gesamte affine Gerade, die durch $V(0)$ beschrieben wird. Alle anderen abgeschlossenen Teilmengen werden durch $V(\mathfrak{a})$ mit $\mathfrak{a} \neq 0$ beschrieben. Da $K[X]$ ein Hauptidealbereich ist, kann man sogar $\mathfrak{a} = (f)$, $f \neq 0$, ansetzen. Die zugehörige Nullstellenmenge besteht also aus endlich vielen Punkten. Andererseits ist jeder einzelne Punkt P mit der Koordinate a die einzige Nullstelle des linearen Polynoms $X - a$, also ist $\{P\} = V(X - a)$ Zariski-abgeschlossen. Eine endliche Ansammlung von Punkten P_1, \dots, P_k mit den Koordinaten a_1, \dots, a_k ist die Nullstellenmenge des Polynoms $(X - a_1) \cdots (X - a_k)$. Die Zariski-abgeschlossenen Mengen der affinen Geraden bestehen also aus allen endlichen Teilmengen (einschließlich der leeren) und der gesamten Menge.



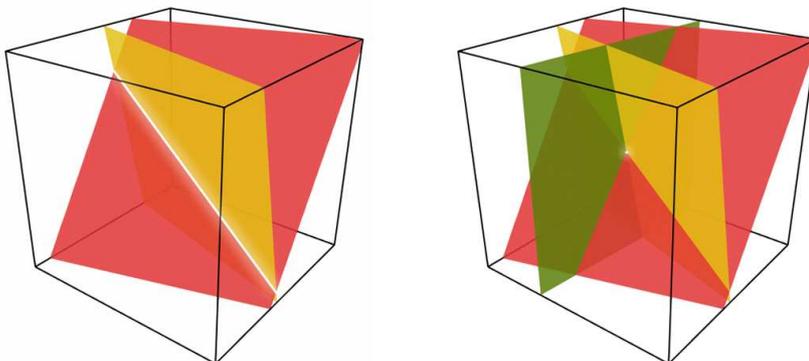
Beispiel 3.3. (Punkt im affinen Raum) Jeder Punkt

$$P = (a_1, \dots, a_n) \in \mathbb{A}_K^n$$

ist Zariski-abgeschlossen, und zwar ist

$$P = V(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n).$$

Punkte sind (neben der leeren Menge und dem gesamten Raum) die einfachsten affin-algebraischen Mengen. Das Ideal $(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$ ist maximal, siehe Aufgabe 2.6.



3.2. Das Verschwindungsideal.

Definition 3.4. Sei $T \subseteq \mathbb{A}_K^n$ eine Teilmenge. Dann nennt man

$$\{F \in K[X_1, \dots, X_n] : F(P) = 0 \text{ für alle } P \in T\}$$

das *Verschwindungsideal* zu T . Es wird mit $\text{Id}(T)$ bezeichnet.

Es handelt sich dabei in der Tat um ein Ideal: wenn $F(P) = 0$ und $G(P) = 0$ ist für alle $P \in T$, so gilt dies auch für die Summe $F + G$ und für jedes Vielfache HF . Damit haben wir zwei Zuordnungen in entgegengesetzte Richtung. Einer Teilmenge im affinen Raum wird das Verschwindungsideal zugeordnet und einem Ideal im Polynomring das zugehörige Nullstellengebilde. Wir interessieren uns dafür, in wie fern sich Ideale und Nullstellengebilde entsprechen.

Beispiel 3.5. (Verschwindungsideal zu einem Punkt) Sei $P = (a_1, \dots, a_n) \in \mathbb{A}_K^n$. Dann ist das Verschwindungsideal $\text{Id}(P)$ gleich dem Ideal $(X_1 - a_1, \dots, X_n - a_n)$. Zunächst ist klar, dass die linearen Polynome $X_i - a_i$ im Punkt P verschwinden (wegen $(X_i - a_i)(P) = a_i - a_i = 0$). Damit gehört auch das von diesen Polynomen erzeugte Ideal zum Verschwindungsideal. Sei umgekehrt F ein Polynom mit $F(P) = 0$. Wir schreiben F in den „neuen Variablen“

$$\tilde{X}_1 = X_1 - a_1, \dots, \tilde{X}_n = X_n - a_n,$$

indem wir X_i durch $X_i - a_i + a_i$ ersetzen. In den neuen Variablen sei $F = \sum_{\nu} b_{\nu} \tilde{X}^{\nu}$. Dieses Polynom besteht aus der Konstanten b_0 , in jedem anderen Monom kommt mindestens eine Variable vor. Also können wir schreiben

$$F = F_1 \tilde{X}_1 + \dots + F_n \tilde{X}_n + c,$$

mit gewissen Polynomen F_i . Daher ist $F(P) = c = 0$ und $F \in (\tilde{X}_1, \dots, \tilde{X}_n)$.

Lemma 3.6. *Seien $V \subseteq W \subseteq \mathbb{A}_K^n$ zwei Teilmengen. Dann gilt für die zugehörigen Verschwindungsideale die Inklusion*

$$\text{Id}(W) \subseteq \text{Id}(V).$$

Beweis. Sei $F \in \text{Id}(W)$, d.h. es ist $F(P) = 0$ für alle $P \in W$. Dann ist erst recht $F(P) = 0$ für alle $P \in V$. Also ist auch $F \in \text{Id}(V)$. \square

Lemma 3.7. *Sei $I \subseteq K[X_1, \dots, X_n]$ ein Ideal und sei $T \subseteq \mathbb{A}_K^n$ eine Teilmenge. Dann gelten folgende Aussagen.*

- (1) *Es ist $T \subseteq V(\text{Id}(T))$.*
- (2) *Es ist $I \subseteq \text{Id}(V(I))$.*
- (3) *Es ist $V(I) = V(\text{Id}(V(I)))$.*
- (4) *Es ist $\text{Id}(T) = \text{Id}(V(\text{Id}(T)))$.*

Beweis. (1). Sei $P \in T$ ein Punkt. Dann verschwindet nach Definition jedes Polynom $F \in \text{Id}(T)$ auf T , also $P \in V(\text{Id}(T))$.

(2). Sei $F \in I$. Dann verschwindet F auf ganz $V(I)$ und daher $F \in \text{Id}(V(I))$.

(3). Nach (1), angewandt auf $T = V(I)$, haben wir die Inklusion „ \subseteq “. Nach (2) ist $I \subseteq \text{Id}(V(I))$. Wendet man darauf $V(-)$ an, so ergibt sich nach Lemma 2.7 die andere Inklusion.

(4). Wie (3). \square

Beispiel 3.8. Die Inklusionen in Lemma 3.7 (1), (2) sind echt. Sei zum Beispiel $T \subset \mathbb{A}_K^1$ eine unendliche echte Teilmenge (was voraussetzt, dass K unendlich ist). Dann ist $\text{Id}(T) = 0$, und also ist $V(0) = \mathbb{A}_K^1$ echt größer als T .

Zu (2): Sei $I = (X^2)$, $R = K[X]$. Dann ist $V(I) = \{0\}$ und $\text{Id}(\{0\}) = (X)$, aber $X^2 \notin (X)$. Ein extremeres Beispiel für $R = \mathbb{R}[X, Y]$ ist $I = (X^2 + Y^2)$ mit $V(I) = \{(0, 0)\}$. Das Verschwindungsideal zu diesem Punkt ist aber das Ideal (X, Y) .

Lemma 3.9. *(Zariski-Abschluss) Sei $T \subseteq \mathbb{A}_K^n$ eine Teilmenge. Dann ist der Zariski-Abschluss von T gleich*

$$\overline{T} = V(\text{Id}(T)).$$

Beweis. Sei zunächst $P \in T$. Dann ist $F(P) = 0$ für alle $F \in \text{Id}(T)$. Dann ist $P \in V(\text{Id}(T))$. Da $V(\text{Id}(T))$ nach Definition abgeschlossen ist, folgt $\overline{T} \subseteq V(\text{Id}(T))$.

Sei umgekehrt $P \in V(\text{Id}(T))$ und sei $P \notin \overline{T}$ angenommen. Dies bedeutet, dass es eine Zariski-offene Menge U gibt mit $P \in U$ und $U \cap T = \emptyset$. Sei $U = D(\mathfrak{a})$. Die Bedingung $P \in U$ bedeutet, dass es ein $G \in \mathfrak{a}$ geben muss mit $G(P) \neq 0$. Es ist dann $P \in D(G) \subseteq U$ und damit $T \cap D(G) = \emptyset$. Also ist $T \subseteq V(G)$ und somit $G \in \text{Id}(T)$. Wegen $G(P) \neq 0$ ergibt sich ein Widerspruch zu $P \in V(\text{Id}(T))$. \square

3.3. Das Radikal.

Definition 3.10. Ein Ideal \mathfrak{a} in einem kommutativen Ring R heißt *Radikal* (oder *Radikalideal*), wenn folgendes gilt: falls $f^n \in \mathfrak{a}$ ist für ein $n \in \mathbb{N}$, so ist bereits $f \in \mathfrak{a}$.

Definition 3.11. Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann nennt man die Menge

$$\{f \in R : \text{es gibt ein } r \text{ mit } f^r \in \mathfrak{a}\}$$

das *Radikal* zu \mathfrak{a} . Es wird mit $\text{rad}(\mathfrak{a})$ bezeichnet.

Das Radikal zu einem Ideal ist selbst ein Radikal und insbesondere ein Ideal.

Lemma 3.12. Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist das Radikal zu \mathfrak{a} ein Radikalideal.

Beweis. Wir zeigen zunächst, dass ein Ideal vorliegt. 0 gehört offenbar zum Radikal und mit $f \in \text{rad}(\mathfrak{a})$, sagen wir $f^r \in \mathfrak{a}$, ist auch $(af)^r = a^r f^r \in \mathfrak{a}$, also gehört af zum Radikal. Zur Summeneigenschaft seien $f, g \in \text{rad}(\mathfrak{a})$ mit $f^r \in \mathfrak{a}$ und $g^s \in \mathfrak{a}$. Dann ist

$$\begin{aligned} (f+g)^{r+s} &= \sum_{i+j=r+s} \binom{r+s}{i} f^i g^j \\ &= \sum_{i+j=r+s, i < r} \binom{r+s}{i} f^i g^j + \sum_{i+j=r+s, i \geq r} \binom{r+s}{i} f^i g^j \in \mathfrak{a} \end{aligned}$$

Sei nun $f^k \in \text{rad}(\mathfrak{a})$. Dann ist $(f^k)^r = f^{kr} \in \mathfrak{a}$, also $f \in \text{rad}(\mathfrak{a})$. \square

Lemma 3.13. Sei $T \subseteq \mathbb{A}_K^n$ eine Teilmenge. Dann ist das Verschwindungsideal zu T ein Radikal.

Beweis. Sei $F \in K[X_1, \dots, X_n]$ ein Polynom, und sei $F^s \in \text{Id}(T)$. Dann ist $F^s(P) = 0$ für alle $P \in T$. Dann ist aber auch $F(P) = 0$ für alle $P \in V$, also $F \in \text{Id}(T)$. \square

Wir werden später sehen, dass über einem algebraisch abgeschlossenen Körper sich Radikale und algebraische Nullstellengebilde entsprechen. Das ist der Inhalt des *Hilbertschen Nullstellensatzes*.

4. VORLESUNG

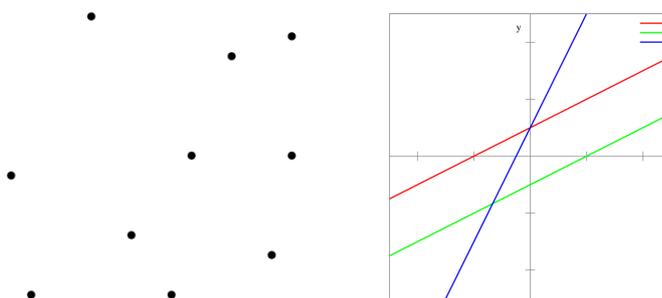
4.1. Irreduzible affin-algebraische Mengen.

Definition 4.1. Eine affin-algebraische Menge $V \subseteq \mathbb{A}_K^n$ heißt *irreduzibel*, wenn $V \neq \emptyset$ ist und es keine Zerlegung $V = Y \cup Z$ mit affin-algebraischen Mengen $Y, Z \subset V$ gibt.

Die Zariski-abgeschlossene Menge V ist also irreduzibel genau dann, wenn $V \neq \emptyset$ ist und eine Zerlegung $V = Y \cup Z$ nur möglich ist mit $V = Y$ oder mit $V = Z$. Dasselbe folgt dann sofort für endliche Darstellungen.

Die Irreduzibilität ist eine rein topologische Eigenschaft, wobei man obige Definition mit abgeschlossenen Mengen formulieren muss anstatt mit affin-algebraischen Mengen (den abgeschlossenen Mengen in der Zariski-Topologie).

Die folgenden Bilder zeigen einige nicht irreduzible affin-algebraische Teilmengen. Was sind dabei die irreduziblen Komponenten (siehe unten)?



Beispiel 4.2. (Der affine Raum) Wir betrachten den affinen Raum \mathbb{A}_K^n . Wenn K endlich ist, so besteht der Raum nur aus endlich vielen Punkten und nur die einpunktigen Teilmengen sind irreduzibel. Insbesondere ist der affine Raum außer bei $n = 1$ nicht irreduzibel.

Bei unendlichem K ist der affine Raum \mathbb{A}_K^n hingegen irreduzibel. Sei nämlich $\mathbb{A}_K^n = Y \cup Z$ mit echten affin-algebraischen Teilmengen. D.h. für die offenen Komplemente $U = \mathbb{A}_K^n - Y$ und $W = \mathbb{A}_K^n - Z$ ist einerseits $U, W \neq \emptyset$, aber $U \cap W = \emptyset$. Das widerspricht aber Aufgabe 3.8.

Lemma 4.3. Sei $V \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge mit Verschwindungsideal $\text{Id}(V)$. Dann ist V irreduzibel genau dann, wenn $\text{Id}(V)$ ein Primideal ist.

Beweis. Sei $\text{Id}(V)$ kein Primideal. Dann gibt es Polynome $F, G \in K[X_1, \dots, X_n]$ mit $FG \in \text{Id}(V)$, aber $F, G \notin \text{Id}(V)$. Dies bedeutet, dass es Punkte $P, Q \in V$ gibt mit $F(P) \neq 0$ und $G(Q) \neq 0$. Wir betrachten die beiden Ideale $\mathfrak{a}_1 = \text{Id}(V) + (F)$ und $\mathfrak{a}_2 = \text{Id}(V) + (G)$. Wegen $P \in V(\mathfrak{a}_1)$ und $Q \in V(\mathfrak{a}_2)$ ist $V(\mathfrak{a}_1), V(\mathfrak{a}_2) \subset V$. Andererseits ist

$$V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cdot \mathfrak{a}_2) = V(\text{Id}(V)) = V,$$

so dass eine nicht-triviale Zerlegung von V vorliegt und somit V nicht irreduzibel ist.

Sei nun V nicht irreduzibel, mit der nicht-trivialen Zerlegung $V = Y \cup Z$. Sei $Y = V(\mathfrak{a}_1)$ und $Z = V(\mathfrak{a}_2)$. Wegen $Y \subset V$ gibt es $F \in \mathfrak{a}_1$, $F \notin \text{Id}(V)$. Ebenso gibt es $G \in \mathfrak{a}_2$, $G \notin \text{Id}(V)$. Für $P \in V = Y \cup Z$ ist $(FG)(P) = 0$,

da F auf Y und G auf Z verschwindet. Also ist $FG \in \text{Id}(V)$ und daher ist $\text{Id}(V)$ kein Primideal. \square

Definition 4.4. Sei V eine affin-algebraische Menge. Eine affin-algebraische Teilmenge $W \subseteq V$ heißt eine *irreduzible Komponente* von V , wenn sie irreduzibel ist und wenn es keine irreduzible Teilmenge $W \subset W' \subseteq V$ gibt.

Ist V irreduzibel, so ist V selbst die einzige irreduzible Komponente von V . Wir werden später sehen, dass jede affin-algebraische Menge sich schreiben lässt als eine endliche Vereinigung von irreduziblen Komponenten.

Beispiel 4.5. Wir betrachten die Gleichung

$$F = Y^2 + X^2(X + 1)^2 = 0.$$

In den reellen Zahlen hat diese Gleichung zwei Lösungen: da ein reelles Quadrat nie negativ ist, kann F nur dann 0 sein, wenn beide Summanden null sind, und das impliziert einerseits $Y = 0$ und andererseits $X = 0$ oder $X = -1$. Insbesondere ist die reelle Lösungsmenge nicht zusammenhängend und nicht irreduzibel (und das Verschwindungsideal zur reellen Situation ist sehr groß).

Betrachtet man F dagegen über den komplexen Zahlen, so gibt es eine Faktorisierung

$$F = (Y + iX(X + 1))(Y - iX(X + 1))$$

in irreduzible Polynome. Dies zeigt zugleich, dass F als Polynom in $\mathbb{R}[X, Y]$ irreduzibel ist (obwohl das reelle Nullstellengebilde nicht irreduzibel ist). Die Nullstellenmenge über den komplexen Zahlen besteht aus den beiden Graphen $Y = \pm iX(X + 1)$, die sich in $(0, 0)$ und $(-1, 0)$ schneiden.

Bei der Gleichung $Y^2 + Z^2 + X^2(X + 1)^2$ gibt es wieder nur zwei reelle Lösungspunkte, das Polynom ist aber sowohl reell als auch komplex betrachtet irreduzibel.

Beispiel 4.6. (Zwei Zylinder) Wir betrachten im affinen Raum \mathbb{A}_K^3 ($K = \mathbb{R}$) die beiden *Zylinder*

$$S_1 = \{(x, y, z) : x^2 + y^2 = 1\} \text{ und } S_2 = \{(x, y, z) : y^2 + z^2 = 1\}.$$

Das sind beides irreduzible Mengen, wie wir später sehen werden (für K unendlich). Wie sieht ihr Durchschnitt aus? Der Durchschnitt wird beschrieben durch das Ideal \mathfrak{a} , das durch $X^2 + Y^2 - 1$ und $Y^2 + Z^2 - 1$ erzeugt wird. Zieht man die eine Gleichung von der anderen ab, so erhält man

$$X^2 - Z^2 = (X - Z)(X + Z) \in \mathfrak{a}.$$



Die beiden einzelnen Faktoren gehören aber nicht zu \mathfrak{a} , da bspw. $(1, 0, -1)$ ein Punkt des Schnittes ist, an dem $X - Z$ nicht verschwindet (Charakteristik $\neq 2$), und $(1, 0, 1)$ ein Punkt des Schnittes ist, an dem $X + Z$ nicht verschwindet. Die Komponenten des Schnittes werden vielmehr beschrieben durch

$$\mathfrak{b}_1 = \mathfrak{a} + (X - Z) \text{ und } \mathfrak{b}_2 = \mathfrak{a} + (X + Z).$$

Das sind beides Primideale, der Restklassenring ist

$$K[X, Y, Z]/(\mathfrak{b}_1) = K[X, Y, Z]/(\mathfrak{a} + (X - Z)) \cong K[X, Y](X^2 + Y^2 - 1).$$

Um dies zu sehen, eliminiert man Z mit der hinteren Gleichung, und die beiden Zylindergleichungen werden dann identisch. Ebenso ist die Argumentation für das andere Ideal. Geometrisch gesprochen heißt dies, dass ein Punkt des Durchschnittes $S_1 \cap S_2$ in der Ebene $E_1 = V(Z - X)$ oder in der Ebene $E_2 = V(Z + X)$ liegt. Es ist

$$E_1 \cap S_1 = E_1 \cap S_1 \cap S_2 = E_1 \cap S_2$$

und ebenso für E_2 , da auf diesen Ebenen die beiden Zylindergleichungen identisch werden.

Wie sehen die Durchschnitte in den Ebenen aus? Wir betrachten die Ebene E_1 mit den Koordinaten Y und $U = Z + X$. Es ist dann $X = \frac{1}{2}((Z + X) - (Z - X))$ und damit kann man die erste Zylindergleichung als

$$\left(\frac{1}{2}((Z + X) - (Z - X))\right)^2 + Y^2 = 1$$

schreiben. Auf der Ebene E_1 , die ja durch $Z = X$ festgelegt ist, wird aus dieser Gleichung

$$\left(\frac{1}{2}U\right)^2 + Y^2 = 1,$$

also $\frac{1}{4}U^2 + Y^2 = 1$. Dies ist die Gleichung einer *Ellipse*, was auch anschaulich klar ist. Man beachte, dass in der obigen Berechnung des Restklassenringes $K[X, Y, Z]/(\mathfrak{b}_1)$ aber eine Kreisgleichung auftritt. Dies sollte deshalb nicht überraschen, da Kreis und Ellipse durch eine lineare Variablentransformation ineinander überführbar sind und dass daher insbesondere die Restklassenringe isomorph sind. Als „metrisches Gebilde“ sind Kreis und Ellipse verschieden, und der Durchschnitt der beiden Zylinder besteht aus zwei Ellipsen. Bei einer *orthonormalen Variablentransformation* bleibt die metrische Struktur erhalten. Die Variablen $Y, X+Z, X-Z$ definieren eine orthogonale Transformation, so dass zumindest die Winkel und Formen erhalten bleiben, obwohl die Längen sich ändern.

Halten wir also fest: Der Durchschnitt der beiden Zylinder ist

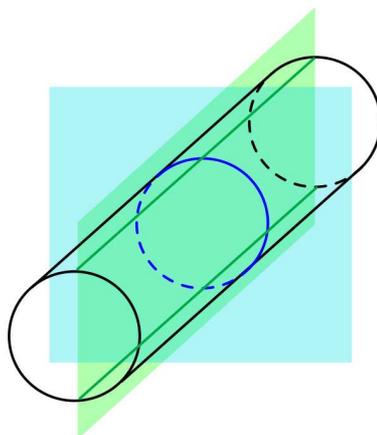
$$S_1 \cap S_2 = V(\mathfrak{b}_1) \cup V(\mathfrak{b}_2),$$

wobei $\mathfrak{b}_1 = (X^2 + Y^2 - 1, X - Z)$ und $\mathfrak{b}_2 = (X^2 + Y^2 - 1, X + Z)$ zwei Ellipsen beschreiben.

Wie liegen diese beiden Ellipsen zueinander? Dazu berechnen wir ihren Durchschnitt, der durch die Summe von \mathfrak{b}_1 und \mathfrak{b}_2 beschrieben wird. Es ist

$$\mathfrak{b}_1 + \mathfrak{b}_2 = (X^2 + Y^2 - 1, X - Z, X + Z) = (Y^2 - 1, X, Z).$$

Die Lösungsmenge davon besteht aus den beiden Punkten $(0, 1, 0)$ und $(0, -1, 0)$.



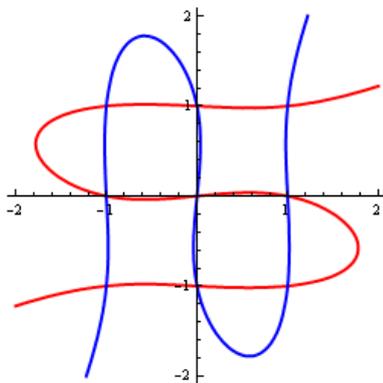
4.2. Zur Anzahl der Punkte auf Kurven.

Wir haben bereits gesehen, dass der Schnitt einer Kurven mit einer Geraden nur aus endlich vielen Punkten besteht, es sei denn die Gerade sei selbst eine Komponente der Kurve (siehe Lemma 1.3). Dies wollen wir zunächst auf den Schnitt von zwei beliebigen ebenen Kurven verallgemeinern. Als Hilfsmittel benötigen wir die folgende Definition.

Definition 4.7. Sei K ein Körper und $K[X]$ der Polynomring in einer Variablen über K . Dann nennt man den Quotientenkörper $Q(K[X])$ den *rationalen Funktionenkörper* über K (oder *Körper der rationalen Funktionen über K*). Er wird mit $K(X)$ bezeichnet.

Satz 4.8. (*Schnitt von ebenen Kurven*) Sei K ein Körper und seien $F, G \in K[X, Y]$ zwei Polynome ohne gemeinsamen nichtkonstanten Faktor. Dann gibt es nur endlich viele Punkte P_1, \dots, P_n mit $P_i \in V(F, G)$.

Beweis. Wir betrachten $F, G \in K[X, Y]$ als Elemente in $K(X)[Y]$, wobei $K(X)$ den Körper der rationalen Funktionen in X bezeichne. Es haben dann nach Aufgabe 4.8 auch F und G keinen gemeinsamen Teiler in $K(X)[Y]$. Da dieser Ring ein Hauptidealbereich ist, erzeugen sie zusammen das Einheitsideal, d.h. es gibt Polynome $A, B \in K(X)[Y]$ mit $AF + BG = 1$. Multiplikation mit dem Hauptnenner von A und B ergibt in $K[X, Y]$ die Gleichung $\tilde{A}F + \tilde{B}G = H$ mit $H \in K[X]$. Eine gemeinsame Nullstelle in \mathbb{A}_K^2 von F und von G muss also eine Nullstelle von H sein. Es gibt also nur endlich viele Werte für X , für die eine gemeinsame Nullstelle vorliegt. Wenn man die Rollen von X und von Y vertauscht, so sieht man, dass es auch nur endlich viele Werte für Y gibt, an denen eine gemeinsame Nullstelle vorliegen kann. Damit kann es überhaupt nur endlich viele gemeinsame Nullstellen geben. \square



5. VORLESUNG

5.1. Homogene Komponenten.

Definition 5.1. Sei S ein kommutativer Ring und $R = S[X_1, \dots, X_n]$ der Polynomring über R in n Variablen. Dann heißt zu einem Monom

$$G = X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$$

die Zahl

$$|\nu| = \sum_{j=1}^n \nu_j$$

der *Grad* von G . Zu einem Polynom $F = \sum_{\nu} a_{\nu} X^{\nu} \neq 0$ heißt das Maximum

$$\max\{|\nu| : a_{\nu} \neq 0\}$$

der *Grad* von F .

Definition 5.2. Sei S ein kommutativer Ring und $R = S[X_1, \dots, X_n]$ der Polynomring über R in n Variablen. Dann heißt zu einem Polynom $F \in R$ mit $F = \sum_{\nu} a_{\nu} X^{\nu}$ die Zerlegung

$$F = \sum_{i=0}^d F_i$$

mit

$$F_i = \sum_{\nu: |\nu|=i} a_{\nu} X^{\nu}$$

die *homogene Zerlegung* von F . Die F_i nennt man die *homogenen Komponenten* von F zum Grad i . Das Polynom F selbst heißt *homogen*, wenn in der homogenen Zerlegung von F nur ein F_i vorkommt.

Beispiel 5.3. Das Polynom

$$F = 4X^3YZ^2 + 2X^2Y^5 + 5XYZ^7 - 3X^4YZ^4 + X^8 - Y^7 + 2Y^6Z^3 + X + 5$$

hat den Grad 9 und die homogenen Komponenten sind

$$F_9 = 5XYZ^7 - 3X^4YZ^4 + 2Y^6Z^3,$$

$$F_8 = X^8,$$

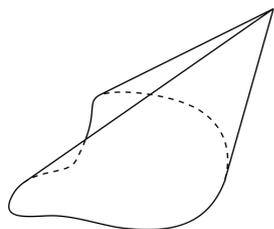
$$F_7 = 2X^2Y^5 - Y^7,$$

$$F_6 = 4X^3YZ^2,$$

$$F_5 = F_4 = F_3 = F_2 = 0,$$

$$F_1 = X \text{ und } F_0 = 5.$$

Wenn man es als Polynom in $(K[Y, Z])[X]$ auffasst und sich nur dafür interessiert, in welcher Potenz X vorkommt, so spricht man vom X -Grad. Der X -Grad von F ist 8. Es gibt natürlich auch eine homogene Zerlegung entlang der X -Graduierung; dabei ist bspw. die Komponente zum X -Grad 0 gleich $-Y^7 + 2Y^6Z^3 + 5$ und zum X -Grad 1 gleich $5XYZ^7 + X$.



Die Nullstellenmenge eines homogenen Polynoms F ist ein (Geraden-)Kegel durch den Nullpunkt. D.h. mit einem Punkt P gehört auch die ganze Gerade durch P und 0 zu $V(F)$.

5.2. Zur Anzahl der Punkte auf Kurven II.

Satz 5.4. (Noethersche Normalisierung im ebenen Fall) Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X, Y]$ ein nicht-konstantes Polynom vom Grad d , das die algebraische Kurve $C = V(F)$ definiert. Dann gibt es eine lineare Koordinatentransformation derart, dass in den neuen Koordinaten \tilde{X}, \tilde{Y} das transformierte Polynom die Form hat

$$\tilde{F} = \tilde{X}^d + \text{Terme von kleinerem Grad in } \tilde{X}.$$

Beweis. Wir schreiben F in homogener Zerlegung als

$$F = F_d + F_{d-1} + \dots + F_1 + F_0$$

mit den homogenen Komponenten

$$F_i = \sum_{a+b=i} c_{a,b} X^a Y^b.$$

Ein homogenes Polynom in zwei Variablen hat die gleichen Faktorisierungseigenschaften wie ein Polynom in einer Variablen. Da wir uns über einem algebraisch abgeschlossenen Körper befinden, gibt es eine Faktorisierung

$$F_d = c(Y - e_1 X) \cdots (Y - e_k X) X^{d-k}.$$

Da c eine d -te Wurzel besitzt können wir durch Streckung der Variablen erreichen, dass $c = 1$ ist. Da K insbesondere unendlich ist, finden wir ein e , das von allen e_j verschieden ist. Wir schreiben die Gleichung in den neuen Variablen

$$\tilde{Y} = Y - eX \text{ und } \tilde{X} = X$$

und erhalten eine Gleichung \tilde{F} , wo die Linearfaktoren von \tilde{F}_d die Gestalt

$$Y - e_j X = Y - eX + eX - e_j X = \tilde{Y} - (e_j - e)X = \tilde{Y} - (e_j - e)\tilde{X}$$

(mit $e_j - e \neq 0$) bzw. $\tilde{X} = X$ haben. Multipliziert man dies aus so sieht man, dass \tilde{X}^d mit einem bestimmten Vorfaktor aus K vorkommt, den wir wieder durch Streckung als 1 annehmen können. Dann hat \tilde{F}_d die Gestalt $\tilde{X}^d +$ Terme, in denen maximal \tilde{X}^{d-1} vorkommt. Die homogenen Komponenten von kleinerem Grad behalten auch ihren Grad, so dass in \tilde{F} nur noch weitere Monome vom \tilde{X} -Grad $\leq d - 1$ gibt. \square

Korollar 5.5. Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X, Y]$ ein nicht-konstantes Polynom, das die algebraische Kurve $C = V(F)$ definiert. Dann besitzt C unendlich viele Elemente.

Beweis. Aufgrund von Satz 5.3 können wir annehmen, dass F die Gestalt hat

$$F = X^d + P_{d-1}(Y)X^{d-1} + \dots + P_1(Y)X + P_0(Y)$$

mit Polynomen $P_i(Y) \in K[Y]$. Zu jedem beliebig vorgegebenen Wert $a \in K$ für Y ergibt sich also ein normiertes Polynom in X vom Grad d . Da der Körper algebraisch abgeschlossen ist, gibt es jeweils (mindestens) eine Nullstelle in

X . D.h. zu jedem $a \in K$ gibt es ein $b \in K$ derart, dass (a, b) eine Nullstelle von F ist, also zur Kurve gehört. Da K unendlich ist, gibt es also unendlich viele Punkte auf der Kurve. \square

5.3. Polynomiale Abbildungen zwischen affinen Räumen.

Wir betrachten nun Abbildungen

$$\begin{aligned} \varphi : \mathbb{A}_K^r &\longrightarrow \mathbb{A}_K^n, \\ (t_1, \dots, t_r) &\longmapsto (\varphi_1(t_1, \dots, t_r), \dots, \varphi_n(t_1, \dots, t_r)) = (x_1, \dots, x_n), \end{aligned}$$

wobei die Komponentenfunktionen $\varphi_i \in K[X_1, \dots, X_r]$ Polynome sind. Die Abbildung wird also in jeder Komponenten durch ein Polynom in r Variablen gegeben. Der Fall $n = 1$ ist der eines Polynoms in r Variablen, der Fall $r = 1$ und $n = 2$ ist der Fall der Parametrisierung von algebraischen Kurven. Später werden wir allgemeiner Morphismen zwischen affin-algebraischen Mengen definieren.

Eine wichtige „Begleiterscheinung“ einer polynomialen Abbildung $\varphi : \mathbb{A}_K^r \rightarrow \mathbb{A}_K^n$ ist, dass sie einen K -Algebra Homomorphismus zwischen den zugehörigen Polynomringen in die entgegengesetzte Richtung induziert, nämlich den durch $X_i \mapsto \varphi_i$ definierten *Einsetzungshomomorphismus*. Diesen bezeichnen wir mit

$$\tilde{\varphi} : K[X_1, \dots, X_n] \longrightarrow K[T_1, \dots, T_r], F \longmapsto F \circ \varphi = F(\varphi_i/X_i)$$

(die Schreibweise φ_i/X_i bedeutet, dass X_i durch φ_i zu ersetzen ist). Als Funktion auf \mathbb{A}_K^r betrachtet ist $F \circ \varphi$ die *hintereinandergeschaltete Abbildung*

$$\mathbb{A}_K^r \xrightarrow{\varphi} \mathbb{A}_K^n \xrightarrow{F} \mathbb{A}_K^1.$$

Für die Nullstellenmenge $V(F) \subseteq \mathbb{A}_K^n$ gilt dabei

$$\varphi^{-1}(V(F)) = V(\tilde{\varphi}(F)).$$

Die einfachsten polynomialen Abbildungen sind, neben den *konstanten Abbildungen*, die *affin-linearen Abbildungen*, die durch lineare Polynome gegeben sind, also

$$\varphi_i = a_{i1}T_1 + \dots + a_{ir}T_r + c_i.$$

Man beachte, dass dies keine linearen Abbildungen sind, da der Nullpunkt nicht auf den Nullpunkt gehen muss, sondern auch *Verschiebungen* zugelassen sind. Eine affin-lineare Abbildung ist die Hintereinanderschaltung einer linearen Abbildung und einer Verschiebung. Im Fall $r = n$ betrachtet man eine solche affin-lineare Abbildung, wenn sie zusätzlich bijektiv ist, als eine (*Koordinaten- oder Variablen-*)*Transformation* des Raumes.

Definition 5.6. Sei K ein Körper. Dann nennt man eine Abbildung $\varphi : \mathbb{A}_K^n \rightarrow \mathbb{A}_K^n$ der Form

$$\varphi(x_1, \dots, x_n) = M(x_1, \dots, x_n) + (v_1, \dots, v_n),$$

wobei M eine invertierbare Matrix ist, eine *affin-lineare Variablentransformation*.

Man kann sich dabei darüber streiten, ob bei einer linearen Variablentransformation im Raum etwas bewegt wird oder ob sich nur die Koordinaten ändern. Jedenfalls sind solche Transformationen wichtige Hilfsmittel, um ein Polynom, ein algebraisches Gleichungssystem oder eine affin-algebraische Menge auf eine einfachere Gestalt zu bringen. Unter einer Variablentransformation wird eine affin-algebraische Menge $V = V(F_1, \dots, F_m)$ zu $\tilde{V} = V(\tilde{F}_1, \dots, \tilde{F}_m)$ (mit $\tilde{F}_i = \tilde{\varphi}(F_i)$) transformiert, und zwar ist dann \tilde{V} das Urbild unter der Abbildung φ .

Definition 5.7. Zwei affin-algebraische Mengen $V, \tilde{V} \subseteq \mathbb{A}_K^n$ heißen *affin-linear äquivalent*, wenn es eine affin-lineare Variablentransformation φ gibt mit $\varphi^{-1}(V) = \tilde{V}$.

Dies ist also ein Begriff, der Bezug darauf nimmt, wie die Situation eingebettet ist. Wir werden später sehen, dass die Parabel und eine Gerade in der Ebene „isomorph“ sind (da sie beide isomorph zur affinen Geraden sind), aber nicht linear äquivalent.

Die wesentlichen algebraischen und topologischen Eigenschaften einer affin-algebraischen Menge bleiben unter einer affin-linearen Variablentransformation erhalten: Irreduzibilität, Singularitäten (später), Überschneidungen, Zusammenhang, Kompaktheit. Dagegen verändern sich typische Eigenschaften der reell-metrischen Geometrie: Winkel, Längen und Längenverhältnisse, Volumina, Formen. Diese zuletzt genannten Begriffe sind nicht relevant für die algebraische Geometrie. Wir werden von nun an ohne große Betonung eine Situation in eine gewünschte Gestalt transformieren, so fern das möglich ist.

Satz 5.8. Sei K ein Körper und seien $V, \tilde{V} \subseteq \mathbb{A}_K^n$ zwei affin-algebraische Teilmengen, die affin-linear äquivalent seien. Es seien $\text{Id}(V), \text{Id}(\tilde{V})$ die zugehörigen Verschwindungsideale. Dann sind die Restklassenringe isomorph, also

$$K[X_1, \dots, X_n]/\text{Id}(V) \cong K[X_1, \dots, X_n]/\text{Id}(\tilde{V}).$$

Beweis. Nach Definition von affin-linear äquivalent gibt es eine affin-lineare Variablentransformation

$$\varphi : \mathbb{A}_K^n \longrightarrow \mathbb{A}_K^n, P \longmapsto \varphi(P),$$

mit $\varphi^{-1}(V) = \tilde{V}$. Es sei $\tilde{\varphi}$ der zugehörige Automorphismus des Polynomrings $K[X_1, \dots, X_n]$. Dabei ist

$$\tilde{\varphi}^{-1}(\text{Id}(\tilde{V})) = \text{Id}(V)$$

Nach dem Isomorphiesatz folgt die Isomorphie der Restklassenringe. \square

Bemerkung 5.9. In diesem Satz kommt zum ersten Mal ein wichtiges Prinzip der algebraischen Geometrie zum Ausdruck, nämlich, dass das algebraische Objekt, das zu einer Nullstellenmenge gehört, der *Restklassenring des Polynomringes nach dem Verschwindungsideal* ist. Dies ist eine „intrinsische Invariante“ der Nullstellenmenge, d.h., unabhängig von einer Einbettung. Unter dieser Betrachtungsweise rückt auch die Noethersche Normalisierung im ebenen Fall in ein neues Licht. Man kann unter den Voraussetzungen der Aussage annehmen, dass die Kurvengleichung die Form

$$F = X^d + P_{d-1}(Y)X^{d-1} + \dots + P_1(Y)X + P_0(Y)$$

besitzt. Wenn man dieses Polynom „gleich null setzt“, so bedeutet dies eine *Ganzheitsgleichung* für X . Genauer, über dem Polynomring $K[Y]$ in einer Variablen ist die Restklasse von X im Restklassenring $K[X, Y]/(F)$ ganz. Diese Begriffe sind vielleicht aus der elementaren Zahlentheorie bekannt und werden auch hier wieder eine wichtige Rolle spielen. Da X über $K[Y]$ den Polynomring erzeugt, liegt überhaupt eine *ganze* (sogar *endliche*) Ringerweiterung

$$K[Y] \longrightarrow K[X, Y]/(X^d + P_{d-1}(Y)X^{d-1} + \dots + P_1(Y)X + P_0(Y))$$

vor. Damit kann man den Noetherschen Normalisierungssatz auch so formulieren, dass sich über einem algebraisch abgeschlossenen Körper zu jeder algebraischen Kurve der zugehörige Restklassenring als endliche Erweiterung des Hauptidealbereiches $K[Y]$ realisieren lässt. Dies ist eine direkte Analogie zu den Ganzheitsringen der Zahlentheorie, die ebenfalls endliche Erweiterungen über dem Hauptidealbereich \mathbb{Z} sind.

Unter beliebigen polynomialen Abbildungen zwischen affinen Räumen können sich, im Gegensatz zu affin-linearen Transformationen, viele algebraische Eigenschaften ändern, die Dimension kann sich ändern, Singularitäten können entstehen, etc. Dagegen überträgt sich die Irreduzibilität auf (den Zariski-Abschluss des) das Bild der Abbildung.

Satz 5.10. *Es sei K ein unendlicher Körper und*

$$\varphi : \mathbb{A}_K^r \longrightarrow \mathbb{A}_K^n$$

sei eine durch n Polynome in r Variablen gegebene Abbildung. Dann ist der Zariski-Abschluss des Bildes der Abbildung irreduzibel.

Beweis. Sei $B = \varphi(\mathbb{A}_K^r)$ das Bild der Abbildung. Nach Lemma 3.8 ist

$$\overline{B} = V(\text{Id}(B)).$$

Nun gilt für $P = \varphi(Q)$ mit $Q \in \mathbb{A}_K^r$ und für $F \in K[X_1, \dots, X_n]$ die Beziehung

$$F(P) = F(\varphi(Q)) = (F \circ \varphi)(Q),$$

wobei $F \circ \varphi \in K[T_1, \dots, T_r]$ das Polynom ist, das sich ergibt, wenn man in F die Variable X_i durch die i -te Koeffizientenfunktion $\varphi_i \in K[T_1, \dots, T_r]$ ersetzt. Daher ist $F(P) = 0$ genau dann, wenn $(F \circ \varphi)(Q) = 0$ ist, und F

verschwindet auf ganz B genau dann, wenn $F \circ \varphi$ auf dem ganzen \mathbb{A}_K^r verschwindet. Da K unendlich ist, bedeutet dies, dass $F \circ \varphi$ das Nullpolynom ist. Daher gilt, dass $F \in \text{Id}(B)$ ist genau dann, wenn F unter dem zugehörigen Ringhomomorphismus

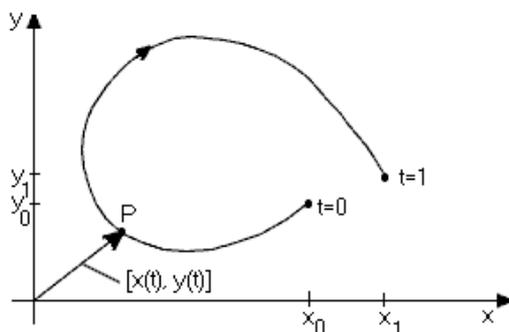
$$\tilde{\varphi} : K[X_1, \dots, X_n] \longrightarrow K[T_1, \dots, T_r]$$

auf null abgebildet wird. Damit ist $\text{Id}(B)$ das Urbild eines Primideals (nämlich des Nullideals) und somit nach Aufgabe 16.8 zur Vorlesung über Zahlentheorie selbst ein Primideal. Aufgrund von Lemma 4.2 ist $V(\text{Id}(B))$ irreduzibel. \square

6. VORLESUNG

6.1. Ebene polynomiale Parametrisierungen.

Wir betrachten jetzt Abbildungen $\varphi : \mathbb{A}_K^1 \rightarrow \mathbb{A}_K^2$, die durch zwei Polynome $P, Q \in K[T]$ in einer Variablen gegeben sind. Das Bild einer solchen Abbildung liegt in einer affinen algebraischen Kurve, wie das folgende Lemma zeigt. Man spricht auch von *parametrisierten Kurven* oder genauer von *polynomial parametrisierten Kurven*. Es konkurrieren hier zwei Standpunkte, wie man eine algebraische Kurve beschreiben kann. Die Punkte einer durch eine Kurvengleichung gegebene Kurve sind nur implizit gegeben. Man kann zwar zu jedem Punkt der Ebene leicht überprüfen, ob er auf der Kurve liegt, es ist aber im Allgemeinen schwierig, Punkte auf der Kurve zu finden oder explizit anzugeben. Eine parametrisierte Kurve ist hingegen explizit gegeben, zu jedem Punkt der affinen Geraden kann man den Bildpunkt einfach ausrechnen und erhält so die Kurvenpunkte explizit. Es ist aber nicht jede algebraische Kurve durch Polynome parametrisierbar.



Eine parametrisierte Kurve kann man sich als einen Bewegungsablauf vorstellen.

Satz 6.1. Sei K ein Körper und seien $P, Q \in K[T]$ zwei Polynome. Dann gibt es ein Polynom $F \in K[X, Y]$, $F \neq 0$, mit $F(Q, P) = 0$. D.h. das Bild einer polynomial parametrisierten Kurve liegt in einer ebenen algebraischen Kurve $C = V(F)$. Wenn K unendlich ist und (P, Q) nicht beide konstant sind, so ist der Zariski-Abschluss des Bildes eine irreduzible Kurve C .

Beweis. Es seien d und e die Grade von P und Q . Wir berechnen die Monome

$$P^i Q^j.$$

Dies sind Polynome in T vom Grad $di + ej$. Zu $i \leq n$ und $j \leq m$ gibt es $(n+1)(m+1)$ solche Monome. Die Monome $P^i Q^j$, $i \leq n$, $j \leq m$, leben also allesamt in dem $dn + em + 1$ -dimensionalen K -Vektorraum, der von $1 = T^0, T^1, T^2, \dots, T^{dn+em}$ erzeugt wird. Bei $(n+1)(m+1) > dn + em + 1$ muss es also eine nicht-triviale lineare Abhängigkeit zwischen diesen $P^i Q^j$ geben. Diese ergibt ein Polynom $F(X, Y) \neq 0$ mit $F(P, Q) = 0$.

Die angegebene numerische Bedingung $(n+1)(m+1) > dn + em + 1$ lässt sich mit n, m hinreichend groß erfüllen.

Von nun an sei K unendlich. Der Zariski-Abschluss des Bildes $B = \varphi(\mathbb{A}_K^1)$ ist $V(\text{Id}(B))$ nach Lemma 3.9 und irreduzibel nach Satz 5.7. Da K unendlich ist und die Abbildung nicht konstant ist, muss wegen der Irreduzibilität auch $V(\text{Id}(B))$ unendlich viele Punkte enthalten. Nach Lemma 4.3 ist $\text{Id}(B)$ ein Primideal und enthält nach dem ersten Teil ein $F \in \text{Id}(B)$, $F \neq 0$. Da $K[X, Y]$ faktoriell ist, muss auch ein Primfaktor von F dazu gehören, so dass wir annehmen können, dass F ein Primpolynom ist. Wir haben die Inklusion

$$B \subseteq \overline{B} = V(\text{Id}(B)) \subseteq V(F).$$

Für ein $H \in \text{Id}(B)$ ist

$$V(\text{Id}(B)) \subseteq V(H) \cap V(F)$$

unendlich, so dass es nach Satz 4.8 einen gemeinsamen nichtkonstanten Faktor geben muss. Da F prim ist, muss H ein Vielfaches von F sein und $\text{Id}(B) = (F)$. \square

Beispiel 6.2. Wir betrachten die Kurve, die durch die Parametrisierung

$$x = t^2 + t + 1 \text{ und } y = 2t^2 + 3t - 1$$

gegeben ist. Es ist $x - 1 = t^2 + t$ und $y + 1 = 2t^2 + 3t$. Eine einfache Addition ergibt

$$(y + 1) - 2(x - 1) = 3t - 2t = t.$$

Daher können wir schreiben

$$x - 1 = t^2 + t = (y - 2x + 3)^2 + (y - 2x + 3).$$

Ausmultiplizieren ergibt insgesamt die Gleichung

$$y^2 + 4x^2 - 4xy - 15x + 7y + 13 = 0.$$

Beispiel 6.3. Wir betrachten die durch

$$P = t^2 - 1 \text{ und } Q = t^3 - t = t(t^2 - 1)$$

gegebene Abbildung $\mathbb{A}_K^1 \rightarrow \mathbb{A}_K^2$. Für die beiden Punkte $t = \pm 1$ ergibt sich der Wert $(0, 0)$. Für alle anderen Stellen $t \neq \pm 1$ kann man schreiben

$$t = \frac{t^3 - t}{t^2 - 1} = \frac{Q(t)}{P(t)}.$$

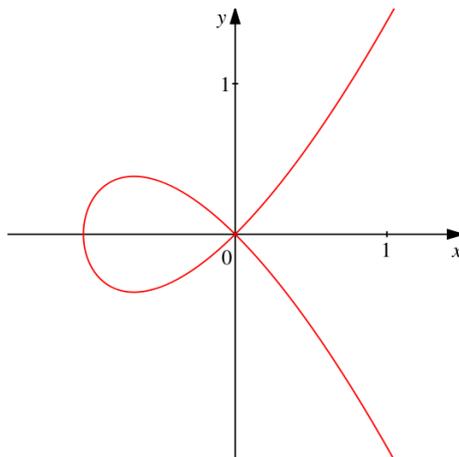
D.h. dass t aus den Bildwerten rekonstruierbar ist, und das bedeutet, dass die Abbildung dort injektiv ist. Die Bildkurve ist also eine Kurve, die sich an genau einer Stelle überschneidet.

Wir bestimmen die Kurvengleichung, und schreiben $x = t^2 - 1$ und $y = t^3 - t$. Es ist $t^2 = x + 1$ und

$$y^2 = t^2 x^2 = (x + 1)x^2 = x^3 + x^2.$$

Das beschreibende Polynom ist also

$$Y^2 - X^3 - X^2.$$



Beispiel 6.4. Wir betrachten die durch

$$X^2 + Y^2 - Z^2 - Z^3 = 0$$

gegebene Fläche im \mathbb{A}_K^3 . Diese Fläche wird auch auf der Seite des Osnabrücker Fachbereiches gezeigt, siehe dort. Wenn man mit einer durch $aX + bY$ gegebenen Ebene (also einer Ebene, die durch eine Grundgerade in der $X - Y$ -Ebene durch den Nullpunkt gegeben ist) schneidet, so erhält man immer eine Gleichung der Form $W^2 - Z^2 - Z^3 = 0$, siehe Beispiel. Die Fläche entsteht, wenn man diese Kurve um die Z -Achse dreht.

6.2. Rationale Parametrisierungen.

Betrachten wir eine rationale Funktion

$$Y = \frac{P}{Q}$$

mit Polynomen $P, Q \in K[X]$ in einer Variablen. Hier hat man in natürlicher Weise sofort eine neue Form der Parametrisierung, indem man die Abbildung

$$\mathbb{A}_K^1 \supseteq D(Q) \longrightarrow \mathbb{A}_K^2, x \longmapsto \left(x, \frac{P(x)}{Q(x)}\right),$$

betrachtet. Dabei ist $D(Q)$ der Definitionsbereich der Abbildung, und zwar besteht $D(Q) = \mathbb{A}_K^1 - V(Q)$ aus allen Punkten, wo das Nennerpolynom nicht null ist. Offenbar kann man mit dieser Abbildung wieder alle Punkte des Graphen der rationalen Funktion erfassen, d.h. sie leistet ebenso wie eine polynomiale Parametrisierung eine explizite Beschreibung der Kurve. Es ist also zur Beschreibung von Kurven sinnvoll, auch Parametrisierungen zuzulassen, bei denen die Komponentenfunktionen rational sind.

Definition 6.5. Zwei rationale Funktionen $\varphi_1 = \frac{P_1}{Q_1}$ und $\varphi_2 = \frac{P_2}{Q_2}$ mit $P_1, P_2, Q_1, Q_2 \in K[T]$, $Q_1, Q_2 \neq 0$, heißen eine *rationale Parametrisierung* einer algebraischen Kurve $C = V(F)$ ($F \in K[X, Y]$ nicht konstant), wenn

$$F(\varphi_1(T), \varphi_2(T)) = 0$$

ist und (φ_1, φ_2) nicht konstant ist.

Man beachte, dass die Gleichheit in der vorstehenden Definition im rationalen Funktionenkörper zu verstehen ist, also in $K(T)$. Bei unendlichem K ist dies äquivalent damit, dass diese Gleichheit gilt für alle Werte $t \in K$, für die die Nennerpolynome definiert sind.

Definition 6.6. Eine ebene algebraische Kurve $C = V(F)$ heißt *rational*, wenn sie irreduzibel ist und es eine rationale Parametrisierung für sie gibt.

Das folgende einfache Beispiel zeigt, dass man mit rationalen Funktionen mehr Kurven parametrisieren kann, als wenn man nur mit Polynomen arbeitet. Es sei aber schon hier erwähnt, dass dieser Unterschied im Kontext der projektiven Geometrie wieder verschwindet.

Beispiel 6.7. (Hyperbel) Wir betrachten die *Hyperbel* $H = V(XY - 1)$ und behaupten, dass es keine polynomiale Parametrisierung davon gibt. Dies folgt einfach daraus, dass zu zwei Polynomen $P(t)$ und $Q(t)$ die Bedingung, für jedes t auf H zu liegen, gerade

$$P(t)Q(t) = 1 \text{ für alle } t \in \mathbb{A}_K^1$$

bedeutet, bzw., dass $P(t)Q(t) = 1$ ist im Polynomring $K[t]$ (was im Fall eines unendlichen Körpers äquivalent ist; bei einem endlichen Körper ist die zweite Identität die „richtige“ Bedingung). Das bedeutet aber, dass diese Polynome invers zueinander sind und daher Einheiten sind. Im Polynomring sind aber lediglich die Konstanten $\neq 0$ Einheiten. Also sind beide Polynome konstant und damit ist die dadurch definierte Abbildung konstant, und es liegt keine Parametrisierung vor.

Wir wollen zeigen, dass das Bild einer nicht-konstanten rationalen Abbildung stets eine algebraische Gleichung erfüllt, also stets eine rationale Parametrisierung einer algebraischen Kurve liefert. Im polynomialen Fall ergab sich eine algebraische Gleichung aus einem Abzählargument (es musste eine Gleichung geben, da die Anzahl der Monome in zwei Variablen „schneller mit dem Grad wächst“ als die in einer Variablen. Wir werden ein ähnliches Argument verwenden, allerdings in Kombination mit einem weiteren Trick, der „Homogenisierung“. Bei diesem Trick wird unter Hinzunahme einer weiteren Variablen (das ist der Preis, den man dabei zahlen muss) eine nicht-homogene Situation homogen gemacht. Diesen Prozess verwenden wir hier rein algebraisch, dahinter steht aber das Zusammenspiel zwischen affiner und projektiver Geometrie.

Definition 6.8. Sei $F \in K[X_1, \dots, X_n]$, $F \neq 0$, ein Polynom in n Variablen mit der homogenen Zerlegung

$$F = \sum_{i=0}^d F_i$$

und sei Z eine weitere Variable. Dann nennt man das homogene Polynom

$$\tilde{F} = \sum_{i=0}^d F_i Z^{d-i}$$

vom Grad d die *Homogenisierung* von F .

Aus der Homogenisierung kann man das ursprüngliche Polynom zurückgewinnen, wenn man die zusätzliche Variable gleich 1 setzt. Man spricht von *dehomogenisieren*.

Lemma 6.9. *Es seien $P_1, P_2, P_3 \in K[S, T]$ drei homogene Polynome. Dann gibt es ein homogenes Polynom $F \in K[X, Y, Z]$, $F \neq 0$, mit*

$$F(P_1, P_2, P_3) = 0.$$

Beweis. Dies folgt aus einem ähnlichen Abzählargument wie im Beweis zu Satz 6.1. \square

Beispiel 6.10. Wir betrachten die Abbildung

$$(S, T) \longmapsto (S^2, T^2, ST) = (X, Y, Z),$$

die durch homogene Polynome (sogar durch Monome) gegeben ist. Es ist einfach, eine algebraische Relation für das Bild zu finden, es ist nämlich

$$Z^2 = (ST)^2 = S^2 T^2 = XY,$$

d.h. das Bild der Abbildung liegt in $V(Z^2 - XY)$. Siehe auch Aufgabe 6.3.

Satz 6.11. *Es seien zwei rationale Funktionen $\varphi_1 = \frac{P_1}{Q_1}$ und $\varphi_2 = \frac{P_2}{Q_2}$ mit $P_1, P_2, Q_1, Q_2 \in K[T]$, $Q_1, Q_2 \neq 0$, gegeben, die nicht beide konstant seien. Dann gibt es ein nicht konstantes Polynom $F \in K[X, Y]$ mit*

$$F(\varphi_1(T), \varphi_2(T)) = 0.$$

Das bedeutet, dass φ_1 und φ_2 eine rationale Parametrisierung definieren.

Beweis. Wir können durch Übergang zu einem Hauptnenner annehmen, dass die rationale Abbildung durch

$$\varphi_1 = \frac{P_1}{Q} \text{ und } \varphi_2 = \frac{P_2}{Q}$$

mit $P_1, P_2, Q \in K[T]$, $Q \neq 0$ gegeben ist. Es seien $H_1, H_2, H_3 \in K[T, S]$ die Homogenisierungen von diesen Polynomen. Dann gibt es nach Lemma 6.9 ein homogenes Polynom F , $F \neq 0$, vom Grad d mit

$$F(H_1, H_2, H_3) = 0.$$

Wir betrachten

$$\frac{1}{Z^d} F(X, Y, Z) = F\left(\frac{X}{Z}, \frac{Y}{Z}, \frac{Z}{Z}\right),$$

welches ein Polynom in den beiden rationalen Funktionen $\frac{X}{Z}, \frac{Y}{Z}$ ist. Für diesen Übergang ist es wichtig, dass F homogen ist. Einsetzen der homogenen Polynome ergibt

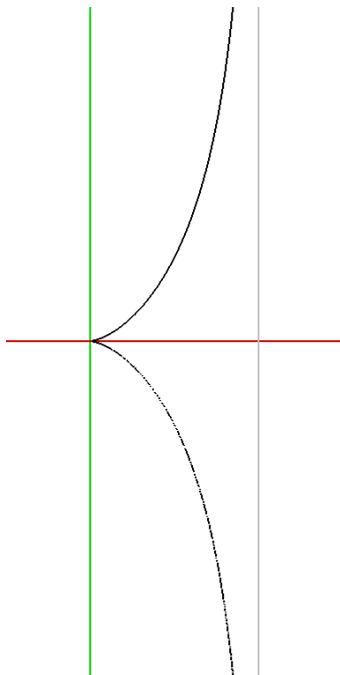
$$0 = F\left(\frac{H_1}{H_3}, \frac{H_2}{H_3}, 1\right).$$

Dies ist eine Gleichheit im Quotientenkörper von $K[S, T]$. Wenn man darin $S = 1$ setzt (also dehomogenisiert), so erhält man

$$0 = F\left(\frac{P_1}{Q}, \frac{P_2}{Q}\right),$$

also eine Gleichung für die ursprünglichen rationalen Funktionen. □

Bemerkung 6.12. Man kann einen Schritt weiter gehen und sich fragen, ob es noch andere Möglichkeiten gibt, eine algebraische Kurve $C = V(F)$ durch eine Abbildung $\varphi : K \rightarrow K^2$ zu beschreiben, wo φ aus einer größeren Funktionenklasse sein darf. Ein wichtiger Satz ist hier der *Satz über implizite Funktionen*, der für $K = \mathbb{R}$ oder $K = \mathbb{C}$ besagt, dass falls die partiellen Ableitung von F an einem Punkt der Kurve nicht beide null sind, dass es dann eine (unendlich oft und sogar analytisch) differenzierbare Abbildung φ gibt, die die Kurve in einer gewissen kleinen offenen Umgebung des Punktes beschreibt. Eine algebraische Version des Satzes über implizite Funktionen findet sich im Potenzreihenansatz wieder, den wir später behandeln werden.



Die Zissoide des Diokles (im Bild schwarz) ist rational parametrisierbar.

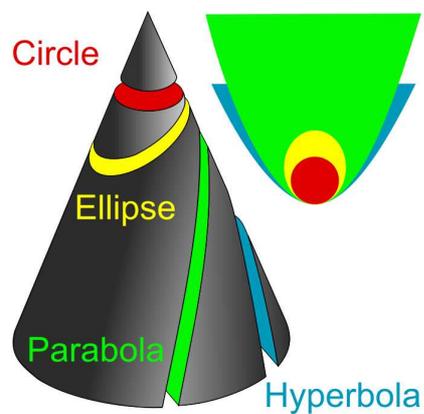
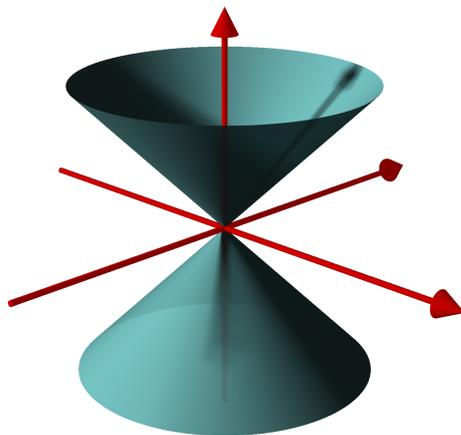
7. VORLESUNG

7.1. Kegelschnitte und Quadriken.

Der *Standardkegel* im dreidimensionalen affinen Raum ist gegeben durch die homogene Gleichung

$$Z^2 = X^2 + Y^2$$

Das kann man sich so vorstellen, dass z den Radius eines Kreises vorgibt, der in der zur $x - y$ -Ebene parallelen Ebene durch den Punkt $(0, 0, z)$ liegt. Jeden Schnitt dieses Kegels mit einer affinen Ebenen E nennt man einen *Kegelschnitt*.



Definition 7.1. Ein *Kegelschnitt* C ist der Durchschnitt des Standardkegels $V(Z^2 - X^2 - Y^2)$ mit einer affinen Ebenen $V(aX + bY + cZ + d)$ (nicht alle $a, b, c = 0$), also

$$C = V(Z^2 - X^2 - Y^2) \cap V(aX + bY + cZ + d).$$

Die Theorie der Kegelschnitte ist ein klassisches Thema, über das schon Apollonios von Perge eine Arbeit geschrieben hat. Da die Ebene durch eine Gleichung $aX + bY + cZ + d = 0$ gegeben wird, kann man nach einer Variablen linear auflösen und erhält eine neue Gleichung in zwei Variablen für den Kegelschnitt. Dies ist eine affin-lineare Variablensubstitution, daher hat die neue Gleichung ebenfalls den Grad zwei.

Wir betrachten daher generell *affine Quadriken* in zwei Variablen.

Definition 7.2. Ein Polynom der Form

$$F = \alpha X^2 + \beta XY + \gamma Y^2 + \delta X + \epsilon Y + \eta \text{ mit } \alpha, \beta, \gamma, \delta, \epsilon, \eta \in K,$$

wobei mindestens einer der Koeffizienten α, β, γ ungleich null ist, heißt eine *quadratische Form in zwei Variablen* (über K) oder eine *Quadrik in zwei Variablen*. Das zugehörige Nullstellengebilde

$$V(F) \subseteq \mathbb{A}_K^2$$

nennt man ebenfalls *Quadrik*.

Wir interessieren uns dafür, wie viele verschiedene Typen von Quadriken es gibt. Die Antwort hängt vom Grundkörper ab. Darüber hinaus muss man festlegen, welchen Äquivalenzbegriff man jeweils verwenden möchte. Zu zwei Quadriken

$$F, G \in K[X, Y]$$

sind die folgenden Äquivalenzbegriffe untersuchenswert.

- F und G sind als Polynome *affin äquivalent*, d.h. es gibt eine (bijektive) affin-lineare Variablentransformation

$$\varphi : K[X, Y] \longrightarrow K[X, Y], X \longmapsto rX + sY + t, Y \longmapsto \tilde{r}X + \tilde{s}Y + \tilde{t},$$

derart, dass $G = \varphi(F)$ ist.

- Die Hauptideale (F) und (G) sind *affin äquivalent*, d.h. es gibt eine (bijektive) affin-lineare Variablentransformation φ derart, dass $(G) = \varphi((F))$ ist.

- Die Restklassenringe

$$K[X, Y]/(F) \text{ und } K[X, Y]/(G)$$

sind als K -Algebren isomorph.

- Die Nullstellenmengen $V(F)$ und $V(G)$ sind affin-linear äquivalent (im Sinne von Definition 5.7)

Der erste Äquivalenzbegriff ist stärker als der zweite, und der zweite ist stärker als die beiden letzten. Ein wesentlicher Unterschied zwischen (1) und (2) ist, dass man bei (2) immer mit einer Einheit multiplizieren darf (das ändert auch nicht das Nullstellengebilde). Über einem Körper, der nicht algebraisch abgeschlossen ist, kann die Äquivalenz in (4) sehr schwach sein, da alle F mit leerem Nullstellengebilde im Sinne von (4) äquivalent sind.

Bei $K = \mathbb{R}$ und $K = \mathbb{C}$ interessiert man sich auch dafür, ob topologische Eigenschaften der zugehörigen Nullstellengebilde übereinstimmen. Wir werden hier für zwei Quadriken F und G die verschiedenen Äquivalenzbegriffe parallel betrachten, aber vor allem an (2) interessiert sein.

Lemma 7.3. *Sei K ein Körper der Charakteristik $\neq 2$. Es sei*

$$F = \alpha X^2 + \beta XY + \gamma Y^2 + \delta X + \epsilon Y + \eta$$

eine Quadrik. Dann gibt es eine Variablentransformation der affinen Ebene, so dass das transformierte Polynom in den neuen Variablen die Form

$$G = \gamma Y^2 + H(X) \text{ mit } H(X) = aX^2 + bX + c$$

hat. Über einem algebraisch abgeschlossenen Körper kann man (durch eine Variablentransformation) $\gamma = 1$ erreichen. Wenn man sich für das erzeugte Ideal bzw. das Nullstellengebilde interessiert, so kann man (durch Division) ebenfalls $\gamma = 1$ erreichen.

Beweis. Zunächst reduzieren wir auf den Fall wo $\gamma \neq 0$ ist. Bei $\gamma = 0$ und $\alpha \neq 0$ kann man X und Y vertauschen. Bei $\alpha = \gamma = 0$ muss $\beta \neq 0$ sein. Dann kann man durch $X \mapsto X + Y$, $Y \mapsto Y$ erreichen, dass der Koeffizient von Y^2 nicht null ist. Sei also im Folgenden $\gamma \neq 0$.

Wir schreiben die Gleichung als

$$\gamma Y^2 + (\beta X + \epsilon)Y + \tilde{H}(X),$$

wobei \tilde{H} ein Polynom in X vom Grad ≤ 2 ist. Durch quadratisches Ergänzen kann man das schreiben als

$$\gamma \left(Y + \frac{\beta X + \epsilon}{2\gamma} \right)^2 + \tilde{H}(X) - \frac{(\beta X + \epsilon)^2}{4\gamma}.$$

In den neuen Variablen $Y + (\beta X + \epsilon)/2\gamma$ und X schreibt sich die Gleichung als

$$G = \gamma Y^2 + H(X) \text{ mit } H(X) = aX^2 + bX + c.$$

Bei K algebraisch abgeschlossen besitzt γ eine Quadratwurzel, so dass man durch $Y \mapsto Y/\sqrt{\gamma}$ den Koeffizient zu 1 machen kann. Der andere Zusatz ist klar. \square

7.2. Klassifikation von reellen und komplexen Quadriken.

Beispiel 7.4. Sei $K = \mathbb{R}$. Wir wollen die reellen Quadriken klassifizieren, und zwar hauptsächlich hinsichtlich der affin-linearen Äquivalenz für die erzeugten Hauptideale. D.h. wir dürfen affine Variablentransformationen durchführen und teilen. Aufgrund von Lemma 6.2 kann man annehmen, dass die beschreibende Gleichung die Form

$$Y^2 = aX^2 + bX + c$$

hat. Bei $a = b = 0$ kann man durch eine Transformation $Y \mapsto \sqrt{c}Y$ (bei $c > 0$) bzw. $Y \mapsto \sqrt{-c}Y$ (bei $c < 0$) und anschließende Division durch $\pm c$ erreichen, dass die rechte Seite gleich 1, -1 oder 0 ist.

Bei $a = 0$ und $b \neq 0$ kann man $bX + c$ als neue Variable nehmen, und erhält die Gleichung $Y^2 = X$.

Sei nun $a \neq 0$. Dann kann man durch eine Transformation $X \mapsto X/\sqrt{a}$ bzw. $X \mapsto X/\sqrt{-a}$ erreichen, dass $a = \pm 1$ ist. Durch quadratisches Ergänzen kann man b zu null machen. Bei $c = 0$ kann man auf $Y^2 = \pm X^2$ transformieren. Sei also $c \neq 0$. Dann kann man durch eine simultane Transformation $X \mapsto uX$, $Y \mapsto uY$ ($u = \sqrt{\pm c}$) und anschließende Division erreichen, dass $c = \pm 1$ ist. Wir haben also noch die Möglichkeiten $Y^2 = \pm X^2 \pm 1$ zu betrachten, wobei $Y^2 - X^2 = \pm 1$ zueinander äquivalent sind.

Wir wissen also, dass jede reelle Quadrik auf eine der folgenden neun Formen gebracht werden kann.

- $Y^2 = 0$ Das ist eine *verdoppelte Gerade*.
- $Y^2 = 1$ Das bedeutet $Y = \pm 1$, das sind also *zwei parallele Geraden*.
- $Y^2 = -1$ Das ist *leer*.
- $Y^2 = X$ Das ist eine *Parabel*.
- $Y^2 = X^2$ Das bedeutet $(Y - X)(Y + X) = 0$, es handelt sich also um *zwei sich kreuzende Geraden*.
- $Y^2 = -X^2$ Die einzige Lösung ist der *Punkt* $(0, 0)$.
- $Y^2 = X^2 + 1$ Das bedeutet $(Y - X)(Y + X) = 1$, das ist also eine *Hyperbel*.
- $Y^2 = -X^2 + 1$ Das ist ein *Einheitskreis*.
- $Y^2 = -X^2 - 1$ Das ist wieder *leer*.

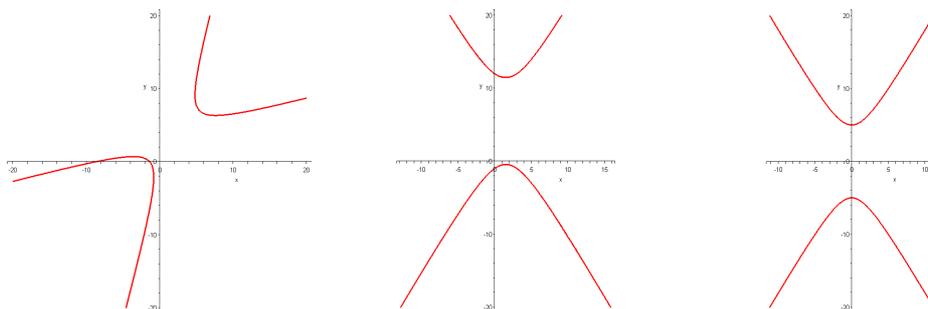
Sind diese neun Typen alle untereinander verschieden? Das hängt davon ab, welchen Äquivalenz-Begriff man zugrunde legt. Die Typen III und IX sind beide leer, haben also identisches Nullstellengebilde. Andererseits sind die

zugehörigen Restklassenringe

$$\mathbb{R}[X, Y]/(Y^2 + 1) \text{ und } \mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$$

nicht isomorph, und über den komplexen Zahlen sind die Nullstellengebilde nicht gleich. Deshalb werden sie auch hier als verschieden betrachtet. Ansonsten sind diese Nullstellengebilde meistens schon aus topologischen Gründen verschieden (z.B. ist der Einheitskreis kompakt, die Hyperbel ist nicht kompakt und hat zwei Zusammenhangskomponenten, die Parabel ist nicht kompakt mit einer Zusammenhangskomponenten, etc.). Allerdings ist die verdoppelte Gerade und die Parabel reell-topologisch gleich, und die Hyperbel und die parallelen Geraden ebenfalls. Hier sind aber jeweils die Restklassenringe und im zweiten Fall auch die komplexen Versionen verschieden. Z. B. ist $K[X, Y]/(Y^2)$ nicht reduziert, aber $K[X, Y]/(Y^2 - X) \cong K[Y]$ ist ein Integritätsbereich. Die komplexe Hyperbel ist zusammenhängend, da sie isomorph zu $\mathbb{C}^\times = \mathbb{C} - \{0\}$ ist, also zur punktierten komplexen Geraden $\mathbb{A}_{\mathbb{C}}^1 - \{0\}$.

Die folgenden Bilder zeigen die Drehung und die Verschiebung einer Quadrik.



Beispiel 7.5. Sei $K = \mathbb{C}$. Wir wollen die komplexen Quadriken klassifizieren. Aufgrund von Lemma 6.2 kann man annehmen, dass die beschreibende Gleichung die Form

$$Y^2 = aX^2 + bX + c$$

hat. Bei $a = b = 0$ kann man durch eine Transformation $Y \mapsto \sqrt{c}Y$ und anschließende Division durch $\pm c$ erreichen, dass die rechte Seite 1 oder 0 ist.

Bei $a = 0$ und $b \neq 0$ kann man $bX + c$ als neue Variable nehmen, und erhält die Gleichung $Y^2 = X$.

Sei nun $a \neq 0$. Dann kann man durch die Transformation $X \mapsto X/\sqrt{a}$ erreichen, dass $a = 1$ ist. Durch quadratisches Ergänzen kann man b zu null machen. Schließlich kann man durch simultane Transformation $X \mapsto uX$, $Y \mapsto uY$ und anschließende Division erreichen, dass $c = 1$ ist.

Wir wissen also, dass jede komplexe Quadrik auf eine der folgenden fünf Formen gebracht werden kann:

- $Y^2 = 0$ Das ist eine *verdoppelte Gerade*.

- $Y^2 = 1$ Das bedeutet $Y = \pm 1$, das sind also *zwei parallele komplexe Geraden*.
- $Y^2 = X$ Das ist eine *komplexe Parabel*.
- $Y^2 = X^2$ Das bedeutet $(Y - X)(Y + X) = 0$, es handelt sich also um *zwei komplexe Geraden*, die sich in einem Punkt kreuzen.
- $Y^2 = X^2 + 1$ Das bedeutet $(Y - X)(Y + X) = 1$, das ist also eine *komplexe Hyperbel*.

Typ I und Typ III sind dabei komplex-topologisch betrachtet eine komplexe affine Gerade, also eine reelle Ebene und damit topologisch gleich (von komplexer Ebene zu sprechen ist im Kontext der algebraischen Geometrie gefährlich, es kann \mathbb{C} und \mathbb{C}^2 gemeint sein). Die Restklassenringe sind aber verschieden, weshalb sie hier als verschieden aufgelistet werden. Ansonsten sind alle Typen komplex-topologisch untereinander verschieden. Neben der reellen Ebene gibt es die punktierte komplexe affine Gerade (die Hyperbel, die topologisch eine punktierte reelle Ebene ist), zwei disjunkte Geraden und zwei sich (in einem Punkt) schneidende Geraden.

Die im letzten Beispiel vorgestellte Klassifikation von komplexen Quadriken gilt über jedem algebraisch abgeschlossenen Körper mit Charakteristik $\neq 2$.

7.3. Parametrisierung von Quadriken.

In der elementaren Zahlentheorie lernt man, wie sich alle pythagoreischen Tripel systematisch erfassen lassen. Der Grund dafür ist, dass es eine Parametrisierung für den Einheitskreis mit rationalen Funktion gibt. Wir zeigen jetzt, dass sich jede irreduzible Quadrik rational parametrisieren lässt.

Satz 7.6. (*Parametrisierung von Quadriken*) Sei $C = V(F)$ eine Quadrik in zwei Variablen, also

$$F = \alpha X^2 + \beta XY + \gamma Y^2 + \delta X + \epsilon Y + \eta$$

(mit α, β, γ nicht alle null). Es sei vorausgesetzt, dass es mindestens einen Punkt auf der Quadrik gibt. Dann gibt es Polynome $P_1, P_2, Q \in K[T]$, $Q \neq 0$, derart, dass das Bild der rationalen Abbildung

$$\mathbb{A}_K^1 \supseteq D(Q) \longrightarrow \mathbb{A}_K^2 \quad \text{mit } t \longmapsto \left(\frac{P_1(t)}{Q(t)}, \frac{P_2(t)}{Q(t)} \right)$$

in C liegt. Besitzt C zumindest zwei Punkte, so ist die Abbildung nicht konstant und bis auf endlich viele Ausnahmen injektiv. Ist C zusätzlich irreduzibel, so ist die Abbildung bis auf endlich viele Ausnahmen surjektiv. Insbesondere ist eine irreduzible Quadrik mit mindestens zwei Punkten eine rationale Kurve.

Beweis. Wir können durch eine Variablentransformation erreichen, dass $\alpha \neq 0$, und dann können wir durch α teilen, und annehmen, dass $\alpha = 1$ ist. Wir können durch verschieben annehmen, dass der Nullpunkt $(0, 0)$ auf der Kurve liegt. Dann ist $\eta = 0$. Wenn zwei sich kreuzende Geraden vorliegen, so können wir durch verschieben annehmen, dass der Nullpunkt nicht der Kreuzungspunkt ist (aber auf einer der Geraden liegt).

Die Idee ist, zu einem Punkt $H = (t, 1)$ die Gerade durch 0 und H zu betrachten und den Schnitt dieser Geraden mit C zu betrachten. Dieser Schnitt besteht aus maximal zwei Punkten (es sei denn, der Schnitt ist die volle Gerade), und da 0 einer der Punkte ist, ist der andere Punkt, den es geben muss, eindeutig bestimmt.

Sei also $H = (t, 1)$ gegeben. Die Gerade durch H und durch 0 besteht aus allen Punkten (at, a) , $a \in K$. Die Schnittpunkte mit C erhält man also, wenn man $(x, y) = (at, a)$ in F einsetzt und nach den Lösungen in a sucht. Einsetzen ergibt die Bedingung

$$F(at, a) = (at)^2 + \beta(ata) + \gamma a^2 + \delta at + \epsilon a = a(at^2 + \beta at + \gamma a + \delta t + \epsilon) = 0.$$

Die Lösung $a = 0$ entspricht dem Nullpunkt, die wir schon kennen, die zweite Lösung ist

$$a_2 = \frac{-\delta t - \epsilon}{t^2 + \beta t + \gamma}.$$

Dieser Ausdruck ist wohldefiniert, wenn $Q(t) = t^2 + \beta t + \gamma \neq 0$ ist (was maximal zwei Werte für t ausschließt).

Zu a_2 gehört auf C der Punkt

$$a_2(t, 1) = (a_2 t, a_2) = \left(t \frac{-\delta t - \epsilon}{t^2 + \beta t + \gamma}, \frac{-\delta t - \epsilon}{t^2 + \beta t + \gamma} \right),$$

so dass

$$P_1 = -t(\delta t + \epsilon) \text{ und } P_2 = -\delta t - \epsilon$$

zu setzen ist.

Dies Abbildung ist auf der durch $D(Q)$ gegebenen Zariski-offenen Menge wohldefiniert (und diese Menge ist nicht leer, sobald der Körper mindestens drei Elemente besitzt).

Von nun an sei vorausgesetzt, dass C mindestens zwei Punkte besitzt. Bei $\delta = \epsilon = 0$ hat F die Gestalt $F = X^2 + \beta XY + \gamma Y^2$. Da wir vorausgesetzt haben, dass es mindestens zwei Punkte auf C gibt, folgt, dass F das Produkt von zwei homogenen Linearformen ist. Wenn F das Quadrat einer Linearform ist, so liegt geometrisch einfach eine „verdoppelte Gerade“ vor, die sich direkt (bijektiv) parametrisieren lässt. Andernfalls ist F das Produkt von zwei verschiedenen homogenen Linearformen und die zugehörigen Geraden verlaufen beide durch den Nullpunkt, was wir ausgeschlossen haben. In diesem Fall kann also nicht sowohl δ als auch $\epsilon = 0$ sein.

Wir haben also nur noch die Situation zu betrachten, wo $\delta t + \epsilon$ nicht das Nullpolynom ist. Daraus folgt, dass die Abbildung auf ihrem Definitionsbereich bis auf endlich viele Ausnahmen injektiv ist, da sich bei $\delta t + \epsilon \neq 0$ wegen

$$t = \frac{P_1}{Q} \cdot \frac{Q}{P_2}$$

aus dem Bild das Urbild t rekonstruieren lässt.

Um zu zeigen, dass die Abbildung surjektiv bis auf endlich viele Ausnahmen ist, brauchen wir die Voraussetzung, dass C irreduzibel ist. Dies bedeutet insbesondere, dass C nicht die Vereinigung von zwei Geraden ist. Sei $P \in C$, und die y -Koordinate von P sei nicht null (es gibt maximal zwei Punkte mit y -Koordinate null). Dann hat die Gerade durch P und 0 einen Schnittpunkt $H = (t, 1)$ mit der Parametrisierungsgeraden $V(Y - 1)$. Bis auf endlich viele Werte von t ist die Abbildung in diesem Punkt H definiert und P ist dann der Bildpunkt der Abbildung. Wegen der Irreduzibilität liegen auf den Ausnahmegeraden nur endlich viele Punkte von C , daher werden fast alle Punkte erreicht. \square

Die (singularitätenfreien) Kegelschnitte sind auch die Bewegungsbahnen von Himmelskörpern. Die möglichen Himmelsbahnen wurden erstmals von Johannes Kepler beschrieben. Das zugrunde liegende Gesetz ist, dass die Beschleunigung zu jedem Zeitpunkt proportional zur Gravitationskraft zwischen dem zentralen Massenpunkt (dem Stern, der Sonne) und dem bewegten Massenpunkt (dem Planeten, dem Kometen) ist. Die Anziehungskraft selbst hängt von den beiden Massen und dem Quadrat ihrer Entfernung ab. Es gibt „gebundene“ (Ellipsen) und „ungebundene“ Bahnen (Parabel, Hyperbel).

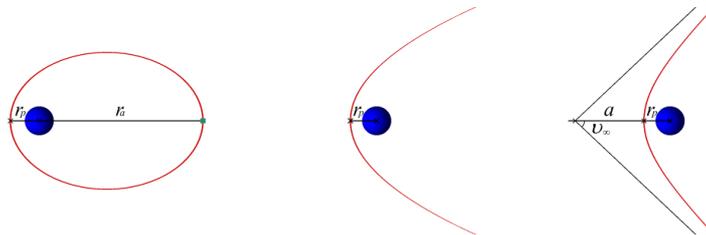


Johannes Kepler
(1571-1630)

Kreis und Ellipse können durch eine lineare Variablentransformation ineinander überführt werden. Man beachte, dass die rationalen Parametrisierungen nicht die „physikalischen Parametrisierungen“ sind. Letztere beschreiben wirklich den Bewegungsablauf, d.h. der Parameter ist dort die Zeit und die Ableitung an einem Zeitpunkt ist die Momentangeschwindigkeit. Die rationalen Parametrisierungen beschreiben „nur“ die Bahn. Der Kreis wird bekanntlich durch

$$(x, y) = (\cos t, \sin t)$$

gleichmäßig (mit konstantem Geschwindigkeitsbetrag) durchlaufen.



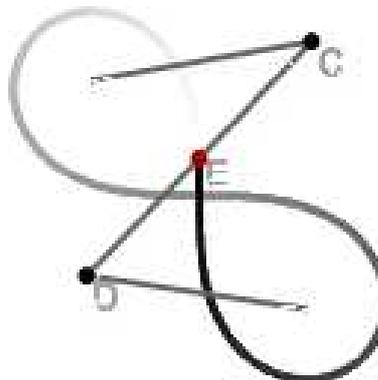
Bemerkung 7.7. Die Parametrisierung einer Quadrik hängt nicht vom Grundkörper ab, denn die Terme, die die Abbildung definieren, sind immer dieselben. Allerdings kann über einem endlichen Körper der Definitionsbereich einer rationalen Abbildung leer sein. Wenn man aber zu einem größeren endlichen Körper \mathbb{F}_q übergeht, so hat die Abbildung stets einen nichtleeren Definitionsbereich.

Geometrisch gesprochen rühren die Definitionslücken der Parametrisierung daher, dass die konstruierten Geraden außer dem Nullpunkt keinen weiteren Schnittpunkt mit der Quadrik besitzen, oder aber die volle Gerade auf der Quadrik liegt (was nur im reduziblen Fall oder bei einer verdoppelten Geraden sein kann). Die Ausnahmemenge der Punkte der Quadrik, die nicht im Bild der Abbildung liegen, sind die Punkte auf der x -Achse (insbesondere der Nullpunkt), und, im reduziblen Fall, die Punkte auf der Geraden, die ganz auf der Quadrik liegt und durch den Nullpunkt geht.

8. VORLESUNG

8.1. Mechanisch definierte algebraische Kurven.

Es sei S eine feste Stange (man denke an ein mechanisches Maschinenteil) mit zwei fixierten Punkten $P_1, P_2 \in S$ (man denke an Gelenke). Diese Stange kann sich in der Ebene (dem \mathbb{R}^2) bewegen, wobei die beiden Punkte sich jeweils in zwei bestimmten Bahnen B_1 und B_2 (man denke an Schienen) befinden müssen. Die Bahnen können dabei recht einfach gegeben sein, etwa durch Geraden oder durch Kreise. Bei einer Dampfmaschine hat man ein drehbares Rad und eine gerade Schiene, die durch eine Stange gekoppelt sind. Wie beschreibt man den zugehörigen Bewegungsprozess?



Was sind die erlaubten *Konfigurationen des Systems*? Wenn man einen Punkt P der Stange fixiert, wie sieht die *Bewegungsbahn (Trajektorie)* dieses Punktes aus?

Für die Extremfälle $P = P_1$ und $P = P_2$ sind die Bewegungsbahnen Teilmengen (in der Regel echte!) von B_1 und B_2 . Für Punkte dazwischen erwartet man eine *stetige Deformation* der einen Bahn in die andere.

Situation 8.1. (Mechanisches Stangensystem) Seien B_1 und B_2 zwei ebene algebraische Kurven, die durch die Gleichungen $F_1 = 0$ und $F_2 = 0$ beschrieben werden, $F_1, F_2 \in K[X, Y]$. Sei S eine „bewegliche Gerade“ (eine Stange) mit zwei Punkten $P_1, P_2 \in S$, $P_1 \neq P_2$, die voneinander den Abstand d haben. Das *mechanische System*, das durch alle Lagen von S in der Ebene gegeben ist, bei denen gleichzeitig $P_1 \in B_1$ und $P_2 \in B_2$ ist, wird folgendermaßen beschrieben.

Eine Lage der Stange in der Ebene ist eindeutig bestimmt, wenn für die beiden Punkte die Lage festgelegt ist (dies berücksichtigt noch nicht die Abstandsbedingung), also durch vier Variablen $(P_1, P_2) = (x_1, y_1, x_2, y_2)$. Eine *erlaubte Konfiguration* muss dann die folgenden drei algebraischen Bedingungen erfüllen.

- (1) $F_1(x_1, y_1) = 0$
- (2) $F_2(x_2, y_2) = 0$
- (3) $(y_2 - y_1)^2 + (x_2 - x_1)^2 = d^2$ (Abstandsbedingung)

Es handelt sich also um drei algebraische Gleichungen in vier Variablen, als Lösungsmenge erwartet man also eine Kurve im \mathbb{A}_K^4 . Ein Punkt $P \in S$ wird durch den Abstand zu P_1 bzw. P_2 beschrieben. Da sich diese Punkte im mechanischen System bewegen, setzen wir die Koordinaten für den *mitbewegten Punkt* P an als

$$P = P_1 + u(P_2 - P_1)$$

(der Abstand von P zu P_1 ist also $\|u(P_2 - P_1)\| = |ud|$) und schreiben seine Koordinaten als

$$(x, y) = (x_1, y_1) + u(x_2 - x_1, y_2 - y_1) = (ux_2 + (1 - u)x_1, uy_2 + (1 - u)y_1).$$

Man kann dann das gesamte mechanische System (durch eine lineare Transformation) in den vier Variablen x_1, y_1, x, y ausdrücken, indem man (bei $u \neq 0$)

$$x_2 = \frac{x - (1 - u)x_1}{u} \quad \text{und} \quad y_2 = \frac{y - (1 - u)y_1}{u}$$

in den Gleichungen ersetzt. In den neuen Variablen erhält man die drei Gleichungen

- (1) $F_1(x_1, y_1) = 0$
- (2) $F_2\left(\frac{x - (1 - u)x_1}{u}, \frac{y - (1 - u)y_1}{u}\right) = 0$
- (3) $(y - y_1)^2 + (x - x_1)^2 = u^2 d^2$

Die zu P gehörende Trajektorie kann man grundsätzlich dadurch erhalten, dass man aus diesem Gleichungssystem die Variablen x_1 und x_2 „eliminiert“, was eine algebraische Gleichung für x und y ergibt. Dies ist allerdings leichter

gesagt als getan, häufig ist es sinnvoller, durch geschickte Manipulationen das Gleichungssystem zu vereinfachen.

Bemerkung 8.2. Manchmal interessiert man sich auch für die Situation, wo sich mit der Stange eine ganze Ebene mitbewegt, und für die Trajektorien von solchen Punkten. Dies ist etwa der Fall, wenn auf der Stange weitere Maschinenteile montiert sind. In diesem Fall kann man jeden Punkt der Ebene bzgl. P_1 und P_2 ansetzen als

$$(x, y) = (x_1, x_2) + u(x_2 - x_1, y_2 - y_1) + v(x_2 - x_1, -y_1 + y_2).$$

Es wird also der Punkt P_1 als Ursprung der bewegten Ebene, die Verbindungsgerade zu P_2 als erste Koordinatenachse und die dazu senkrechte Achse als zweite Koordinatenachse genommen.

Das gesamte mechanische (Stangen-)System wird also durch vier Variablen mit drei Gleichungen beschrieben. Die sichtbare Wirkungsweise, nämlich der Bewegungsablauf eines fixierten Punktes P auf S , liefert aber eine Trajektorie in der affinen Ebene.

Wir betrachten einige Beispiele.

8.2. Zwei Geraden als Bahnen.

Beispiel 8.3. (Zwei Geraden) Seien L_1 und L_2 zwei Geraden in der reellen Ebene \mathbb{R}^2 und sei S eine bewegliche Gerade (eine Stange) mit zwei Punkten P_1, P_2 , die voneinander den Abstand d haben. Erlaubte Konfigurationen des Systems sind diejenigen Lagen von S , für die gleichzeitig $P_1 \in L_1$ und $P_2 \in L_2$ gelten. Die Geraden seien durch $L_1 = \{(x, y) \mid a_1x + b_1y = c_1\}$ und $L_2 = \{(x, y) \mid a_2x + b_2y = c_2\}$ festgelegt.

Die erlaubten Konfigurationen werden dann gemäß der Situationsbeschreibung durch die drei Bedingungen festgelegt:

- (1) $a_1x_1 + b_1y_1 = c_1$
- (2) $a_2x_2 + b_2y_2 = c_2$
- (3) $(x_2 - x_1)^2 + (y_2 - y_1)^2 = d^2$.

Die Lösungsmenge der beiden linearen Gleichungen sind (einzeln betrachtet) dreidimensionale Unterräume. Die Lösungsmenge der ersten Gleichung kann man auffassen als das Produkt eines Kreises (in den Variablen $x_2 - x_1$ und $y_2 - y_1$) mit einer affinen Ebene. Das ist eine Art von Zylinder, wobei allerdings die Fasern zweidimensional sind. Wie kann man die gemeinsame Nullstellenmenge beschreiben, und wie sieht die Trajektorie des mechanischen Systems aus, die ein Punkt $P \in S$ erzeugt?

Durch eine Variablentransformation kann man annehmen, dass die erste Gerade die x -Achse ist, also durch die Gleichung $y = 0$ definiert ist, und die andere durch $ax + by = c$. Das liefert für das System die Bedingung $y_1 = 0$, und das bedeutet, dass man die Variable y_1 eliminieren kann. Man gelangt

dann zu einem System mit den drei Variablen x_1, x_2, y_2 und den zwei Bedingungen

$$\begin{aligned} (1) \quad & (x_2 - x_1)^2 + y_2^2 = d^2 \\ (2) \quad & ax_2 + by_2 = c. \end{aligned}$$

Parallele Geraden



Wenn die zweite Gerade parallel zur ersten ist, so ist $a = 0$ und man kann die zweite Gleichung nach y_2 auflösen und erhält $y_2 = \frac{c}{b} = e$ ($b \neq 0$, sonst liegt keine Gerade vor). Die Zahl e ist der Abstand der parallelen Geraden. Man kann nun auch y_2 eliminieren, und übrig bleibt die einzige Gleichung $(x_2 - x_1)^2 + e^2 = d^2$, also

$$(x_2 - x_1)^2 = d^2 - e^2 = (d - e)(d + e).$$

Bei $e > d$ gibt es hierfür keine Lösung (der konstante Abstand der parallelen Geraden ist größer als der Koppelungsabstand auf der Stange).

Bei $e = d$ ergibt sich die Bedingung $x_1 = x_2$. Dies entspricht der Situation, wo der Parallelabstand der Geraden genau gleich dem Koppelungsabstand ist. Dann sind die einzigen erlaubten Konfigurationen diejenigen, wo die Stange senkrecht zu den beiden Geraden ist. Die Lösungsmenge ist also eine Gerade. Für jeden Punkt auf der Stange ist die Trajektorie einfach eine weitere parallele Gerade.

Sei nun $e < d$. Dann ist

$$x_2 - x_1 = \pm \sqrt{(d - e)(d + e)}.$$

Die Lösungsmenge besteht aus zwei disjunkten Geraden. Dies entspricht den beiden unterschiedlichen Einhängungen, die nicht ineinander überführt werden können. Das mechanische System besteht also aus zwei Zusammenhangskomponenten. Für einen Punkt auf der Stange ergibt sich aber bei beiden Einhängungen die gleiche Trajektorie, nämlich eine parallele Gerade, die in gewissem Sinne doppelt durchlaufen wird. Hier besteht also die Lösungsmenge des vollen mechanischen Systems aus zwei (parallelen) affinen Geraden im vierdimensionalen affinen Raum, deren Trajektorien zu einem fixierten Punkt aber nur eine Gerade ist.

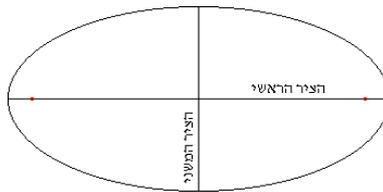
Nicht parallele Geraden

Wir betrachten nun den Fall, wo die beiden Geraden nicht parallel sind. Dann treffen sie sich und die Lösungsmenge kann nicht leer sein. Wir können durch eine weitere lineare Transformation annehmen, dass der Schnittpunkt gleich dem Nullpunkt $(0, 0)$ ist. Die zweite Gleichung wird dann durch $x_2 = ey_2$ beschrieben. Damit kann man x_2 eliminieren und erhält in den beiden

Variablen x_1, y_2 die einzige Gleichung

$$(ey_2 - x_1)^2 + y_2^2 = d^2 .$$

Der Konfigurationsraum des mechanischen Systems spielt sich also in einer (durch $y_1 = 0$ und $x_2 = ey_2$ definierten) Ebene ab und wird durch eine Quadrik beschrieben. Betrachtet man $ey_2 - x_1$ als eine neue Variable, so sieht man, dass es sich um eine Ellipse (in den Koordinaten x_1, y_2 ; in den Koordinaten $ey_2 - x_1, y_2$ ist es ein Kreis) handelt.



Wie sehen die Trajektorien aus? Sei P derjenige Punkt auf der Stange, der durch $P_1 + u(P_2 - P_1)$ gegeben ist. Nach der Situationsbeschreibung hat der Punkt P die Koordinaten

$$((1 - u)x_1 + uey_2, uy_2),$$

wobei $(ey_2 - x_1)^2 + y_2^2 = d^2$ sein muss. In den Extremfällen $u = 0$ und $u = 1$ ergeben sich $(x_1, 0)$ (x_1 beliebig) bzw. (sey_2, sy_2) (s beliebig) als Lösungsmenge. Hierbei muss nach wie vor $(ey_2 - x_1)^2 + y_2^2 = d^2$ erfüllt sein, d.h. es muss zu gegebenem x_1 (bzw. y_2) eine Lösung der Gleichung in der anderen Variablen geben. Die gibt es, wenn x_1 (bzw. y_2) hinreichend klein ist. Insgesamt ergeben sich also gewisse Strecken auf den Ausgangsgeraden. Die Punkte P_1 und P_2 müssen ja auf ihren Bahnen bleiben, und können sich von der anderen Geraden nicht beliebig weit entfernen.

Sei also $u \neq 0, 1$. Aus dem Ansatz

$$(x, y) = ((1 - u)x_1 + uey_2, uy_2)$$

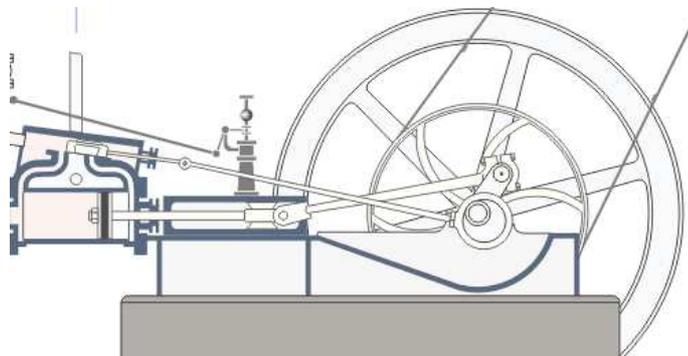
folgt $y_2 = \frac{y}{u}$ und $x_1 = x - \frac{uey_2}{1-u} = x - \frac{ey}{1-u}$ (das Urbild ist also eindeutig festgelegt). Die Gleichung wird dann zu

$$\left(\frac{ey}{u} - x + \frac{ey}{1-u}\right)^2 + \frac{y^2}{u^2} = d^2 ,$$

was wieder die Gleichung einer Ellipse ist.

8.3. Gerade und Kreis als Bahnen.

Wir betrachten nun den Fall, wo die eine Bahn eine Gerade und die zweite Bahn ein Kreis ist. Dies ist die Situation bei einer Dampfmaschine (insbesondere, wenn die Gerade durch den Kreismittelpunkt verläuft).



Wir können ohne Einschränkung annehmen, dass die Gerade durch $y = 0$ gegeben ist. Die Koordinaten des Punktes auf der Geraden sind dann

$$P_1 = (x_1, y_1) = (x_1, 0).$$

Für den Kreis kann man annehmen, dass er den Mittelpunkt $(0, b)$ und den Radius r besitzt. Der Kreisbahnpunkt $P_2 = (x_2, y_2)$ erfüllt dann die Bedingung $x_2^2 + (y_2 - b)^2 = r^2$. Das gesamte mechanische System wird also durch die zwei Bedingungen

$$\begin{aligned} (1) \quad & x_2^2 + (y_2 - b)^2 = r^2 \\ (2) \quad & (x_2 - x_1)^2 + y_2^2 = d^2 \end{aligned}$$

beschrieben, wobei d wieder der Koppelungsabstand sei. Betrachtet man diese zwei Gleichungen in den Koordinaten x_2, y_2 und $x_2 - x_1$, so sieht man, dass es sich um den Schnitt von zwei Zylindern handelt wie in Beispiel 4.6. Die erlaubten Stangenkonfigurationen des mechanischen Systems lassen sich also in drei geeigneten Koordinaten als der Durchschnitt von zwei Zylindern deuten. Dabei müssen allerdings weder die Radien übereinstimmen noch müssen die Innenachsen der Zylinder sich treffen. Ein solcher Durchschnitt und die zugehörigen Trajektorien können schon relativ kompliziert sein.

In den folgenden Beispielen brauchen wir ein Lemma, das eine einfache *Eliminationssituation* beschreibt.

Lemma 8.4. *Sei R ein Integritätsbereich und seien*

$$F_1 = a_1X^2 + b_1X + c_1 \text{ und } F_2 = a_2X^2 + b_2X + c_2$$

zwei quadratische Polynome in einer Variablen über R mit $a_1 \neq 0$ und (a_1, b_1) und (a_2, b_2) linear unabhängig. Dann gehört zum Ideal $(F_1, F_2) \cap R$ das Element

$$(a_2c_1 - a_1c_2)^2 - b_1(-a_2c_1b_2 - c_2a_2b_1 + a_1b_2c_2) + c_1(a_1b_2^2 - 2a_2b_1b_2).$$

Beweis. Wir haben zunächst

$$a_2F_1 - a_1F_2 = (a_2b_1 - a_1b_2)X + a_2c_1 - a_1c_2.$$

Daraus ergibt sich der Ausdruck (dieses Argument ist nicht ganz richtig, es lässt sich aber auch rigoroser durchführen)

$$X = -\frac{a_2c_1 - a_1c_2}{a_2b_1 - a_1b_2}.$$

Wie setzen das in F_1 ein und multiplizieren mit dem Quadrat des Nenners und erhalten

$$a_1(a_2c_1 - a_1c_2)^2 - b_1(a_2c_1 - a_1c_2)(a_2b_1 - a_1b_2) + c_1(a_2b_1 - a_1b_2)^2.$$

Hier kommt im zweiten Summand $-b_1a_2c_1a_2b_1$ und im dritten Summand $c_1a_2^2b_1^2$ vor; diese beiden Summanden heben sich weg, in allen übrigen Monomen kommt a_1 vor. Wir können also a_1 wegekürzen und übrig bleibt

$$(a_2c_1 - a_1c_2)^2 - b_1(-a_2c_1b_2 - c_2a_2b_1 + a_1b_2c_2) + c_1(a_1b_2^2 - 2a_2b_1b_2).$$

□

Beispiel 8.5. (Kreis und Tangente) Wir betrachten das mechanische Koppelungssystem, das durch den Einheitskreis und die dazu tangentielle Gerade durch $(0, 1)$ mit dem Koppelungsabstand $d = 2$ definiert ist, also durch den Geradenbahnpunkt und Kreisbahnpunkt

$$P_1 = (x_1, 1) \text{ und } P_2 = (x_2, y_2)$$

mit den beiden Bedingungen

$$\begin{aligned} (1) \quad & x_2^2 + y_2^2 = 1 \\ (2) \quad & (x_2 - x_1)^2 + (y_2 - 1)^2 = 4. \end{aligned}$$

Es handelt sich also um den Schnitt von zwei Zylindern, allerdings mit unterschiedlichen Radien und auch mit Innenachsen, die sich nicht treffen. Interessant sind die beiden Geraden

$$G_1 = V(x_2, y_2 + 1)$$

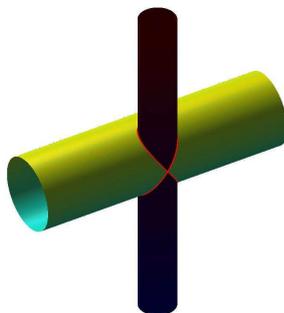
und

$$G_2 = V(x_2 - x_1, y_2 + 1),$$

die sich im Punkt

$$P = (0, 0, -1)$$

schneiden. Die Gerade G_1 liegt auf dem einen Zylinder und schneidet den anderen Zylinder tangential, und umgekehrt. Das geometrische Bild ist, dass der kleinere Zylinder aus dem größeren eine „gebogene Acht“ herausstanzt, wobei P der Kreuzungspunkt der Acht ist.



Die erlaubten Stangenkonfigurationen lassen sich folgendermaßen gewinnen. Zu jedem Kreispunkt gibt es zwei Möglichkeiten, wie die Stange liegen kann, mit der Ausnahme des Kreisbahnpunktes $(0, -1)$, wo der Geradenbahnpunkt $(0, 1)$ sein muss.

Wir starten mit der Situation, wo der Punkt $(0, 1)$ der Kreisbahnpunkt ist, und wo $(-2, 1)$ der Geradenbahnpunkt ist (die Stange liegt also links auf der Geraden), und lassen den Kreisbahnpunkt im Uhrzeigersinn um den Kreis wandern. Der Kreisbahnpunkt zieht dann den Geradenbahnpunkt hinter sich her, bis er unten bei $(0, -1)$ angekommen ist. Die Stange ist dann der vertikale Durchmesser des Kreises (der Geradenbahnpunkt ist dann in $(0, 1)$ und der Kreisbahnpunkt ganz unten). Ab dann wandert der Kreisbahnpunkt auf dem linken Kreisbogen nach oben und schiebt dabei die Stange weiter nach rechts, bis der Geradenbahnpunkt bei $(2, 1)$ ankommt.

Die andere Möglichkeit, wo der Punkt $(0, 1)$ der Kreisbahnpunkt ist, ist die, wo die Stange rechts auf der Geraden liegt (mit $(2, 1)$ als Geradenbahnpunkt). Der Kreisbahnpunkt bewegt sich erneut im Uhrzeigersinn. Dabei schiebt er den Geradenbahnpunkt zuerst nach rechts bis zu einem gewissen Extremum, bei dem die Stange senkrecht zum Kreis im Kreisbahnpunkt steht. Von da an zieht der Kreisbahnpunkt den Geradenbahnpunkt zurück nach links, wobei sich die Stange aufrichtet, bis sie den vertikalen Durchmesser des Kreises einnimmt. Weiter wandert der Kreisbahnpunkt auf dem linken Kreisbogen wieder nach oben, wobei er den Geradenbahnpunkt bis zum Extremum nach links schiebt, und im letzten Stück wieder nach $(-2, 1)$ zieht.

Insbesondere wird der vertikale Durchmesser des Kreises zweimal von der Stange eingenommen, diese Stangenkonfiguration entspricht also dem Kreuzungspunkt der Acht.

Wir wollen nun die Trajektorie zum Mittelpunkt der Stange berechnen, also zu

$$\begin{aligned} P &= P_1 + \frac{1}{2}(P_2 - P_1) = (x_1, 1) + \frac{1}{2}(x_2 - x_1, y_2 - 1) \\ &= \left(\frac{1}{2}x_1 + \frac{1}{2}x_2, \frac{1}{2}y_2 + \frac{1}{2}\right) =: (x, y). \end{aligned}$$

Wir interessieren uns für eine Gleichung für x und y , und führen die Variable $z = \frac{1}{2}x_1 - \frac{1}{2}x_2$ ein. Dann ist

$$x_1 = x + z, \quad x_2 = x - z \quad \text{und} \quad y_2 = 2y - 1$$

und das Gleichungssystem schreibt sich in den neuen Variablen als

$$(x - z)^2 + (2y - 1)^2 = 1 \quad \text{und} \quad (-2z)^2 + (2y - 2)^2 = 4,$$

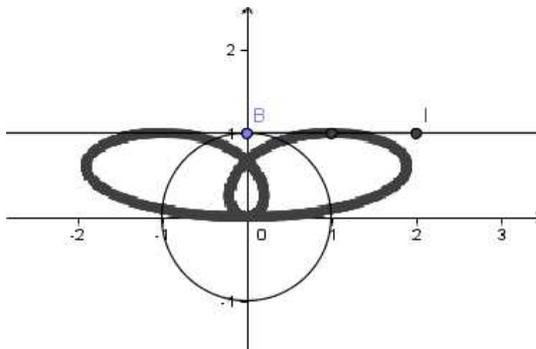
wobei man letzteres als $z^2 + (y - 1)^2 = 1$ schreiben kann bzw. als $z^2 + y^2 - 2y = 0$. Die erste Gleichung ergibt ausgerechnet

$$z^2 - 2zx + x^2 + 4y^2 - 4y = 0.$$

Damit ergibt sich nach Lemma 8.4 (mit $a_1 = a_2 = 1$ und $b_1 = 0$) die Gleichung

$$\begin{aligned} (c_1 - c_2)^2 + c_1 b_2^2 &= (y^2 - 2y - x^2 - 4y^2 + 4y)^2 + (y^2 - 2y)(2x)^2 \\ &= (-3y^2 + 2y - x^2)^2 + (y^2 - 2y)(2x)^2 \\ &= 9y^4 + x^4 + 4y^2 - 12y^3 + 6x^2y^2 - 4x^2y + 4x^2y^2 - 8x^2y \\ &= 9y^4 + 10x^2y^2 + x^4 - 12y^3 - 12x^2y + 4y^2. \end{aligned}$$

Das ist eine Quartik (Kurve vom Grad vier) mit zwei Singularitäten.



Beispiel 8.6. (Kreis und Gerade durch Mittelpunkt) Wir betrachten das mechanische System aus Einheitskreis und x -Achse, wo der Koppelungsabstand $d = 1$ ist. Das mechanische System wird dann durch die zwei Gleichungen

$$\begin{aligned} (1) \quad &x_2^2 + y_2^2 = 1 \\ (2) \quad &(x_2 - x_1)^2 + y_2^2 \end{aligned}$$

beschrieben. Es handelt sich um den Durchschnitt von zwei Zylindern mit gleichem Radius und sich treffenden Innenachsen, d.h. wir können auf die Ergebnisse von Beispiel 4.6 zurückgreifen. Dort wurde gezeigt, dass der Durchschnitt durch zwei Ellipsen gegeben ist, die sich in zwei Punkten schneiden. Diese Beschreibung muss sich auch im Kontext des mechanischen Systems wiederfinden. Welche Stangenkonfigurationen entsprechen der einen Ellipse, welche der anderen, welche Konfigurationen liegen auf beiden?

Machen wir uns also einen Überblick über die erlaubten Konfigurationen. Wenn der Geradenpunkt (also der Punkt auf der Geradenbahn) der Kreismittelpunkt ist, so ist jeder Punkt des Kreises als Kreisbahnpunkt erlaubt. Die radialen Strahlen des Kreises bilden also eine Schar von erlaubten Stangenkonfigurationen, und diese bilden zusammen die eine Ellipse. Die andere Ellipse entspricht der Menge der Stangenkonfigurationen, bei denen der Geradenbahnpunkt von -2 nach $+2$ läuft und dabei den Kreisbahnpunkt im oberen oder unteren Kreisbogen vor sich herschiebt bzw. hinterherzieht. Es gibt zwei Stangenkonfigurationen, die zu beiden Familien gehören, nämlich die mit dem Kreismittelpunkt als Geradenbahnpunkt und $(0, 1)$ bzw. $(0, -1)$ als Kreisbahnpunkt. In einer solchen Stangenkonfiguration kann das mechanische System nicht nur vorwärts und rückwärts laufen, sondern wesentlich die Richtung wechseln.

Wie sehen die Trajektorien eines Punktes auf der bewegten Stange aus? Die Gesamttrajektorie ist die Vereinigung der beiden Trajektorien, die zu den beiden irreduziblen Komponenten des Systems gehören. Wie viele Selbstdurchdringungspunkte gibt es?

Für einen Punkt $P = P_1 + u(P_2 - P_1)$ der Koppelungsstange sind die Koordinaten gleich

$$(z_1, z_2) = (x_1 + u(x_2 - x_1), uy_2).$$

Bei $u = 0$ ist die Trajektorie das reelle Intervall $[-2, 2]$, und bei $u = 1$ ist es der Einheitskreis. Sei also nun $u \neq 0, 1$. Die Projektion der radialen Komponenten des Systems ist einfach der Kreis mit Radius u . Die Projektion der anderen Ellipse ist wieder eine Ellipse, die den Kreis in unterschiedlicher Weise schneiden kann. Siehe auch Aufgabe 8.2.

9. VORLESUNG

9.1. Noethersche Ringe.

Unser Ziel ist es zu zeigen, dass wenn R ein noetherscher Ring ist, dass dann auch der Polynomring $R[X]$ ein noetherscher Ring ist (Hilbertscher Basissatz). Dies gilt dann auch für die Hinzunahme von mehreren (endlich vielen) Variablen und insbesondere für Polynomringe in endlich vielen Variablen über einem Körper. Wir erinnern an den Begriff des noetherschen Ringes.

Definition 9.1. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.



Emmy Noether (1882-1935)

Proposition 9.2. Für einen kommutativen Ring R sind folgende Aussagen äquivalent.

- (1) R ist noethersch.
- (2) Jede aufsteigende Idealkette

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

wird stationär, d.h. es gibt ein n mit $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$

Beweis. (1) \Rightarrow (2). Sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

eine aufsteigende Idealkette in R . Wir betrachten die Vereinigung $\mathfrak{a} = \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$, die wieder ein Ideal in R ist. Da R noethersch ist, ist \mathfrak{a} endlich erzeugt, d.h. $\mathfrak{a} = (f_1, \dots, f_k)$. Da diese f_i in der Vereinigung der Ideale \mathfrak{a}_n liegen, und da die Ideale aufsteigend sind, muss es ein n geben derart, dass $f_1, \dots, f_k \in \mathfrak{a}_n$ liegt. Wegen

$$(f_1, \dots, f_k) \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+m} \subseteq \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n \subseteq (f_1, \dots, f_k)$$

für $m \geq 0$ muss hier Gleichheit gelten, so dass die Idealkette ab n stationär ist.

(2) \Rightarrow (1). Sei \mathfrak{a} ein Ideal in R . Wir nehmen an, \mathfrak{a} sei nicht endlich erzeugt, und konstruieren sukzessive eine unendliche echt aufsteigende Idealkette $\mathfrak{a}_n \subset \mathfrak{a}$, wobei die \mathfrak{a}_n alle endlich erzeugt sind. Sei dazu

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots \subset \mathfrak{a}_n \subset \mathfrak{a}$$

bereits konstruiert. Da \mathfrak{a}_n endlich erzeugt ist, aber \mathfrak{a} nicht, ist die Inklusion $\mathfrak{a}_n \subseteq \mathfrak{a}$ echt und es gibt ein Element

$$f_{n+1} \in \mathfrak{a}, f_{n+1} \notin \mathfrak{a}_n$$

Dann setzt das Ideal $\mathfrak{a}_{n+1} := \mathfrak{a}_n + (f_{n+1})$ die Idealkette echt aufsteigend fort. \square

Lemma 9.3. (*Restklassenringe noetherscher Ringe*) Sei R ein noetherscher Ring. Dann ist auch jeder Restklassenring R/\mathfrak{b} noethersch.

Beweis. Sei $\mathfrak{a} \subseteq R/\mathfrak{b}$ ein Ideal und sei $\tilde{\mathfrak{a}} \subseteq R$ das Urbildideal davon. Dieses ist endlich erzeugt nach Voraussetzung, also $\tilde{\mathfrak{a}} = (f_1, \dots, f_n)$. Die Restklassen dieser Erzeuger, also $\bar{f}_1, \dots, \bar{f}_n$, bilden ein Idealerzeugendensystem von \mathfrak{a} : Für ein Element $\bar{g} \in \mathfrak{a}$ gilt ja $g = \sum_{i=1}^n r_i f_i$ in R und damit $\bar{g} = \sum_{i=1}^n \bar{r}_i \bar{f}_i$ in R/\mathfrak{b} . \square

9.2. Der Hilbertsche Basissatz.

Wie viele grundlegende Aussagen der kommutativen Algebra geht der Hilbertsche Basissatz, dem wir uns jetzt zuwenden, auf David Hilbert zurück, genauer auf seine Arbeit von 1890, „Ueber die Theorie der algebraischen Formen“.



David Hilbert (1862-1943)

Satz 9.4. (*Hilbertscher Basissatz*) Sei R ein noetherscher Ring. Dann ist auch der Polynomring $R[X]$ noethersch.

Beweis. Sei \mathfrak{b} ein Ideal im Polynomring $R[X]$. Zu $n \in \mathbb{N}$ definieren wir ein Ideal \mathfrak{a}_n in R durch

$$\mathfrak{a}_n = \{c \in R : \text{es gibt } F \in \mathfrak{b} \text{ mit } F = cX^n + c_{n-1}X^{n-1} + \dots + c_1X + c_0\}.$$

Das Menge \mathfrak{a}_n besteht also aus allen Leitkoeffizienten von Polynomen vom Grad n aus \mathfrak{b} . Es handelt sich dabei offensichtlich um Ideale in R (wobei wir hier 0 als Leitkoeffizient zulassen). Ferner ist $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, da man ja ein Polynom F vom Grad n mit Leitkoeffizient c mit der Variablen X multiplizieren

kann, um ein Polynom vom Grad $n + 1$ zu erhalten, das wieder c als Leitkoeffizienten besitzt. Da R noethersch ist, muss diese aufsteigende Idealkette stationär werden; sei n so, dass $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$ ist.

Zu jedem $i \leq n$ sei nun $\mathfrak{a}_i = (c_{i1}, \dots, c_{ik_i})$ ein endliches Erzeugendensystem, und es seien

$$F_{ij} = c_{ij}X^i + \text{Terme von kleinerem Grad}$$

zugehörige Polynome aus \mathfrak{b} (die es nach Definition der \mathfrak{a}_i geben muss).

Wir behaupten, dass \mathfrak{b} von allen $\{F_{ij} : 0 \leq i \leq n, 1 \leq j \leq k_i\}$ erzeugt wird. Dazu beweisen wir zu $G \in \mathfrak{b}$ durch Induktion über den Grad von G , dass es als Linearkombination mit diesen F_{ij} darstellbar ist. Für G konstant, also $G \in R$, ist dies klar. Sei nun der Grad von G gleich d und die Aussage sei für kleineren Grad bewiesen. Wir schreiben

$$G = cX^d + c_{d-1}X^{d-1} + \dots + c_1X + c_0.$$

Es ist $c \in \mathfrak{a}_d$ und damit kann man c schreiben als R -Linearkombination der c_{ij} , $0 \leq i \leq n$, $1 \leq j \leq k_i$. Bei $d \leq n$ kann man c sogar schreiben als R -Linearkombination der c_{dj} , $j = 1, \dots, k_d$, sagen wir $c = \sum_{j=1}^{k_d} r_j c_{dj}$. Dann ist $G - \sum_{j=1}^{k_d} r_j F_{dj} \in \mathfrak{b}$ und hat einen kleineren Grad, so dass man darauf die Induktionsvoraussetzung anwenden kann. Bei $d > n$ ist

$$c = \sum_{i=0, \dots, n, j=1, \dots, k_i} r_{ij} c_{ij}.$$

Damit gehört

$$G - \sum_{i=0, \dots, n, j=1, \dots, k_i} r_{ij} X^{d-i} F_{ij}$$

ebenfalls zu \mathfrak{b} und hat einen kleineren Grad, so dass man wieder die Induktionsvoraussetzung anwenden kann. \square

Korollar 9.5. *Sei R ein noetherscher Ring. Dann ist auch $R[X_1, \dots, X_n]$ noethersch.*

Beweis. Dies folgt durch induktive Anwendung des Hilbertschen Basissatzes auf die Kette

$$\begin{aligned} R \subset R[X_1] \subset (R[X_1])[X_2] &= R[X_1, X_2] \subset (R[X_1, X_2])[X_3] \\ &= R[X_1, X_2, X_3] \subset \dots \subset R[X_1, \dots, X_n]. \end{aligned}$$

\square

Korollar 9.6. *Sei K ein Körper. Dann ist $K[X_1, \dots, X_n]$ noethersch.*

Beweis. Dies ist ein Spezialfall von Korollar 9.5. \square

Der Hilbertsche Basissatz bedeutet insbesondere, dass jede abgeschlossene Untervarietät $V \subset \mathbb{A}_K^n$ in einem affinen Raum durch endlich viele Polynome beschrieben werden kann. Jedes algebraische Nullstellengebilde ist also bereits das Nullstellengebilde von endlich vielen Polynomen.

Korollar 9.7. Sei $V \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge. Dann gibt es eine Abbildung

$$\varphi : \mathbb{A}_K^n \rightarrow \mathbb{A}_K^m,$$

die komponentenweise durch Polynome $F_i \in K[X_1, \dots, X_n]$ gegeben ist, also $\varphi = (F_1, \dots, F_m)$, derart, dass V das Urbild des Nullpunktes $0 \in \mathbb{A}_K^m$ ist.

Beweis. Es sei \mathfrak{a} ein beschreibendes Ideal für V , also $V = V(\mathfrak{a})$. Nach dem Hilbertschen Basissatz gibt es $F_1, \dots, F_m \in K[X_1, \dots, X_n]$ mit $\mathfrak{a} = (F_1, \dots, F_m)$. Damit ist insbesondere

$$V = V(\mathfrak{a}) = V(F_1) \cap \dots \cap V(F_m).$$

Diese F_i kann man zu einer Abbildung

$$\varphi = (F_1, \dots, F_m) : \mathbb{A}_K^n \longrightarrow \mathbb{A}_K^m$$

zusammenfassen. Dann ist $\varphi(P) = 0$ genau dann, wenn alle Komponentenfunktionen null sind, und das ist genau dann der Fall, wenn $P \in V(F_i)$ ist für alle i . \square

Definition 9.8. Sei R ein kommutativer Ring. Eine R -Algebra A heißt *von endlichem Typ* (oder *endlich erzeugt*), wenn sie die Form

$$A = R[X_1, \dots, X_n]/\mathfrak{a}$$

besitzt.

Eine endlich erzeugte R -Algebra besitzt also eine Darstellung als Restklassenring einer Polynomialalgebra über R in endlich vielen Variablen. Eine solche Darstellung ist keineswegs eindeutig.

Korollar 9.9. Sei R ein noetherscher Ring. Dann ist jede R -Algebra von endlichem Typ ebenfalls noethersch. Insbesondere ist für einen Körper K jede K -Algebra von endlichem Typ noethersch.

Beweis. Dies folgt aus Korollar 9.5 und aus Lemma 9.3. \square

9.3. Zerlegung in irreduzible Komponenten.

Aus dem Hilbertschen Basissatz folgt, dass eine aufsteigende Idealkette

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$$

in $K[X_1, \dots, X_n]$ stationär werden muss. Dies hat für absteigende Ketten von affin-algebraischen Teilmengen in einem affinen Raum folgende Konsequenz:

Satz 9.10. In einem affinen Raum \mathbb{A}_K^n wird jede absteigende Folge von abgeschlossenen Mengen

$$V_1 \supseteq V_2 \supseteq \dots$$

stationär.

Beweis. Sei

$$V_1 \supseteq V_2 \supseteq \dots$$

eine absteigende Kette von affin-algebraischen Teilmengen im \mathbb{A}_K^n . Daraus folgt nach Lemma 3.6 $\text{Id}(V_i) \subseteq \text{Id}(V_{i+1})$ für die zugehörigen Verschwindungsideale. Nach Korollar 9.6 wird diese Idealkette stationär, sagen wir für $i \geq i_0$. Nach Lemma 3.7 ist $V_i = V(\text{Id}(V_i))$. Daraus folgt dann aber für $i \geq i_0$, dass

$$V_i = V(\text{Id}(V_i)) = V(\text{Id}(V_{i+1})) = V_{i+1},$$

so dass die absteigende Kette stationär werden muss. \square

Es ergibt sich daraus durch Übergang zu den Komplementen, dass jede aufsteigende Kette von Zariski-offenen Mengen in einem affinen Raum stationär wird. Eine solche Topologie nennt man auch *noethersch* (generell nennt man eine (partielle) Ordnung, für die jede aufsteigende Kette stationär wird, noethersch). Für einen noetherschen Raum gilt: jede nicht-leere Teilmenge von offenen Mengen (abgeschlossenen Mengen) besitzt ein maximales (minimales) Element. Dies kann man vorteilhaft als Beweisprinzip einsetzen (*Beweis durch noethersche Induktion*): Man möchte zeigen, dass eine gewisse Eigenschaft E für alle abgeschlossenen Teilmengen gilt, und man betrachtet die Menge derjenigen abgeschlossenen Teilmengen, die E nicht erfüllen. Man möchte zeigen, dass die Menge leer ist, und nimmt an, dass sie nicht leer ist. Dann besitzt sie auch ein minimales Element, und dies muss man dann zum Widerspruch führen. Die Gültigkeit dieses Beweisprinzips beruht darauf, dass man in einer nicht-leeren Menge ohne einem minimalen Element eine unendlich absteigende Kette konstruieren kann. Ein typisches Beispiel für dieses Beweisprinzip liefert der Beweis der folgenden Aussage.

Satz 9.11. *Sei $V \subset \mathbb{A}_K^n$ eine affin-algebraische Menge. Dann gibt es eine eindeutige Zerlegung*

$$V = V_1 \cup \dots \cup V_k$$

mit irreduziblen Mengen V_i mit $V_i \not\subseteq V_j$ für $i \neq j$.

Beweis. Die Existenz beweisen wir durch noethersche Induktion. Angenommen, nicht jede affin-algebraische Menge habe eine solche Zerlegung. Dann gibt es auch eine minimale Teilmenge, sagen wir V , ohne eine solche Zerlegung. V kann nicht irreduzibel sein, sondern es gibt eine nicht-triviale Darstellung $V = V_1 \cup V_2$. Da V_1 und V_2 echte Teilmengen von V sind, gibt es für diese beiden jeweils endliche Darstellungen als Vereinigung von irreduziblen Teilmengen. Diese beiden vereinigen sich zu einer Darstellung von V , was ein Widerspruch ist.

Zur Eindeutigkeit. Sei

$$V = V_1 \cup \dots \cup V_k = W_1 \cup \dots \cup W_m$$

zwei Zerlegungen in irreduzible Teilmengen (jeweils ohne Inklusionsbeziehung). Es ist

$$V_1 = V_1 \cap V = V_1 \cap (W_1 \cup \dots \cup W_m) = (V_1 \cap W_1) \cup \dots \cup (V_1 \cap W_m).$$

Da V_1 irreduzibel ist, muss $V_1 \subseteq W_j$ für ein j sein. Umgekehrt ist mit dem gleichen Argument $W_j \subseteq V_i$ für ein i , woraus $i = 1$ und $V_1 = W_j$ folgt. Ebenso findet sich V_2 etc. in der Zerlegung rechts wieder, so dass die Zerlegung eindeutig ist. \square

9.4. Moduln.

Definition 9.12. Sei R ein kommutativer Ring und $M = (M, +, 0)$ eine kommutative Gruppe. Man nennt M einen R -Modul, wenn es eine Operation

$$R \times M \longrightarrow M, (r, v) \longmapsto rv = r \cdot v,$$

gibt, die folgende Axiome erfüllt (dabei seien $r, s \in R$ und $u, v \in M$ beliebig):

- (1) $r(su) = (rs)u$,
- (2) $r(u + v) = (ru) + (rv)$,
- (3) $(r + s)u = (ru) + (su)$,
- (4) $1u = u$.

Definition 9.13. Sei R ein kommutativer Ring und M ein R -Modul. Eine Teilmenge $U \subseteq M$ heißt *Unterm modul*, wenn sie eine Untergruppe von M ist und wenn für jedes $u \in U$ und $r \in R$ gilt, dass auch $ru \in U$ ist.

Definition 9.14. Sei R ein kommutativer Ring und M ein R -Modul. Eine Teilmenge $v_i \in M, i \in I$, heißt *Erzeugendensystem* für M , wenn es für jedes Element $v \in M$ eine Darstellung

$$v = \sum_{i \in J} r_i v_i$$

gibt, wobei $J \subseteq I$ endlich ist und $r_i \in R$.

Definition 9.15. Sei R ein kommutativer Ring und M ein R -Modul. Der Modul M heißt *endlich erzeugt* oder *endlich*, wenn es ein endliches Erzeugendensystem $v_i, i \in I$, für ihn gibt (also mit einer endlicher Indexmenge).

Ein kommutativer Ring R selbst ist in natürlicher Weise ein R -Modul, wenn man die Ringmultiplikation als Skalarmultiplikation interpretiert. Die Ideale sind dann genau die R -Unterm oduln von R . Die Begriffe Ideal-Erzeugendensystem und Modul-Erzeugendensystem stimmen für Ideale überein.

10. VORLESUNG

10.1. Noethersche Moduln.

Wir wollen zeigen, dass für einen noetherschen Ring R und einen endlich erzeugten R -Modul jeder R -Untermodule wieder endlich erzeugt ist. Solche Moduln nennt man noethersch.

Definition 10.1. Sei R ein kommutativer Ring und M ein R -Modul. Dann heißt M *noethersch*, wenn jeder R -Untermodule von M endlich erzeugt ist.

In den folgenden Aussagen verwenden wir folgende Sprech- bzw. Schreibweise.

Definition 10.2. Sei R ein kommutativer Ring und seien M_1, M, M_3 R -Moduln. Man nennt ein Diagramm der Form

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_3 \longrightarrow 0$$

eine *kurze exakte Sequenz* von R -Moduln, wenn M_1 ein R -Untermodule von M ist, und wenn M_3 ein Restklassenmodule von M ist, der isomorph zu M/M_1 ist.

Lemma 10.3. Sei R ein kommutativer Ring und

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_3 \longrightarrow 0$$

eine *kurze exakte Sequenz* von R -Moduln. Dann ist M genau dann noethersch, wenn sowohl M_1 als auch M_3 noethersch sind.

Beweis. Sei zunächst M noethersch, und $U \subseteq M_1$ ein Untermodule. Dann ist U direkt auch ein Untermodule von M , also nach Voraussetzung endlich erzeugt. Sei nun $V \subseteq M_3$ ein Untermodule des Restklassenmoduls. Das Urbild von V in M unter der Restklassenabbildung sei \tilde{V} . Dieser Modul ist nach Voraussetzung endlich erzeugt, und die Bilder eines solchen Erzeugendensystems erzeugen auch den Bildmodule V .

Seien nun die äußeren Moduln M_1 und M_3 noethersch, und sei $U \subseteq M$ ein Untermodule. Es sei $U_3 \subseteq M_3$ der Bild-Untermodule davon. U_3 wird von endlich vielen Elementen s_1, \dots, s_n erzeugt, und wir können annehmen, dass diese $s_i = \bar{r}_i$ die Bilder von Elementen $r_i \in U$ sind. Betrachte $U \cap M_1$. Dies ist ein Untermodule von M_1 , und daher endlich erzeugt, sagen wir von t_1, \dots, t_k , die wir als Elemente in U auffassen. Wir behaupten, dass

$$r_1, \dots, r_n, t_1, \dots, t_k$$

ein Erzeugendensystem von U bilden. Sei dazu $m \in U$ ein beliebiges Element. Dann ist $\bar{m} = \sum_{i=1}^n a_i \bar{r}_i$ und daher geht das Element $m - \sum_{i=1}^n a_i r_i$ rechts auf null. Dann gehört es aber zum Kern der Restklassenabbildung, also zu

M_1 . Andererseits gehört dieses Element auch zu U , also zum Durchschnitt $M_1 \cap U$, der ja von den t_1, \dots, t_k erzeugt wird. Also kann man schreiben

$$m - \sum_{i=1}^n a_i r_i = \sum_{j=1}^k b_j t_j$$

bzw. $m = \sum_{i=1}^n a_i r_i + \sum_{j=1}^k b_j t_j$. □

Satz 10.4. *Sei R ein noetherscher Ring und M ein endlich erzeugter R -Modul. Dann ist M ein noetherscher Modul.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl n der Modul-Erzeuger von M . Bei $n = 0$ liegt der Nullmodul vor. Sei $n = 1$. Dann gibt es eine surjektive Abbildung $R \rightarrow M \cong R/\mathfrak{a}$ vor. Nach Lemma 10.3 ist aber ein Restklassenmodul eines noetherschen Moduls wieder noethersch, und der Ring selbst ist nach Voraussetzung noethersch, also ist M noethersch.

Sei nun $n \geq 2$ und die Aussage für kleinere n bereits bewiesen. Sei m_1, \dots, m_n ein Erzeugendensystem von M . Wir betrachten den durch m_1, \dots, m_{n-1} erzeugten R -Untermodul, den wir mit M_1 bezeichnen. Dieser Untermodul gibt Anlass zu einer kurzen exakten Sequenz, nämlich

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M/M_1 =: M_3 \longrightarrow 0.$$

Hier wird der linke Modul von $n - 1$ Elementen erzeugt und ist nach Induktionsvoraussetzung noethersch. Der rechte Modul wird von der Restklasse von m_n , also von einem Element erzeugt, also noethersch. Nach Lemma 10.3 ist dann M noethersch. □

10.2. Hilbertscher Nullstellensatz - algebraische Version.

Wir wollen die algebraische Version des Hilbertschen Nullstellensatzes beweisen. Dazu benötigen wir die folgenden zwei Lemmata.

Lemma 10.5. *Sei R ein noetherscher kommutativer Ring und A eine endlich erzeugte R -Algebra. Es sei $B \subseteq A$ eine R -Unteralgebra, über der A endlich (als B -Modul) sei. Dann ist auch B eine endlich erzeugte R -Algebra.*

Beweis. Wir schreiben $A = R[x_1, \dots, x_n]$ und $A = Ba_1 + \dots + Ba_m$ mit $a_i \in A$. Wir setzen

$$x_i = \sum_{j=1}^m b_{ij} a_j \quad \text{und} \quad a_i a_j = \sum_{k=1}^m b_{ijk} a_k$$

mit Koeffizienten $b_{ij}, b_{ijk} \in B$. Wir betrachten die von diesen Koeffizienten erzeugte R -Unteralgebra S von B und den S -Modul $\tilde{A} = Sa_1 + \dots + Sa_m$. Die Produkte $a_i a_j$ gehören wieder zu diesem Modul, daher ist \tilde{A} sogar eine S -Algebra. Weil die x_i ebenfalls zu \tilde{A} gehören, gilt sogar $A = \tilde{A}$. Dies bedeutet, dass A ein endlicher S -Modul ist. Nach Korollar 9.9 zum Hilbertschen Basissatz ist S ein noetherscher Ring und nach Satz 10.4 ist der S -Untermodul

$B \subseteq A$ ebenfalls endlicher S -Modul. Die Kette $R \subseteq S \subseteq B$ zeigt schließlich, dass B eine endlich erzeugte R -Algebra ist. \square

Lemma 10.6. *Sei K ein Körper und $R = K(X)$ der zugehörige rationale Funktionenkörper. Dann ist R keine endlich erzeugte K -Algebra.*

Beweis. Sei angenommen, dass die rationalen Funktionen $F_i = \frac{P_i}{Q_i}$, $i = 1, \dots, n$, ein endliches Erzeugendensystem von $K(X)$ bilden, mit $P_i, Q_i \in K[X]$, $Q_i \neq 0$. Durch Übergang zu einem Hauptnenner kann man annehmen, dass $Q_i = Q$ konstant ist. Die Annahme bedeutet also insbesondere, dass der Körper der rationalen Funktionen sich durch Nenneraufnahme an nur einem Element ergeben würde. Da Q keine Konstante ist (sonst wäre $K[X] = K(X)$, was nicht der Fall ist), ist $Q - 1 \neq 0$ und daher ist $\frac{1}{Q-1} \in K(X)$. Also gibt es eine Darstellung

$$\frac{1}{Q-1} = \frac{P}{Q^s}$$

mit einem geeigneten s . Daraus folgt $Q^s = (Q-1)P$. Da Q^s und $Q-1$ das Einheitsideal erzeugen, folgt daraus, dass bereits $Q-1$ das Einheitsideal erzeugt, also selbst eine Einheit ist. Dann wäre Q aber doch eine Konstante, was es nicht ist. \square

Satz 10.7. *(Hilbertscher Nullstellensatz - algebraische Version) Sei K ein Körper und sei $K \subseteq L$ eine Körpererweiterung, die (als K -Algebra) endlich erzeugt sei. Dann ist L endlich über K .*

Beweis. Wir setzen $L = K[x_1, \dots, x_n]$. Sei K_i der Quotientenkörper von $K[x_1, \dots, x_i]$ (innerhalb von L). Wir haben also eine Körperkette

$$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{n-1} \subseteq K_n = L.$$

Wir wollen zeigen, dass L endlich über K ist, und dazu genügt es zu zeigen, dass jeder Schritt in der Körperkette endlich ist. Sei angenommen, dass $K_i \subseteq K_{i+1}$ nicht endlich ist, aber alle folgenden Schritte endlich sind. Wir wenden Lemma 10.5 auf

$$K \subseteq K_{i+1} \subseteq L$$

an und erhalten, dass K_{i+1} endlich erzeugt über K ist. Dann ist insbesondere K_{i+1} auch endlich erzeugt über K_i . Andererseits ist K_{i+1} der Quotientenkörper von $K_i[x_{i+1}]$. Wir haben also eine Kette

$$K_i \subseteq K_i[x_{i+1}] \subseteq Q(K_i[x_{i+1}]) = K_{i+1},$$

wo K_{i+1} endlich erzeugt über K_i ist, aber nicht endlich. Wäre x_{i+1} algebraisch über K_i , so auch endlich, und dann wäre $K_i[x_{i+1}]$ bereits ein Körper. Dann wäre die letzte Kette insgesamt endlich, im Widerspruch zur Wahl von i . Also ist x_{i+1} transzendent über K_i . Dann ist aber $K_i[x_{i+1}]$ isomorph zu einem Polynomring in einer Variablen und $Q(K_i[x_{i+1}])$ ist isomorph zu einem rationalen Funktionenkörper über K_i . Dieser ist aber nach Lemma 10.6 nicht endlich erzeugt, so dass sich erneut ein Widerspruch ergibt. \square

Satz 10.8. *Sei K ein Körper und seien A und B zwei K -Algebren von endlichem Typ. Es sei $\varphi : A \rightarrow B$ ein K -Algebra-Homomorphismus. Dann ist für jedes maximale Ideal \mathfrak{m} aus B auch das Urbild $\varphi^{-1}(\mathfrak{m})$ ein maximales Ideal.*

Beweis. Sei \mathfrak{m} ein maximales Ideal aus B . Wir wissen, dass unter jedem Ringhomomorphismus das Urbild eines Primideals wieder prim ist, also ist $\varphi^{-1}(\mathfrak{m})$ zunächst ein Primideal, das wir \mathfrak{p} nennen. Wir erhalten induzierte Ringhomomorphismen

$$K \longrightarrow A/\mathfrak{p} \longrightarrow B/\mathfrak{m} = L,$$

wobei L ein Körper ist und wobei beide Homomorphismen injektiv und von endlichem Typ sind. Da die Gesamtabbildung von endlichem Typ ist und K und L Körper sind, folgt nach Satz 10.7, dass diese Abbildung endlich ist. Dann ist erst recht die hintere Abbildung endlich. Wir wollen zeigen, dass A/\mathfrak{p} ein Körper ist. Dies folgt aber aus Aufgabe 10.1. \square

Satz 10.9. *Sei K ein Körper und sei A eine K -Algebra von endlichem Typ. Dann ist jedes Radikal in A der Durchschnitt von maximalen Idealen.*

Beweis. Wir wissen, dass jedes Radikal der Durchschnitt von Primidealen ist. Es genügt also zu zeigen, dass jedes Primideal in einer endlich erzeugten Algebra der Durchschnitt von maximalen Idealen ist. Sei \mathfrak{p} ein Primideal und $f \notin \mathfrak{p}$. Dann ist \mathfrak{p} ein Primideal in der Nenneraufnahme $B := A_f$. Es gibt ein (in A_f) maximales Ideal $\mathfrak{m} \subset A_f$ oberhalb von $\mathfrak{p}A_f$. Wir fassen A_f als endlich erzeugte K -Algebra auf und betrachten $\varphi : A \rightarrow A_f$. Dann ist $\mathfrak{p} \subseteq \varphi^{-1}(\mathfrak{m})$ und $f \notin \varphi^{-1}(\mathfrak{m})$. Nach Satz 10.8 ist $\varphi^{-1}(\mathfrak{m})$ maximal. \square

Satz 10.10. *Sei K ein algebraisch abgeschlossener Körper und sei A eine endlich erzeugte K -Algebra. Dann ist jeder Restklassenkörper von A isomorph zu K . Anders formuliert: jedes maximale Ideal ist ein Punktideal.*

Beweis. Sei \mathfrak{m} ein maximales Ideal der endlich erzeugten K -Algebra A und betrachte

$$K \longrightarrow A \longrightarrow A/\mathfrak{m} =: L.$$

Hier ist L ein Körper und zugleich eine endlich erzeugte K -Algebra. Nach Satz 10.7 muss also L eine endliche K -Algebra sein. Da K algebraisch abgeschlossen ist, muss $K = L$ sein. \square

11. VORLESUNG

11.1. Hilbertscher Nullstellensatz - geometrische Version.

Wir wollen nun die geometrische Version des Hilbertschen Nullstellensatzes beweisen, der für den Fall eines algebraisch abgeschlossenen Körpers eine eindeutige Beziehung zwischen den affin-algebraischen Mengen im affinen Raum \mathbb{A}_K^n und den Radikalidealen im Polynomring stiftet.

Satz 11.1. (Hilbertscher Nullstellensatz (geometrische Version)) Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge, die durch das Ideal \mathfrak{a} beschrieben werde. Es sei $F \in K[X_1, \dots, X_n]$ ein Polynom, das auf V verschwindet. Dann gehört F zum Radikal von \mathfrak{a} , d.h. es gibt ein $r \in \mathbb{N}$ mit $F^r \in \mathfrak{a}$.

Beweis. Angenommen, F gehöre nicht zum Radikal von \mathfrak{a} . Dann gibt es nach Satz 10.9 auch ein maximales Ideal $\mathfrak{m} \subset K[X_1, \dots, X_n]$ mit $\mathfrak{a} \subseteq \mathfrak{m}$ und mit $F \notin \mathfrak{m}$. Nach Satz 10.10 ist

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$$

für gewisse $a_1, \dots, a_n \in K$. Die Eigenschaft $F \notin \mathfrak{m}$ bedeutet, dass F im zugehörigen Restkörper nicht 0 ist, und das bedeutet $F(a_1, \dots, a_n) \neq 0$. Wegen $\mathfrak{a} \subseteq \mathfrak{m}$ ist aber (a_1, \dots, a_n) ein Punkt von V , so dass dort nach Voraussetzung F verschwindet. Das ist also ein Widerspruch. \square

Satz 11.2. (Radikale und affin-algebraische Mengen) Sei K ein algebraisch abgeschlossener Körper mit dem Polynomring $K[X_1, \dots, X_n]$ und dem affinen Raum \mathbb{A}_K^n . Dann gibt es eine natürliche Korrespondenz zwischen affin-algebraischen Mengen in \mathbb{A}_K^n und Radikalidealen in $K[X_1, \dots, X_n]$. Dabei gehen Radikale auf ihre Nullstellengebilde und affin-algebraische Mengen auf ihre Verschwindungsideale.

Beweis. Sei $V \subseteq \mathbb{A}_K^n$ affin-algebraisch. Dann gilt $V = V(\text{Id}(V))$ nach Lemma 3.7 (3). Für ein Radikal $I \subseteq K[X_1, \dots, X_n]$ gilt die Inklusion $I \subseteq \text{Id}(V(I))$ ebenfalls nach Lemma 3.7 (2). Die umgekehrte Inklusion, also $\text{Id}(V(I)) \subseteq I$ ist der Inhalt des Hilbertschen Nullstellensatzes 11.1. \square

Korollar 11.3. Sei K ein algebraisch abgeschlossener Körper und seien $F_i \in K[X_1, \dots, X_n]$, $i \in I$, Polynome mit

$$\mathbb{A}_K^n = \bigcup_{i \in I} D(F_i).$$

Dann erzeugen die F_i das Einheitsideal in $K[X_1, \dots, X_n]$.

Beweis. Sei \mathfrak{b} das von den F_i erzeugte Ideal. Die Voraussetzung besagt, dass

$$\bigcap_{i \in I} V(F_i) = V(\mathfrak{b})$$

leer ist. Dann ist $V(1) \subseteq V(\mathfrak{b})$, da ja $V(1)$ ebenfalls leer ist. Aus dem Hilbertschen Nullstellensatz 11.1 folgt, dass eine Potenz von 1, also 1 selbst, zu \mathfrak{b} in $K[X_1, \dots, X_n]$ gehört. D.h. dass \mathfrak{b} das Einheitsideal ist. \square

Der Hilbertsche Nullstellensatz, wie wir ihn für den affinen Raum und den Polynomring formuliert haben, gilt entsprechend für jedes $V(\mathfrak{a})$ und den zugehörigen Restklassenring $K[X_1, \dots, X_n]/\mathfrak{a}$.

Korollar 11.4. Sei K ein algebraisch abgeschlossener Körper und sei $R = K[X_1, \dots, X_n]/\mathfrak{a}$ eine endlich erzeugte K -Algebra mit Nullstellengebilde $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$. Es sei \mathfrak{b} ein Ideal in R und $F \in R$ ein Element, das auf $V(\mathfrak{b}) \subseteq V$ verschwindet. Dann gibt es ein $r \in \mathbb{N}$ mit $F^r \in \mathfrak{b}$ in R .

Beweis. Die Verschwindungsbedingung $V(\mathfrak{b}) \subseteq V(F)$ in $V = V(\mathfrak{a})$ besagt zurückübersetzt in den affinen Raum, dass dort $V(\mathfrak{a} + \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b}) \subseteq V(F)$ gilt, wobei jetzt F ein repräsentierendes Polynom aus $K[X_1, \dots, X_n]$ und \mathfrak{b} das Urbildideal in $K[X_1, \dots, X_n]$ sei. Nach dem Hilbertschen Nullstellensatz 11.1 gibt es ein $r \in \mathbb{N}$ mit $F^r \in \mathfrak{a} + \mathfrak{b}$. Dies bedeutet modulo \mathfrak{a} , dass in R die Beziehung $F^r \in \mathfrak{b}$ gilt. \square

Korollar 11.5. Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge, die durch das Ideal \mathfrak{a} beschrieben werde. Es seien $F_i \in K[X_1, \dots, X_n]$, $i \in I$, Polynome mit

$$V = \bigcup_{i \in I} D(F_i).$$

Dann erzeugen die F_i das Einheitsideal in $K[X_1, \dots, X_n]/\mathfrak{a}$.

Beweis. Sei \mathfrak{b} das von allen F_i , $i \in I$, erzeugte Ideal in $K[X_1, \dots, X_n]/\mathfrak{a}$. Die Voraussetzung besagt, dass

$$V(\mathfrak{b}) = \bigcap_{i \in I} V(F_i)$$

(auf V) leer ist. Dann ist $V(1) \subseteq V(\mathfrak{b})$, da ja $V(1)$ ebenfalls leer ist. Aus dem Hilbertschen Nullstellensatz 11.4 folgt, dass eine Potenz von 1, also 1 selbst, zu \mathfrak{b} in $K[X_1, \dots, X_n]/\mathfrak{a}$ gehört. \square

Korollar 11.6. Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge, die durch das Ideal \mathfrak{a} beschrieben werde. Es sei $F \in K[X_1, \dots, X_n]$ ein Polynom, das auf V keine Nullstelle besitzt. Dann ist F im Restklassenring $K[X_1, \dots, X_n]/\mathfrak{a}$ eine Einheit.

Beweis. Dies ist ein Spezialfall von Korollar 11.5. \square

Korollar 11.7. Sei K ein algebraisch abgeschlossener Körper und seien V_1 und V_2 zwei affin-algebraische Mengen in \mathbb{A}_K^n . Dann gilt

$$\text{Id}(V_1 \cap V_2) = \text{rad}(\text{Id}(V_1) + \text{Id}(V_2)).$$

Beweis. Sei $\mathfrak{a}_1 = \text{Id}(V_1)$ und $\mathfrak{a}_2 = \text{Id}(V_2)$. Die Aussage ergibt sich aus $\text{rad}(\mathfrak{a}_1 + \mathfrak{a}_2) = \text{Id}(V(\text{rad}(\mathfrak{a}_1 + \mathfrak{a}_2))) = \text{Id}(V(\mathfrak{a}_1 + \mathfrak{a}_2)) = \text{Id}(V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2))$, wobei die erste Gleichung auf dem Hilbertschen Nullstellensatz 11.1 beruht. \square

Auch diese Eigenschaften gelten nicht ohne die Voraussetzung algebraisch abgeschlossen, wie das folgende Beispiel zeigt.

Beispiel 11.8. Wir betrachten die beiden algebraischen Kurven

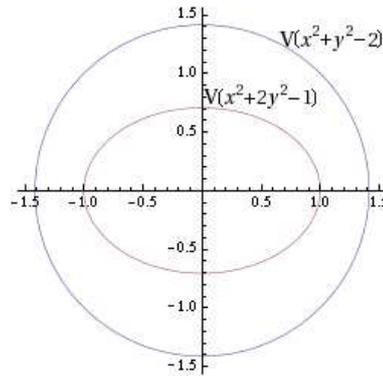
$$V_1 = V(X^2 + Y^2 - 2) \text{ und } V_2 = (X^2 + 2Y^2 - 1) \subseteq \mathbb{A}_K^2.$$

Bei $K = \mathbb{R}$ sind das beides irreduzible Quadriken. Der Durchschnitt wird beschrieben durch das Ideal

$$(X^2 + Y^2 - 2, X^2 + 2Y^2 - 1) = (Y^2 + 1, X^2 - 3).$$

Da das Polynom $Y^2 + 1$ im Reellen keine Nullstelle hat, ist der Durchschnitt $V_1 \cap V_2 = \emptyset$ leer. Das Verschwindungsideal des (leeren) Durchschnittes ist natürlich das Einheitsideal, die Summe der beiden Verschwindungsideale ist aber nicht das Einheitsideal.

Es folgt, dass die Funktion $X^2 + 2Y^2 - 1$ auf $V(X^2 + Y^2 - 2)$ keine Nullstelle besitzt, also dort überall eine Einheit ist, aber dass sie keine Einheit im Koordinatenring $K[X, Y]/(X^2 + Y^2 - 2)$ ist.



11.2. Der Koordinatenring zu einer affin-algebraischen Menge.

Sei $V \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge mit Verschwindungsideal $\text{Id}(V)$. Ein Polynom $F \in K[X_1, \dots, X_n]$ definiert eine Funktion auf dem affinen Raum und induziert damit eine Funktion auf der Teilmenge V .

$$\begin{array}{ccc} \mathbb{A}_K^n & \xrightarrow{F} & K \\ \uparrow & \nearrow & \\ V & & \end{array}$$

Dabei induziert ein Element aus dem Verschwindungsideal (nach Definition) die Nullfunktion auf V , und zwei Polynome $G, H \in K[X_1, \dots, X_n]$, deren Differenz zum Verschwindungsideal gehören, induzieren auf V die gleiche Funktion. Es ist daher naheliegend, den Restklassenring $K[X_1, \dots, X_n]/\text{Id}(V)$ als Ring der polynomialen (oder algebraischen) Funktion auf V zu betrachten.

Definition 11.9. Zu einer affin-algebraischen Menge $V \subseteq \mathbb{A}_K^n$ mit Verschwindungsideal $\text{Id}(V)$ nennt man

$$R(V) = K[X_1, \dots, X_n]/\text{Id}(V)$$

den *Koordinatenring* von V .

Dieser Begriff ist nicht völlig unproblematisch, insbesondere, wenn K nicht algebraisch abgeschlossen ist, siehe die Beispiele weiter unten. Wir erwähnen zunächst einige elementare Eigenschaften.

Proposition 11.10. *Sei $V \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge und sei $R = K[X_1, \dots, X_n]/\text{Id}(V)$ der zugehörige Koordinatenring. Dann gelten folgende Aussagen.*

- (1) R ist reduziert.
- (2) $V = \emptyset$ genau dann, wenn R der Nullring ist.
- (3) V ist irreduzibel genau dann, wenn R ein Integritätsbereich ist.
- (4) V besteht aus einem einzigen Punkt genau dann, wenn $R = K$ ist.
- (5) Ist K algebraisch abgeschlossen, und $V = V(\mathfrak{a})$, so ist $R = K[X_1, \dots, X_n]/\text{rad}(\mathfrak{a})$.

Beweis. Es sei $I = \text{Id}(V)$ das Verschwindungsideal zu V .

- (1). Dies folgt aus Lemma 3.13 und Aufgabe 3.3.
- (2). $V = \emptyset$ ist äquivalent zu $1 \in I$, und das ist äquivalent zu $R = 0$.
- (3). Dies folgt aus Lemma 4.3 und Lemma (siehe die Übersicht zur Restklassenbildung).
- (4). Sei $V = \{P\}$, $P = (a_1, \dots, a_n)$. Dann ist $I = (X_1 - a_1, \dots, X_n - a_n)$ und der Koordinatenring ist

$$K[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n) \cong K.$$

Umgekehrt, wenn der Koordinatenring K ist, so muss der zugehörige Restklassenhomomorphismus ein Einsetzungshomomorphismus $X_i \mapsto a_i$ sein, und das Verschwindungsideal zu V muss ein Punktideal sein, und es ist $P = (a_1, \dots, a_n) \in V$. Wenn es noch einen weiteren Punkt $Q \in V$, $Q \neq P$, gibt, so hat man einen Widerspruch, da nicht alle $X_i - a_i$ in Q verschwinden.

- (5). Bei K algebraisch abgeschlossen ist $\text{Id}(V) = \text{rad}(\mathfrak{a})$ nach dem Hilbertschen Nullstellensatz 11.1. □

Satz 11.11. *Sei K ein unendlicher Körper. Dann ist das Verschwindungsideal des affinen Raumes \mathbb{A}_K^n das Nullideal und der zugehörige Koordinatenring ist der Polynomring $K[X_1, \dots, X_n]$.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl der Variablen. Bei $n = 1$ folgt die Aussage daraus, dass ein Polynom vom Grad d maximal d Nullstellen besitzt. Zum Induktionsschritt sei $F \in K[X_1, \dots, X_n]$ ein Polynom, das an allen Punkten von $\mathbb{A}_K^n = K^n$ verschwindet. Wir schreiben F als

$$F = P_d X_n^d + P_{d-1} X_n^{d-1} + \dots + P_1 X_n + P_0$$

mit Polynomen $P_d, \dots, P_0 \in K[X_1, \dots, X_{n-1}]$. Wir müssen zeigen, dass $F = 0$ ist, was äquivalent zu $P_i = 0$ ist für alle $i = 0, \dots, d$. Sei also (ohne Einschränkung) angenommen, dass P_d nicht das Nullpolynom ist. Nach Induktionsvoraussetzung ist es dann auch nicht die Nullfunktion, d.h. es gibt einen Punkt (a_1, \dots, a_{n-1}) mit $P_d(a_1, \dots, a_{n-1}) \neq 0$. Damit ist $F(a_1, \dots, a_{n-1})$ ein Polynom in der einen Variablen X_n vom Grad d und ist nach dem Fall einer Variablen nicht die Nullfunktion. \square

Beispiel 11.12. Die Aussage 11.11 ist nicht richtig für endliche Körper. Für einen endlichen Körper besteht ein affiner Raum nur aus endlich vielen Punkten und es gibt viele Polynome, die auf all diesen Punkten verschwinden. Typische Beispiele werden gegeben durch die Polynome $X_i^q - X_i$, wobei q die Anzahl der Körperelemente bezeichne.

Beispiel 11.13. Sei $R = \mathbb{R}[X, Y]/(X^2 + Y^2)$. Da Quadrate im Reellen nie negativ sind, besteht die Nullstellenmenge des Polynoms $X^2 + Y^2$ einzig aus dem Nullpunkt, $V(X^2 + Y^2) = \{(0, 0)\}$. Das zugehörige Verschwindungsideal ist das maximale Ideal (X, Y) , und der zugehörige Restklassenring (der Koordinatenring) ist dann $\mathbb{R}[X, Y]/(X, Y) \cong \mathbb{R}$. Der Koordinatenring kann also vom Restklassenring, mit dem man startet und dessen Ideal das Nullstellengebilde definiert, sehr verschieden sein.

12. VORLESUNG

12.1. Das K -Spektrum.

Wie hängen affin-algebraische Mengen und deren Koordinatenringe zusammen? Hier kann man nur für nicht-endliche Grundkörper gehaltvolle Antworten erwarten, da es im endlichen Fall zu wenige Punkte gibt. Eine befriedigende Theorie erfordert sogar, dass man sich auf algebraisch abgeschlossene Körper beschränkt, oder aber - das ist der Standpunkt der von Alexander Grothendieck entwickelten Schematheorie - nicht nur K -Punkte betrachtet, sondern generell maximale Ideale und Primideale als Punkte mitberücksichtigt.



Alexander Grothendieck (1928-)

Eine erste wichtige Frage ist folgende: eine K -Algebra R von endlichem Typ hat mehrere, in aller Regel gleichberechtigte Darstellungen als Restklassenring einer Polynomalgebra, sagen wir

$$K[X_1, \dots, X_n]/\mathfrak{a} \cong R \cong K[X_1, \dots, X_m]/\mathfrak{b}.$$

Dazu gehören die beiden Nullstellengebilde $V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ und $V(\mathfrak{b}) \subseteq \mathbb{A}_K^m$. Wie hängen diese beiden Nullstellengebilde zusammen?

Beispiel 12.1. Wir betrachten den Polynomring in einer Variablen $R = K[T]$. Ihm entspricht zunächst die affine Gerade \mathbb{A}_K^1 . Man kann R aber auch auf ganz verschiedene Arten als Restklassenring einer Polynomalgebra in mehreren Variablen erhalten. Sei beispielsweise $a \in K$, $a \neq 0$, und betrachte den Restklassenring $K[X, Y]/(aY + bX)$. Dieser Ring ist (als K -Algebra) isomorph zu R , wie die Abbildung

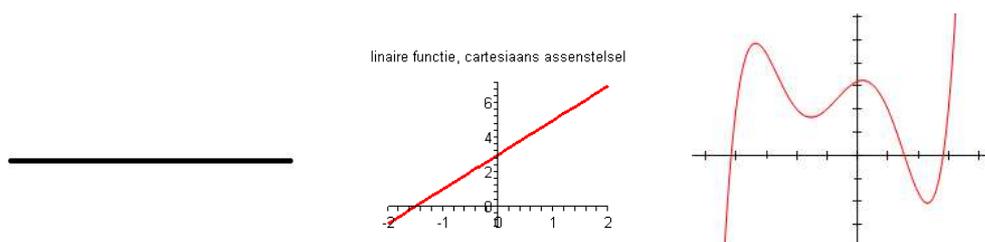
$$K[X, Y]/(aY + bX) \longrightarrow K[T], X \longmapsto T, Y \longmapsto -\frac{b}{a}T,$$

zeigt. Das zugehörige Nullstellengebilde $V(aX + bY)$ ist einfach die Gerade in der affinen Ebene, die durch die Gleichung $Y = -\frac{b}{a}X$ beschrieben wird.

Eine weitere Möglichkeit, den Polynomring in einer Variablen als Restklassenring darzustellen, ist durch $K[X, Y]/(Y - P(X))$ gegeben, wobei $P(X)$ ein beliebiges Polynom in der einen Variablen X ist. Der Ringhomomorphismus

$$K[X, Y]/(Y - P(X)) \longrightarrow K[T], X \longmapsto T, Y \longmapsto P(T),$$

zeigt, dass ein Isomorphismus vorliegt. Das zugehörige Nullstellengebilde ist einfach der Graph des Polynoms $P(X)$.



Der Punkt an diesem Beispiel ist, dass alle drei geometrischen Objekte die Nullstellenmengen zu verschiedenen Restklassendarstellungen von $K[T]$ sind. Vom Standpunkt der algebraischen Geometrie sind das drei gleichberechtigte Darstellungen der affinen Geraden, auch wenn sie unterschiedlich „aussehen“. In der algebraischen Geometrie muss man so hinschauen, dass sie gleich aussehen. Was man sieht sind nur verschiedene Einbettungen des „eigentlichen und wahren“ geometrischen Objektes, das zu einer K -Algebra intrinsisch gehört, nämlich das K -Spektrum.

Definition 12.2. Zu einer kommutativen K -Algebra R von endlichem Typ bezeichnet man die Menge der K -Algebra-Homomorphismen

$$\text{Hom}_K(R, K)$$

als das K -Spektrum von R . Es wird mit $K - \text{Spek}(R)$ bezeichnet.

Die Elemente in einem K -Spektrum $K - \text{Spek}(R)$ betrachten wir als Punkte und bezeichnen sie üblicherweise mit P , obwohl es definitionsgemäß Abbildungen sind, nämlich K -Algebra-Homomorphismen von R nach K . Für ein Ringelement $f \in R$ schreiben wir dann auch einfach $f(P)$ (statt $P(f)$) für den Wert von f unter dem mit P bezeichneten Ringhomomorphismus (es ist

nicht unüblich, einen Punkt als eine Auswertung von Funktionen anzusehen, die in einer gewissen Umgebung des Punktes definiert sind).

Das K -Spektrum wird wieder mit einer *Zariski-Topologie* versehen, wobei zu einem Ideal $\mathfrak{a} \subseteq R$ (oder zu einer beliebigen Teilmenge aus R) die Teilmenge

$$V(\mathfrak{a}) = \{P \in K - \text{Spek}(R) : f(P) = 0 \text{ für alle } f \in \mathfrak{a}\}$$

als abgeschlossen erklärt wird. In der Tat wird dadurch eine Topologie definiert, siehe Aufgabe 12.1.

Lemma 12.3. *Sei K ein Körper und sei $K[X_1, \dots, X_n]$ der Polynomring in n Variablen. Dann stehen die K -Algebra-Homomorphismen von $K[X_1, \dots, X_n]$ nach K in natürlicher Weise in Bijektion mit den Punkten aus dem affinen Raum $\mathbb{A}_K^n = K^n$, und zwar entspricht dem Punkt (a_1, \dots, a_n) der Einsetzungshomomorphismus $X_i \mapsto a_i$. Mit anderen Worten,*

$$K - \text{Spek}(K[X_1, \dots, X_n]) = \mathbb{A}_K^n.$$

Beweis. Ein K -Algebra-Homomorphismus ist stets durch ein K -Algebra Erzeugendensystem festgelegt. D.h. die Werte an den Variablen X_i legen einen K -Algebra-Homomorphismus von $K[X_1, \dots, X_n]$ nach K fest. Ein solcher Einsetzungshomomorphismus ist durch $X_i \mapsto a_i$ definiert. Zugleich ist hier jede Vorgabe von Werten (a_1, \dots, a_n) erlaubt. \square

Beispiel 12.4. Das K -Spektrum zur K -Algebra K besteht einfach aus einem Punkt, und zwar ist die Identität $K \rightarrow K$ der einzige K -Algebra-Homomorphismus von K nach K . Es gibt im Allgemeinen weitere Körperautomorphismen auf K , doch diese sind keine K -Algebra-Homomorphismen.

Entscheidend ist nun der folgende Satz, der eine bijektive Beziehung zwischen dem K -Spektrum von R und dem Nullstellengebilde stiftet, das von einer Restklassendarstellung von R herrührt.

Satz 12.5. *Sei K ein Körper und sei R eine endlich erzeugte kommutative K -Algebra mit K -Spektrum $K - \text{Spek}(R)$. Es sei $R = K[X_1, \dots, X_n]/\mathfrak{a}$ eine Restklassendarstellung von R mit dem zugehörigen Restklassenhomomorphismus $\varphi : K[X_1, \dots, X_n] \rightarrow R$ und dem Nullstellengebilde $V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$. Dann stiftet die Abbildung*

$$K - \text{Spek}(R) \longrightarrow \mathbb{A}_K^n, P \longmapsto P \circ \varphi,$$

eine Bijektion zwischen $K - \text{Spek}(R)$ und $V(\mathfrak{a})$, die bezüglich der Zariski-Topologie ein Homöomorphismus ist.

Beweis. Zunächst ist die angegebene Abbildung wohldefiniert, da die Hintereinanderschaltung

$$P \circ \varphi : K[X_1, \dots, X_n] \xrightarrow{\varphi} K[X_1, \dots, X_n]/\mathfrak{a} \cong R \xrightarrow{P} K$$

einen K -Algebra-Homomorphismus vom Polynomring nach K definiert, der nach Lemma 12.3 der Einsetzungshomomorphismus zu (a_1, \dots, a_n) ist und mit dem entsprechenden Punkt des affinen Raumes identifiziert werden kann.

Da der Homomorphismus $P \circ \varphi$ durch R faktorisiert, wird das Ideal \mathfrak{a} auf 0 abgebildet. D.h. der Bildpunkt $P \circ \varphi = (a_1, \dots, a_n)$ liegt in $V(\mathfrak{a})$, und es liegt eine Abbildung

$$K - \text{Spek}(R) \longrightarrow V(\mathfrak{a}) \subseteq \mathbb{A}_K^n, P \longmapsto P \circ \varphi,$$

vor, die wir als bijektiv nachweisen müssen.

Seien dazu $P_1, P_2 \in K - \text{Spek}(R)$ zwei verschiedene Punkte. Es liegen also zwei verschiedene K -Algebra Homomorphismen vor, und da ein K -Algebra-Homomorphismus auf einem K -Algebra Erzeugendensystem festgelegt ist, müssen sich die beiden auf mindestens einer Variablen unterscheiden. Dann ist aber auch der Wert der zugehörigen Koordinate verschieden, d.h. $P_1 \circ \varphi \neq P_2 \circ \varphi$, und die Abbildung ist injektiv.

Zur Surjektivität sei ein Punkt $(a_1, \dots, a_n) \in V(\mathfrak{a})$ vorgegeben. Der zugehörige K -Algebra-Homomorphismus

$$K[X_1, \dots, X_n] \longrightarrow K, X_i \longmapsto a_i,$$

annuliert daher jedes $F \in \mathfrak{a}$, so dass dieser Ringhomomorphismus durch $K[X_1, \dots, X_n]/\mathfrak{a}$ faktorisiert. Dieser Ringhomomorphismus ist das gesuchte Urbild aus $K - \text{Spek}(R)$.

Zur Topologie muss man einfach nur beachten, dass für $G \in R$ und einem Urbild $\tilde{G} \in K[X_1, \dots, X_n]$ und einem Punkt $P \in K - \text{Spek}(R)$ mit Bildpunkt $\tilde{P} = P \circ \varphi \in V(\mathfrak{a})$ gilt:

$$G(P) = P(G) = P(\varphi(\tilde{G})) = (P \circ \varphi)(\tilde{G}) = \tilde{G}(\tilde{P}),$$

so dass auch die Nullstellen übereinstimmen. □

Dieser Satz besagt also, dass man jedes K -Spektrum einer endlich erzeugten K -Algebra R mit einer Zariski-abgeschlossenen Menge eines \mathbb{A}_K^n identifizieren kann. Man spricht von einer *abgeschlossenen Einbettung*.

Korollar 12.6. *Sei K ein Körper und R eine endlich erzeugte kommutative K -Algebra mit zwei Restklassendarstellungen*

$$R \cong K[X_1, \dots, X_n]/\mathfrak{a} \text{ und } R \cong K[X_1, \dots, X_m]/\mathfrak{b}$$

mit zugehörigen Nullstellengebilden $V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ und $V(\mathfrak{b}) \subseteq \mathbb{A}_K^m$. Dann sind die beiden Nullstellengebilde $V(\mathfrak{a})$ und $V(\mathfrak{b})$ mit ihrer induzierten Zariski-Topologie homöomorph zueinander.

Beweis. Nach Satz 12.3 sind beide Nullstellen homöomorph zu $K - \text{Spek}(R)$, so dass sie auch untereinander homöomorph sein müssen. □

12.2. Das K -Spektrum als Funktor.

Satz 12.7. *Sei K ein Körper und seien R und S zwei kommutative K -Algebren von endlichem Typ. Es sei $\varphi : R \rightarrow S$ ein K -Algebra-Homomorphismus. Dann induziert dies eine Abbildung*

$$\varphi^* : K - \text{Spek}(S) \longrightarrow K - \text{Spek}(R), P \longmapsto P \circ \varphi.$$

Diese Abbildung ist stetig bezüglich der Zariski-Topologie.

Beweis. Die Existenz der Abbildung ist klar, dem K -Algebra-Homomorphismus $P : S \rightarrow K$ wird einfach die Hintereinanderschaltung

$$R \xrightarrow{\varphi} S \xrightarrow{P} K$$

zugeordnet. Das Urbild der offenen Menge $D(f) \subseteq K - \text{Spek}(R)$ ist dabei

$$\begin{aligned} (\varphi^*)^{-1}(D(f)) &= \{P \in K - \text{Spek}(S) : \varphi^*(P) \in D(f)\} \\ &= \{P \in K - \text{Spek}(S) : P \circ \varphi \in D(f)\} \\ &= \{P \in K - \text{Spek}(S) : (P \circ \varphi)(f) \neq 0\} \\ &= \{P \in K - \text{Spek}(S) : P(\varphi(f)) \neq 0\} \\ &= D(\varphi(f)). \end{aligned}$$

Daher sind generell Urbilder von offenen Mengen wieder offen und die Abbildung ist stetig. \square

Die in Satz 11.7 eingeführte Abbildung φ^* nennt man die *Spektrumsabbildung* zu φ :

Proposition 12.8. *Es sei K ein Körper und zu einem K -Algebra-Homomorphismus $\varphi : R \rightarrow S$ zwischen K -Algebren von endlichem Typ sei φ^* die zugehörige Spektrumsabbildung. Dann gelten folgende Aussagen.*

- (1) *Zu einem K -Algebra-Homomorphismus $P : R \rightarrow K$ ist die induzierte Spektrumsabbildung P^* einfach die Abbildung, die dem einzigen Punkt $\{\text{id}\} = K - \text{Spek}(K)$ den Punkt $P \in K - \text{Spek}(R)$ zuordnet.*
- (2) *Der durch ein Element $F \in R$ definierte Einsetzungshomomorphismus*

$$\varphi : K[T] \longrightarrow R, T \longmapsto F,$$

induziert die Spektrumsabbildung

$$\varphi^* : K - \text{Spek}(R) \longrightarrow K - \text{Spek}(K[T]) = \mathbb{A}_K^1, P \longmapsto F(P).$$

- (3) *Zu einer surjektiven Abbildung $\varphi : R \rightarrow S$ von K -Algebren von endlichem Typ ist die zugehörige Spektrumsabbildung*

$$\varphi^* : K - \text{Spek}(S) \longrightarrow K - \text{Spek}(R)$$

eine abgeschlossene Einbettung, und zwar ist das Bild gleich $V(\ker(\varphi))$.

(4) Die zu einer surjektiven Abbildung $K[X_1, \dots, X_n] \longrightarrow S$ gehörende Spektrumsabbildung

$$\varphi^* : K - \text{Spek}(S) \longrightarrow K - \text{Spek}(K[X_1, \dots, X_n]) \cong \mathbb{A}_K^n$$

stimmt mit der in Satz 12.5 definierten Abbildung überein.

Beweis. (1). Dies folgt aus $\text{id} \circ P = P$.

(2). Unter der hintereinandergeschalteten Abbildung

$$K[T] \xrightarrow{\varphi} R \xrightarrow{P} K$$

wird T auf $P(F) = F(P)$ geschickt.

(3) beruht auf ähnlichen Betrachtungen wie sie im Beweis zu Satz 12.5 durchgeführt wurden. Das zeigt auch (4). \square

12.3. Weitere Eigenschaften des K -Spektrums.

Lemma 12.9. Sei K ein Körper und R eine endlich erzeugte kommutative K -Algebra. Dann ist

$$K - \text{Spek}(R[X]) \cong K - \text{Spek}(R) \times \mathbb{A}_K^1.$$

Beweis. Ein K -Algebra-Homomorphismus $R[T] \rightarrow K$ induziert einen K -Algebra-Homomorphismus $R \rightarrow K$, und zugleich wird T auf ein bestimmtes Element $a \in K$ abgebildet. Diese Daten definieren aber auch einen eindeutig bestimmten K -Algebra-Homomorphismus $R[T] \rightarrow K$. \square

Achtung: Die vorstehende Aussage liefert nur eine natürliche Bijektion auf der Punktebene. Würde man die Produktmenge rechts mit der Produkttopologie versehen, so würde hier keine Homöomorphie mit der Zariski-Topologie links vorliegen. Insbesondere ist $\mathbb{A}_K^2 \cong \mathbb{A}_K^1 \times \mathbb{A}_K^1$, aber die Zariski-Topologie der affinen Ebene ist nicht die Produkt-Topologie der affinen Geraden mit sich selbst.

Bemerkung 12.10. Sind $X = K - \text{Spek}(R)$ und $Y = K - \text{Spek}(S)$, so lässt sich die Produktmenge ebenfalls als K -Spektrum einer K -Algebra darstellen, und zwar ist

$$X \times Y \cong K - \text{Spek}(R \otimes_K S),$$

wobei \otimes das Tensorprodukt bezeichnet. Wir werden darauf nicht im Einzelnen eingehen. Um aber doch ein Gefühl dafür zu geben betrachten wir $R = K[X_1, \dots, X_n]/\mathfrak{a}$ und $S = K[Y_1, \dots, Y_m]/\mathfrak{b}$. Dann ist

$$R \otimes_K S \cong K[X_1, \dots, X_n, Y_1, \dots, Y_m]/(\mathfrak{a} + \mathfrak{b})$$

(bei dieser ad hoc Definition ist nicht klar, dass sie unabhängig von den Darstellungen als Restklassenring ist).

13. VORLESUNG

13.1. Die offenen Mengen $D(f)$.

Wir wollen zeigen, dass die Zariski-offenen Teilmengen $D(f) \subseteq K - \text{Spek}(R)$ selbst homöomorph zum K -Spektrum einer endlich erzeugten K -Algebra sind. Dazu benötigen wir den Begriff des multiplikativen Systems und der Nenneraufnahme.

Definition 13.1. Sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikatives System*, wenn die beiden Eigenschaften

- (1) $1 \in S$
- (2) Wenn $f, g \in S$, dann ist auch $fg \in S$

gelten.

Beispiel 13.2. (Potenzen eines Elementes) Sei R ein kommutativer Ring und $f \in R$ ein Element. Dann bilden die Potenzen f^n , $n \in \mathbb{N}$, ein multiplikatives System.

Definition 13.3. Sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$. Dann nennt man den Unterring

$$R_S := \left\{ \frac{f}{g} : f \in R, g \in S \right\} \subseteq Q(R)$$

die *Nenneraufnahme* zu S .

Für die Nenneraufnahme an einem Element f schreibt man einfach R_f statt $R_{\{f^n : n \in \mathbb{N}\}}$. Für den Begriff der Nenneraufnahme für beliebige kommutative Ringe, siehe Aufgabe 13.2.

Satz 13.4. Sei K ein Körper und sei R eine endlich erzeugte K -Algebra, $f \in R$. Dann ist die Zariski-offene Menge $D(f) \subseteq K - \text{Spek}(R)$ in natürlicher Weise isomorph zu $K - \text{Spek}(R_f)$.

Beweis. Wir betrachten die zum K -Algebra-Homomorphismus $\varphi : R \rightarrow R_f$ gehörende natürliche Abbildung

$$\varphi^* : K - \text{Spek}(R_f) \longrightarrow K - \text{Spek}(R), P \longmapsto P \circ \varphi,$$

die nach Satz 12.7 stetig ist. Es ist $f(P \circ \varphi) = P(\varphi(f)) \neq 0$, da ja f in R_f eine Einheit wird. Daher liegt das Bild von φ^* in $D(f)$. Sei $Q \in D(f)$ irgendein Punkt, d.h. Q ist ein K -Algebra-Homomorphismus $Q : R \rightarrow K$ mit $Q(f) \neq 0$. Dann ist $Q(f)$ eine Einheit und daher faktorisiert dieser Homomorphismus nach der universellen Eigenschaft der Nenneraufnahme (siehe Aufgabe 13.5) durch R_f . Dieser Morphismus ist das gesuchte Urbild und daher ist φ^* surjektiv.

Zur Injektivität seien zwei K -Algebra-Homomorphismen $P_1, P_2 : R_f \rightarrow K$ gegeben, deren Verknüpfung mit $R \rightarrow R_f$ übereinstimmen. Wegen

$$P_1\left(\frac{r}{f^s}\right) = P_1(rf^{-s}) = P_1(r)P_1(f^s)^{-1}$$

und ebenso für P_2 ist dann aber $P_1 = P_2$.

Zur Homöomorphie ist lediglich zu beachten, dass die Zariski-offenen Mengen von $K - \text{Spek}(R_f)$ überdeckt werden von $D(g)$, $g \in R_f$. Dabei kann man $g \in R$ annehmen, da f eine Einheit in R_f ist. Dann ist aber dieses $D(g)$ gleich $(\varphi^*)^{-1}(D(gf))$, wo letzteres $D(gf)$ die offene Menge in $K - \text{Spek}(R)$ bezeichnet. \square

Bemerkung 13.5. Die Aussage 13.4 besagt insbesondere, dass eine offene Menge $D(f) \subseteq K - \text{Spek}(R)$ selbst das K -Spektrum einer endlich erzeugten K -Algebra ist (nämlich von R_f , das über R von $1/f$ erzeugt wird), und sich daher auch als Zariski-abgeschlossene Menge eines affinen Raumes realisieren lassen muss. Aus $R_f \cong R[T]/(Tf - 1)$ (siehe Aufgabe 13.6) erhält man eine solche Realisierung. Sei $R = K[X_1, \dots, X_n]/\mathfrak{a}$. Dann liefert der surjektive Ringhomomorphismus

$$\begin{aligned} K[X_1, \dots, X_n, T] &\longrightarrow (K[X_1, \dots, X_n]/\mathfrak{a})[T] \\ &\longrightarrow ((K[X_1, \dots, X_n]/\mathfrak{a})[T])/(Tf - 1) \cong R_f \end{aligned}$$

eine abgeschlossene Einbettung von $D(f)$ in \mathbb{A}_K^{n+1} . Ist ψ die Gesamtinklusion

$$D(f) \subseteq K - \text{Spek}(R) \subseteq \mathbb{A}_K^n,$$

so kann man die abgeschlossene Einbettung auch als

$$\psi \times \frac{1}{f} : D(f) \longrightarrow \mathbb{A}_K^n \times \mathbb{A}_K^1$$

auffassen, wobei hier wieder das Produkt von Varietäten auftritt.

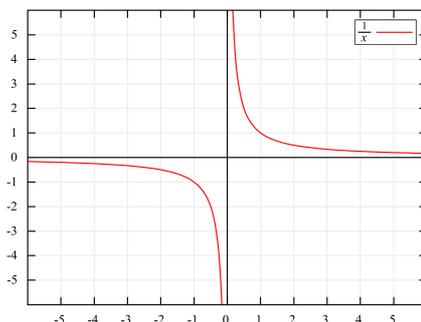
Beispiel 13.6. (Die punktierte affine Gerade als Hyperbel) Betrachten wir in Anschluss an Bemerkung 13.5 die offene Menge

$$D(X) = \{P \in \mathbb{A}_K^1 : P \neq 0\} \subset \mathbb{A}_K^1.$$

Diese offene Menge nennt man die *punktierte affine Gerade*. Auf dieser offenen Menge ist X invertierbar, d.h. die rationale Funktion $\frac{1}{X}$ ist darauf definiert. Diese Abbildung liefert zusammen mit der gegebenen (offenen) Inklusion $D(X) \subset \mathbb{A}_K^1$ die abgeschlossene Inklusion

$$D(X) \longrightarrow V(XY - 1) \subset \mathbb{A}_K^2, x \longmapsto \left(x, \frac{1}{x}\right),$$

dessen Bild eine (in der affinen Ebene abgeschlossene) Hyperbel ist. Die punktierte affine Gerade und die Hyperbel sind also homöomorph (und die zugehörigen Ringe, nämlich $K[X]_X = K[X, X^{-1}]$ und $K[X, Y]/(XY - 1)$, sind isomorph.



13.2. Zusammenhang und idempotente Elemente.

Wir interessieren uns dafür, wie es sich auf den Koordinatenring auswirkt, wenn eine affin-algebraische Menge zusammenhängend ist, und wie sich gegebenenfalls die Zusammenhangskomponenten charakterisieren lassen. Wir beginnen mit einem Beispiel, das zeigt, dass über einem nicht algebraisch abgeschlossenen Körper keine überzeugende Theorie zu erwarten ist.

Beispiel 13.7. Wir betrachten wie in Beispiel 11.8 die beiden algebraischen Kurven

$$V_1 = V(X^2 + Y^2 - 2) \text{ und } V_2 = (X^2 + 2Y^2 - 1) \subseteq \mathbb{A}_K^2.$$

Der Durchschnitt wird beschrieben durch das Ideal

$$(X^2 + Y^2 - 2, X^2 + 2Y^2 - 1) = (Y^2 + 1, X^2 - 3).$$

Sei $K = \mathbb{R}$. Dann ist $V_1 \cap V_2 = \emptyset$ leer.

Die affin-algebraische Menge $V = V_1 \cup V_2$ ist nicht zusammenhängend (V_1 und V_2 sind die irreduziblen Komponenten und die Zusammenhangskomponenten). Der Koordinatenring von V ist

$$\mathbb{R}[X, Y]/(X^2 + Y^2 - 2)(X^2 + 2Y^2 - 1).$$

Man könnte erwarten, dass die Funktion auf V , die auf V_1 konstant gleich 1 und auf V_2 konstant gleich 0 ist, sich im Koordinatenring wiederfindet. Dies ist aber nicht der Fall, und zwar liegt das daran, dass über den komplexen Zahlen $V_{\mathbb{C}}$ zusammenhängend ist. Daher besitzt der komplexe Koordinatenring nur die trivialen idempotenten Elemente, und das überträgt sich auf den reellen Koordinatenring von.

Definition 13.8. Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Definition 13.9. Seien R_1, \dots, R_n kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n,$$

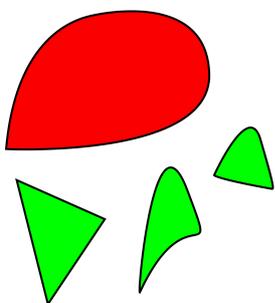
versehen mit komponentenweiser Addition und Multiplikation, der *Produkttring* der R_i , $i = 1, \dots, n$.

In einem Produktring gibt es viele idempotente Elemente, nämlich solche Elemente, deren Komponenten alle null oder eins sind.

Definition 13.10. Ein kommutativer Ring R heißt *zusammenhängend*, wenn er genau zwei idempotente Elemente (nämlich $0 \neq 1$) enthält.

Definition 13.11. Ein topologischer Raum X heißt *zusammenhängend*, wenn es in X genau zwei Teilmengen gibt (nämlich \emptyset und der Gesamttraum X), die sowohl offen als auch abgeschlossen sind.

Die leere Menge und der Gesamttraum sind stets zugleich offen und abgeschlossen. Solche Mengen nennt man auch *randlos* oder *clopen*. Der leere topologische Raum gilt nicht als zusammenhängend, da es in ihm nur eine zugleich offene und abgeschlossene Menge gibt.



Ein zusammenhängender topologischer Raum (rot) und ein nicht zusammenhängender Raum (grün).

Lemma 13.12. Sei K ein Körper und seien R_1 und R_2 endlich erzeugte K -Algebren mit dem Produktring $R = R_1 \times R_2$. Dann gibt es eine natürliche Homöomorphie

$$K - \text{Spek}(R_1 \times R_2) \cong K - \text{Spek}(R_1) \uplus K - \text{Spek}(R_2).$$

Dabei werden die Einbettungen von rechts nach links durch die Projektionen $R \rightarrow R_i$, $i = 1, 2$, induziert.

Beweis. Die Projektion $R_1 \times R_2 \rightarrow R_1$ ist ein K -Algebra-Homomorphismus und liefert daher (nach Proposition 12.8 (3)) eine stetige Abbildung (und zwar eine abgeschlossene Einbettung)

$$K - \text{Spek}(R_1) \longrightarrow K - \text{Spek}(R_1 \times R_2).$$

Ebenso gibt es eine Abbildung auf $K - \text{Spek}(R_2)$. Diese zusammengenommen definieren eine stetige Abbildung

$$K - \text{Spek}(R_1) \uplus K - \text{Spek}(R_2) \longrightarrow K - \text{Spek}(R_1 \times R_2).$$

Sei $P \in K - \text{Spek}(R_1 \times R_2)$, also $P : R_1 \times R_2 \rightarrow K$ sei ein K -Algebra-Homomorphismus. Seien $e_1 = (1, 0)$ und $e_2 = (0, 1)$ die zur Produktzerlegung gehörenden idempotenten Elemente. Wegen $e_1 + e_2 = 1$ und $e_1 e_2 = 0$ wird genau eines dieser Elemente (sagen wir e_1) unter P auf null abgebildet (das andere auf 1). Dann wird aber $R_1 \times 0$ auf null geschickt und P faktorisiert durch eine Projektion. Das beweist die Surjektivität.

Zur Injektivität seien P_1, P_2 in der disjunkten Vereinigung gegeben, $P_1 \neq P_2$. Wenn sie beide in einem der Teilstücke liegen, so bleiben sie unter der Abbildung verschieden, da auf den Teilstücken eine abgeschlossene Einbettung vorliegt. Wenn sie auf verschiedenen Teilstücken liegen, so faktorisieren sie durch die zwei verschiedenen Projektionen und für den einen Punkt ist $P_1(e_1) = 0$ und für den anderen Punkt $P_2(e_1) = 1$. Sie sind also verschieden als Elemente in $K - \text{Spek}(R_1 \times R_2)$.

Eine Homöomorphie liegt vor, da sich die einzelnen abgeschlossenen Einbettungen zu einer abgeschlossenen Abbildung zusammensetzen. \square

Satz 13.13. *Sei K ein algebraisch abgeschlossener Körper und sei R eine reduzierte kommutative K -Algebra von endlichem Typ. Dann stiftet die Abbildung*

$$e \longmapsto D(e)$$

eine Bijektion zwischen den idempotenten Elementen in R und denjenigen Teilmengen aus $K - \text{Spek}(R)$, die sowohl offen also auch abgeschlossen sind.

Beweis. Zunächst ist $D(e) = V(1 - e)$ offen und abgeschlossen. Dies folgt aus

$$D(e) \cup D(1 - e) = D(1) = K - \text{Spek}(R)$$

und aus

$$D(e) \cap D(1 - e) = D(e(1 - e)) = D(e - e^2) = D(0) = \emptyset.$$

D.h. die Abbildung ist wohldefiniert. Seien e_1, e_2 zwei idempotente Elemente mit $U = D(e_1) = D(e_2)$. Da ein idempotentes Element in einem Körper nur die Werte null oder eins annehmen kann, haben sowohl e_1 als auch e_2 auf U den Wert 1 und außerhalb den Wert 0. Damit haben e_1 und e_2 überall den gleichen Wert und sind nach dem Identitätssatz für Polynome (siehe Aufgabe 13.1) überhaupt gleich. Dies beweist die Injektivität.

Sei nun $U = D(\mathfrak{a})$ sowohl offen als auch abgeschlossen. D.h. es gibt ein weiteres Ideal \mathfrak{b} mit

$$D(\mathfrak{a}) \cup D(\mathfrak{b}) = K - \text{Spek}(R) \text{ und } D(\mathfrak{a}) \cap D(\mathfrak{b}) = \emptyset.$$

Nach Korollar 11.5 erzeugen \mathfrak{a} und \mathfrak{b} zusammen das Einheitsideal. D.h. es gibt $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ mit $a + b = 1$. Wegen $D(a) \cap D(b) = D(ab) = \emptyset$ ist nach Aufgabe 13.1 das Element ab nilpotent und wegen der Reduziertheit ist $ab = 0$. Also ist

$$a = a \cdot 1 = a(a + b) = a^2 + ab = a^2$$

idempotent und $U = D(a)$. \square

Es folgt, dass über einem algebraisch abgeschlossenen Körper eine (reduzierte) K -Algebra R von endlichem Typ genau dann zusammenhängend ist, wenn das zugehörige $K - \text{Spek}(R)$ zusammenhängend ist.

14.1. Algebraische Funktionen auf Varietäten.

Was ist ein Morphismus zwischen zwei affin-algebraischen Mengen V und W ? Wir betrachten zuerst die Situation, wo $W = \mathbb{A}_K^1$ die affine Gerade ist. Sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ als abgeschlossene Teilmenge eines affinen Raumes gegeben. Dann liefert jedes Polynom $F \in K[X_1, \dots, X_n]$ eine Abbildung $F : \mathbb{A}_K^n \rightarrow \mathbb{A}_K^1 = K$ und damit auch eine Abbildung auf V . Das haben wir schon bei der Definition des Koordinatenrings betrachtet. Ebenso liefert ein Element $F \in R$ in einer endlich erzeugten K -Algebra R eine Funktion auf $K\text{-Spek}(R)$, nämlich

$$K\text{-Spek}(R) \longrightarrow \mathbb{A}_K^1, P \longmapsto F(P).$$

Dies ist auch die Spektrumsabbildung, die zu $K[T] \rightarrow R, T \mapsto F$, gehört.

Für die offenen Mengen $D(F) \cong K\text{-Spek}(R_F)$ ist $1/F$ nach Satz 13.4 eine wohldefinierte Funktion. Wir werden allgemein für eine Zariski-offene Menge $U \subseteq V$ erklären, was eine algebraische Funktion auf U ist. Die folgende Definition ist so strukturiert, dass die Bedingung „algebraisch“ eine *lokale Eigenschaft* ist.

Definition 14.1. Sei K ein algebraisch abgeschlossener Körper, R eine K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Sei $P \in V$ ein Punkt, $U \subseteq V$ eine Zariski-offene Menge mit $P \in U$ und es sei $f : U \rightarrow \mathbb{A}_K^1 = K$ eine Funktion. Dann heißt f *algebraisch* (oder *regulär* oder *polynomial*) im Punkt P , wenn es Elemente $G, H \in R$ gibt mit $P \in D(H) \subseteq U$ und mit

$$f(Q) = \frac{G(Q)}{H(Q)} \text{ für alle } Q \in D(H).$$

Die Funktion f heißt *algebraisch* (oder *algebraisch auf U*), wenn f in jedem Punkt von U algebraisch ist.

Natürlich definiert jedes Element $f \in R$ eine algebraische Funktion auf jeder offenen Teilmenge des K -Spektrums. Es ist aber im Allgemeinen eher schwierig, die algebraischen Funktionen übersichtlich zu beschreiben.

Bemerkung 14.2. In der Definition 14.1 ist die vorausgesetzte Stetigkeit überflüssig, da sie aus der lokalen algebraischen Bedingung folgt (siehe Aufgabe 15.1).

Ebenso ist die Bedingung $D(H) \subseteq U$ nicht wichtig. Wenn es eine Beschreibung für f mit $f = G/H$ auf $D(H)$ mit $P \in D(H)$ gibt, so betrachtet man ein H' mit $P \in D(H')$, $D(H') \subseteq U$. Dann kann man zu $D(H) \cap D(H') = D(HH')$ übergehen, und dort die Darstellung $f = (GH')/(HH')$ betrachten.

Wenn es im Punkt P eine Bruchdarstellung für f als $f = G/H$ gibt, so kann man diese Darstellung für alle Punkte aus $D(H)$ verwenden. D.h. f ist auf der

ganzen offenen Menge $D(H)$ algebraisch. Insbesondere muss man nicht mit unendlich vielen verschiedenen Darstellungen arbeiten, sondern man kann sich auf die (endlich vielen) Darstellungen G_i/H_i zu einer Überdeckung $U = \bigcup_{i \in I} D(H_i)$ beschränken.

Bei $K = \mathbb{C}$ ist eine algebraische Funktion auch stetig bezüglich der metrischen Topologie, und bei $R = \mathbb{C}[X_1, \dots, X_n]$ ist sie *holomorph*.

Beispiel 14.3. Sei $V = V(WX - ZY) \subseteq \mathbb{A}_K^4$ und sei $U = D(X, Y) = D(X) \cup D(Y) \subset V$ die durch X und Y definierte Zariski-offene Menge. Auf U ist die durch

$$f = \frac{Z}{X} = \frac{W}{Y}$$

definierte Funktion algebraisch. Die beiden rationalen Darstellungen liefern offenbar eine algebraische Funktion auf den beiden offenen Teilmengen $D(X)$ und $D(Y)$. Damit es eine Funktion auf U definiert muss sichergestellt werden, dass die Brüche auf dem Durchschnitt, also auf $D(X) \cap D(Y) = D(XY)$, die gleichen Funktionswerte haben. Sei also $Q = (w, x, y, z) \in D(XY)$, $Q \in V$. D.h. $x, y \neq 0$ und $wx = zy$. Dann ist aber sofort

$$\frac{Z}{X}(Q) = \frac{z}{x} = \frac{w}{y} = \frac{W}{Y}(Q).$$

Lemma 14.4. Sei K ein algebraisch abgeschlossener Körper, R eine K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Es sei $U \subseteq V$ eine Zariski-offene Menge. Dann bildet die Menge der algebraischen Funktionen auf U einen Unterring (und zwar eine K -Unteralgebra) des Rings der Funktionen von U nach K (wobei die Operationen in K ausgeführt werden).

Beweis. Wir müssen zeigen, dass die konstante Nullfunktion und die konstante Einsfunktion auf U , das Negative einer algebraischen Funktion, und die Summe und das Produkt von zwei algebraischen Funktionen auf U wieder algebraisch sind. Wir beschränken uns auf die Summe der algebraischen Funktionen f_1 und f_2 . Sei $P \in U$ ein Punkt. Nach Voraussetzung gibt es Elemente $G_1, H_1, G_2, H_2 \in R$ mit

$$f_1(Q) = \frac{G_1(Q)}{H_1(Q)} \text{ für alle } Q \in D(H_1) \subseteq U, P \in D(H_1),$$

und

$$f_2(Q) = \frac{G_2(Q)}{H_2(Q)} \text{ für alle } Q \in D(H_2) \subseteq U, P \in D(H_2).$$

Sei $H := H_1 H_2$. Dann ist $P \in D(H) = D(H_1) \cap D(H_2) \subseteq U$. Für einen beliebigen Punkt $Q \in D(H)$ ist dann

$$\begin{aligned} (f_1 + f_2)(Q) &= f_1(Q) + f_2(Q) \\ &= \frac{G_1(Q)}{H_1(Q)} + \frac{G_2(Q)}{H_2(Q)} \\ &= \frac{G_1(Q)H_2(Q) + G_2(Q)H_1(Q)}{H_1(Q)H_2(Q)} \\ &= \frac{(G_1H_2 + G_2H_1)(Q)}{(H_1H_2)(Q)}, \end{aligned}$$

was eine polynomiale Darstellung der Summenfunktion in der Zariski-offenen Umgebung $D(H)$ des Punktes P ergibt. \square

Definition 14.5. Sei K ein algebraisch abgeschlossener Körper, R eine K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Sei $U \subseteq V$ eine Zariski-offene Menge. Dann bezeichnet man mit

$$\Gamma(U, \mathcal{O}) = \{f : U \longrightarrow K : f \text{ ist algebraisch}\}$$

den *Ring der algebraischen Funktionen auf U* . Man bezeichnet ihn auch als *Strukturring zu U* oder als *Schnitttring zu U* .

Aufgrund von Lemma 14.4 handelt es sich in der Tat um einen Ring. Das Symbol \mathcal{O} (sprich „ \mathcal{O} “) bezeichnet die sogenannte *Strukturgarbe*.

Lemma 14.6. Sei K ein algebraisch abgeschlossener Körper, R eine K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Es seien $U_1 \subseteq U_2$ offene Teilmengen von V . Dann gibt es einen natürlichen K -Algebra-Homomorphismus

$$\Gamma(U_2, \mathcal{O}) \longrightarrow \Gamma(U_1, \mathcal{O}).$$

Beweis. Die Funktion $f : U_2 \rightarrow K$ liefert sofort durch Einschränkung eine auf U_1 definierte Funktion. Die lokal-algebraische Beschreibung, die für f an jedem Punkt $P \in U_2$ vorliegt, kann direkt auf der kleineren Teilmenge U_1 interpretiert werden. \square

Die im vorstehenden Lemma beschriebene Abbildung heißt *Restriktionsabbildung* oder *Einschränkungsabbildung*.

Lemma 14.7. Sei K ein algebraisch abgeschlossener Körper, R eine K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Es sei $F \in R$ und $U \subseteq D(F) \subseteq V$ eine offene Menge. Dann ist es egal, ob man $\Gamma(U, \mathcal{O})$ mit Bezug auf V oder mit Bezug auf $D(F) = K\text{-Spek}(R_F)$ definiert.

Beweis. Natürlich hängen die stetigen Funktionen auf U nur von U selbst ab, nicht von einem umgebenden Raum. Wir müssen zeigen, dass die lokal-algebraische Bedingung ebenfalls nur von U abhängt. Sei $P \in U$. Eine Beschreibung

$$\varphi = \frac{G}{H} \text{ auf } D(H) \text{ mit } P \in D(H) \text{ und mit } G, H \in R$$

liefert sofort eine Beschreibung als Bruch auf $D(HF)$, da man ja H, G sofort in R_F auffassen kann.

Es liege nun umgekehrt eine Bruchdarstellung

$$\varphi = \frac{\tilde{G}}{\tilde{H}} \text{ auf } D(\tilde{H}) \text{ mit } P \in D(\tilde{H}) \text{ und mit } \tilde{G}, \tilde{H} \in R_F$$

vor. Es sei $\tilde{G} = G/F^r$ und $\tilde{H} = H/F^s$. Dann gilt für jeden Punkt $Q \in D(HF)$ die Gleichheit

$$\varphi(Q) = \frac{\tilde{G}(Q)}{\tilde{H}(Q)} = \frac{G(Q)/F^r(Q)}{H(Q)/F^s(Q)} = \frac{G(Q)F^s(Q)}{H(Q)F^r(Q)}.$$

Dabei haben wir im letzten Schritt mit F^{r+s} erweitert. In der letzten Darstellung sind Zähler und Nenner aus R , und es ist $HF^r(P) \neq 0$, also ist $D(HF^r)$ eine offene Umgebung von P . \square

Lemma 14.8. *Sei K ein algebraisch abgeschlossener Körper, R eine K -Algebra von endlichem Typ und sei $V = K - \text{Spek}(R)$ das K -Spektrum von R . Es sei $U \subseteq V$ eine Zariski-offene Menge, $P \in U$ ein Punkt und es sei $f : U \rightarrow K$ eine algebraische Funktion, für die es die beiden rationalen Darstellungen*

$$\frac{G_1}{H_1} \text{ und } \frac{G_2}{H_2}$$

gebe mit $G_1, H_1, G_2, H_2 \in R$ und mit $P \in D(H_1), D(H_2) \subseteq U$. Dann gibt es ein $r \in \mathbb{N}$ mit

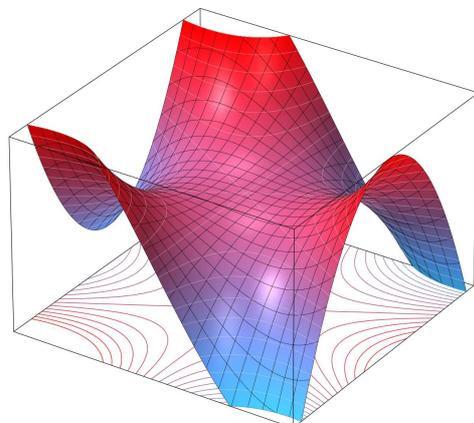
$$H_1^r H_2^r (G_1 H_2 - G_2 H_1)^r = 0 \text{ in } R.$$

Ist R reduziert, so gilt sogar $H_1 H_2 (G_1 H_2 - G_2 H_1) = 0$.

Beweis. Wir betrachten das Element $F = H_1 H_2 (G_1 H_2 - G_2 H_1)$ auf V und behaupten, dass dies die Nullfunktion induziert. Sei $Q \in V$. Bei $H_1(Q) = 0$ oder $H_2(Q) = 0$ ist $F(Q) = 0$, sei also $H_1(Q), H_2(Q) \neq 0$ vorausgesetzt. Dann ist $Q \in D(H_1) \cap D(H_2)$, und dort gelten die beiden rationalen Darstellungen für f , nämlich

$$\frac{G_1(Q)}{H_1(Q)} = f(Q) = \frac{G_2(Q)}{H_2(Q)}.$$

Daraus folgt $G_1(Q)H_2(Q) = G_2(Q)H_1(Q)$ und somit ist die Differenz null. Insgesamt ist also F die Nullfunktion auf V und daher gibt es nach dem Hilbertschen Nullstellensatz ein r mit $F^r = 0$. \square



Der Graph einer globalen Funktion auf \mathbb{A}_K^2 .

Satz 14.9. Sei K ein algebraisch abgeschlossener Körper, R eine reduzierte K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Dann ist

$$\Gamma(V, \mathcal{O}) = R.$$

Beweis. Ein Element $F \in R$ liefert direkt eine algebraische Funktion auf ganz V , was einen K -Algebra Homomorphismus

$$R \longrightarrow \Gamma(V, \mathcal{O})$$

ergibt. Wenn dabei F an jedem Punkt die Nullfunktion induziert, so ist nach Korollar 11.4 und wegen der Reduziertheit auch $F = 0$. D.h. die Abbildung ist injektiv.

Sei nun $f : V \rightarrow K$ eine algebraische Funktion. Dann gibt es zu jedem Punkt $P \in V$ zwei Elemente $G_P, H_P \in R$ mit $P \in D(H_P)$ und mit $f = \frac{G_P}{H_P}$ auf $D(H_P)$. Die $D(H_P)$ bilden eine offene Überdeckung von V und das bedeutet nach Korollar 11.5, dass die H_P in R das Einheitsideal erzeugen. Dann gibt es aber auch eine endliche Auswahl davon, die das Einheitsideal erzeugen, sagen wir $H_i = H_{P_i}$, $i = 1, \dots, m$. Dann wiederum überdecken diese $D(H_i)$, $i = 1, \dots, m$, ganz V .

Auf den Durchschnitten $D(H_i H_j) = D(H_i) \cap D(H_j)$ haben wir die Identitäten

$$f(Q) = \frac{G_i(Q)}{H_i(Q)} = \frac{G_j(Q)}{H_j(Q)} \text{ für alle } Q \in D(H_i H_j).$$

Daraus folgt nach Lemma 14.8 und der Reduziertheit, dass

$$H_i H_j G_i H_j = H_i H_j G_j H_i$$

in R gilt. Wir ersetzen H_i durch H_i^2 und G_i durch $G_i H_i$. Dann ist nach wie vor G_i/H_i eine lokale Beschreibung für f , und die letzte Bedingung vereinfacht sich zu $H_i G_j = H_j G_i$.

Da die H_i das Einheitsideal erzeugen, gibt es Elemente $A_i \in R$ mit

$$\sum_{i=1}^m A_i H_i = 1$$

in R . Wir behaupten, dass das Element

$$F = \sum_{i=1}^m A_i G_i$$

auf ganz V die Funktion f induziert. Dazu sei $Q \in V$ ein beliebiger Punkt, und zwar sei ohne Einschränkung $Q \in D(H_1)$. Dann ist

$$\begin{aligned} f(Q) &= \frac{G_1(Q)}{H_1(Q)} \\ &= \frac{G_1(Q)}{H_1(Q)} \left(\sum_{i=1}^m A_i H_i(Q) \right) \\ &= \sum_{i=1}^m A_i(Q) \frac{G_1(Q) H_i(Q)}{H_1(Q)} \\ &= \sum_{i=1}^m A_i(Q) G_i(Q) \\ &= F(Q). \end{aligned}$$

□

Korollar 14.10. Sei K ein algebraisch abgeschlossener Körper, R eine reduzierte K -Algebra von endlichem Typ und sei $V = K\text{-Spek}(R)$ das K -Spektrum von R . Es sei $F \in R$ mit zugehöriger offener Menge $D(F) \subseteq V$. Dann ist

$$\Gamma(D(F), \mathcal{O}) = R_F.$$

Beweis. Dies folgt direkt aus Lemma 14.7 und Satz 14.9. □

15. VORLESUNG

Definition 15.1. Sei K ein algebraisch abgeschlossener Körper und sei R eine K -Algebra von endlichem Typ. Dann nennt man das K -Spektrum $V = K\text{-Spek}(R)$ von R , wobei alle Zariski-offenen Mengen $U \subseteq V$ mit dem Ring der algebraischen Funktionen $\Gamma(U, \mathcal{O})$ versehen sei, eine *affine Varietät*.

Eine offene Teilmenge einer affinen Varietät, wobei ebenfalls alle offenen Mengen mit den Strukturringen versehen sei, nennt man eine *quasiaffine Varietät*. Eine quasiaffine Varietät wird überdeckt durch endlich viele offene Mengen der Form $D(f)$, welche selbst affine Varietäten sind. Manche Autoren nennen nur irreduzible K -Spektren eine Varietät. Satz 14.9 sichert, dass man beim Übergang von R zu $V = K\text{-Spek}(R)$ nichts verliert, da man den Ring R als $\Gamma(V, \mathcal{O})$ zurückgewinnen kann. Dies ist aus dem topologischen Raum allein nicht möglich.

15.1. Lokale Ringe.

Zu einem gegebenen Punkt P in einem K -Spektrum interessieren wir uns für die Menge aller algebraischen Funktionen, die in P definiert sind und in einer gewissen Umgebung von P eine rationale Darstellung besitzen. Dabei sind die algebraischen Funktionen auf unterschiedlichen Umgebungen definiert, und es gibt keine kleinste Umgebung, auf der alle in P definierten algebraischen Funktionen definiert sind. Es liegt ein System von Ringen $\Gamma(U, \mathcal{O})$, $P \in U$, vor, das wir geometrisch und algebraisch verstehen wollen. Es stellt sich heraus, dass man diesem System einen sinnvollen Limes („direkter Limes“ oder „Kolimes“) zuordnen kann, und dass dieser mit der Lokalisierung $R_{\mathfrak{m}}$ an dem zu P gehörenden maximalen Ideal \mathfrak{m} übereinstimmt. Wir führen zunächst die algebraischen Begriffe ein.

Definition 15.2. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Dazu ist äquivalent, dass das Komplement der Einheitengruppe von R abgeschlossen unter der Addition ist. Die einfachsten lokalen Ringe sind die Körper. Zu jedem lokalen Ring R gehört der Restklassenkörper R/\mathfrak{m} , den man den *Restekörper* von R nennt. Wir werden bald sehen, dass es zu jedem Punkt in einem K -Spektrum einen zugehörigen lokalen Ring gibt, der das „lokale Aussehen“ der Varietät in dem Punkt algebraisch beschreibt.

Definition 15.3. Sei R ein kommutativer Ring und sei \mathfrak{p} ein Primideal. Dann nennt man die Nenneraufnahme an $S = R - \mathfrak{p}$ die *Lokalisierung* von R an \mathfrak{p} . Man schreibt dafür $R_{\mathfrak{p}}$. Es ist also

$$R_{\mathfrak{p}} := \left\{ \frac{f}{g} : f \in R, g \notin \mathfrak{p} \right\}.$$

Der folgende Satz zeigt, dass diese Namensgebung Sinn macht.

Satz 15.4. Sei R ein kommutativer Ring und sei \mathfrak{p} ein Primideal in R . Dann ist die Lokalisierung $R_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal

$$\mathfrak{p}R_{\mathfrak{p}} := \left\{ \frac{f}{g} : g \notin \mathfrak{p}, f \in \mathfrak{p} \right\}.$$

Beweis. Die angegebene Menge ist in der Tat ein Ideal in der Lokalisierung $R_{\mathfrak{p}} = \left\{ \frac{f}{g} : f \in R, g \notin \mathfrak{p} \right\}$. Wir zeigen, dass das Komplement nur aus Einheiten besteht, so dass es sich um ein maximales Ideal handeln muss. Sei also $q = \frac{f}{g} \in R_{\mathfrak{p}}$, aber nicht in $\mathfrak{p}R_{\mathfrak{p}}$. Dann sind $f, g \notin \mathfrak{p}$ und somit gehört der inverse Bruch $\frac{g}{f}$ ebenfalls zur Lokalisierung. \square

15.2. Quotientenkörper und Funktionenkörper.

Wenn R ein Integritätsbereich ist, so ist der Quotientenkörper eine Lokalisierung, und zwar am Primideal 0 . Wir zeigen jetzt, dass für die zugehörige

irreduzible affine Varietät $K\text{-Spek}(R)$ jede algebraische Funktion in natürlicher Weise im Quotientenkörper liegt.

Lemma 15.5. *Sei K ein algebraisch abgeschlossener Körper, R eine integrale K -Algebra von endlichem Typ, und sei $U \subseteq K\text{-Spek}(R)$ eine offene nicht-leere Teilmenge. Dann gibt es einen eindeutig bestimmten injektiven R -Algebra Homomorphismus*

$$\Gamma(U, \mathcal{O}) \longrightarrow Q(R).$$

Insbesondere ist jede auf einer nicht-leeren offenen Menge $U \subseteq K\text{-Spek}(R)$ definierte algebraische Funktion ein Element im Quotientenkörper $Q(R)$.

Beweis. Sei $P \in U$ ein Punkt und die algebraische Funktion f sei in einer Umgebung von P durch $f = G/H$ gegeben, $G, H \in R$, $H \neq 0$. Dann kann man G/H sofort als Element im Quotientenkörper auffassen. Sei $Q \in U$ ein anderer Punkt mit einer Darstellung $f = G'/H'$. Nach Lemma 14.8 und da ein Integritätsbereich vorliegt ist $GH' = G'H$ in R . Daher ist der Quotient im Quotientenkörper wohldefiniert. Die Abbildung ist dann offensichtlich ein Ringhomomorphismus und das Diagramm

$$\begin{array}{ccc} R & & \\ \downarrow & \searrow & \\ \Gamma(U, \mathcal{O}) & \longrightarrow & Q(R) \end{array}$$

kommutiert. Die Abbildung ist auch durch die Eigenschaften eindeutig festgelegt, da die algebraischen Funktionen, die Elementen aus R entsprechen, auf die zugehörigen Elemente im Quotientenkörper gehen müssen. Damit sind bereits die Bilder der Brüche festgelegt.

Die Injektivität ergibt sich daraus, dass aus $G/H = 0$ im Quotientenkörper sofort $G = 0$ folgt, und damit ist auch die zugehörige Funktion auf $D(H)$ die Nullfunktion. Wenn es eine weitere Darstellung $G/H = G'/H'$ gibt, so folgt wiederum $G' = 0$ und erneut ist das die Nullfunktion. \square

Aus der Eindeutigkeit folgt ebenfalls sofort, dass für zwei offene Mengen $U \subseteq U'$ das Diagramm

$$\begin{array}{ccc} \Gamma(U', \mathcal{O}) & & \\ \downarrow & \searrow & \\ \Gamma(U, \mathcal{O}) & \longrightarrow & Q(R) \end{array}$$

kommutiert, wobei links der Restriktionshomomorphismus steht. Wir werden im integren Fall von nun an eine algebraische Funktion mit dem zugehörigen Element im Quotientenkörper identifizieren.

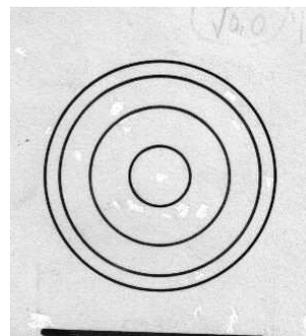
15.3. Topologische Filter und ihre Halme.

Das Ergebnis des letzten Abschnitts besagt, dass man den Quotientenkörper gewinnen kann als eine geordnete Vereinigung aller Schnittringe $\Gamma(U, \mathcal{O})$ über

alle nichtleeren offenen Mengen. Eine ähnliche Konstruktion kann man generell für sinnvoll strukturierte Systeme von offenen Mengen durchführen. Dazu benötigen wir den Begriff des Filters.

Definition 15.6. Sei X ein topologischer Raum. Ein System F aus offenen Teilmengen von X heißt *Filter*, wenn folgende Eigenschaften gelten (U, V seien offen).

- (1) $X \in F$.
- (2) Mit $U \in F$ und $U \subseteq V$ ist auch $V \in F$.
- (3) Mit $U \in F$ und $V \in F$ ist auch $U \cap V \in F$.



Schematische Darstellung eines Umgebungsfilters

Definition 15.7. Sei X ein topologischer Raum und sei $M \subseteq X$ eine Teilmenge. Dann nennt man das System

$$U(M) = \{U \subseteq X \text{ offen} : M \subseteq U\}$$

den *Umgebungsfilter* von M .

Es handelt sich dabei offensichtlich um einen topologischen Filter. Insbesondere gibt es zu einem einzelnen Punkt $P \in X$ den Umgebungsfilter $U(P)$. Der Umgebungsfilter fasst alle offenen Umgebungen des Punktes zusammen. Wenn zwei offene Umgebungen U_1, U_2 von P gegeben sind zusammen mit zwei algebraischen Funktionen

$$f_1 \in \Gamma(U_1, \mathcal{O}) \text{ und } f_2 \in \Gamma(U_2, \mathcal{O}),$$

so hat die Summe $f_1 + f_2$ (ebensowenig das Produkt) zunächst keinen Sinn, da die Definitionsbereiche verschieden sind. Im integren Fall kann man beide Funktionen als Elemente im Quotientenkörper auffassen und dort addieren. Man kann aber auch zum Durchschnitt $U_1 \cap U_2$ (der ebenfalls eine offene Umgebung des Punktes ist) übergehen und dort die Einschränkungen der beiden Funktionen addieren. Wichtig ist hierbei die Eigenschaft eines Filters, dass man zu je zwei offenen Mengen auch den Durchschnitt im Filter hat mit den zugehörigen Inklusionen

$$U_1 \cap U_2 \subseteq U_1, U_2$$

und den zugehörigen Restriktionen

$$\Gamma(U_1, \mathcal{O}), \Gamma(U_2, \mathcal{O}) \longrightarrow \Gamma(U_1 \cap U_2, \mathcal{O}).$$

Diese Beobachtung wird durch den Begriff der gerichteten Menge und des gerichteten Systems präzisiert.

Definition 15.8. Eine geordnete Menge (I, \preceq) heißt *gerichtet geordnet* oder *gerichtet*, wenn es zu jedem $i, j \in I$ ein $k \in I$ gibt mit $i, j \preceq k$.

Wir fassen einen topologischen Filter als eine durch die Inklusion geordnete Menge auf. Aus der Durchschnittseigenschaft eines Filters ergibt sich, dass eine gerichtete Menge vorliegt (Es ist dabei „ $\preceq = \supseteq$ “).

Definition 15.9. Sei (I, \preceq) eine geordnete Indexmenge. Eine Familie

$$M_i, i \in I,$$

von Mengen nennt man ein *geordnetes System von Mengen*, wenn folgende Eigenschaften erfüllt sind.

- (1) Zu $i \preceq j$ gibt es eine Abbildung $\varphi_{ij} : M_i \rightarrow M_j$.
- (2) Zu $i \preceq j$ und $j \preceq k$ ist $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$.

Ist die Indexmenge zusätzlich gerichtet, so spricht man von einem *gerichteten System von Mengen*.

Wenn die beteiligten Mengen M_i allesamt Gruppen (Ringe) sind und alle Abbildungen zwischen ihnen Gruppenhomomorphismen (Ringhomomorphismen), so spricht man von einem geordneten bzw. gerichteten System von Gruppen (Ringern).

Definition 15.10. Es sei $M_i, i \in I$, ein gerichtetes System von Mengen. Dann nennt man

$$\operatorname{colim}_{i \in I} M_i = \bigsqcup_{i \in I} M_i / \sim$$

den *Kolimes* (oder *induktiven Limes*) des Systems. Dabei bezeichnet \sim die Äquivalenzrelation, bei der zwei Elemente $m \in M_i$ und $n \in M_j$ als äquivalent erklärt werden, wenn es ein $k \in I$ mit $i, j \preceq k$ und mit

$$\varphi_{ik}(m) = \varphi_{jk}(n)$$

gibt.

Bei dieser Definition ist insbesondere ein Element $s_i \in M_i$ äquivalent zu seinem Bild $\varphi_{ik}(s_i) \in M_k$ für alle $i \preceq k$. Wenn ein gerichtetes System von Gruppen (Ringern) vorliegt, so kann man auf dem soeben eingeführten Kolimes der Mengen auch eine Gruppenstruktur (Ringstruktur) definieren. Dies beruht darauf, dass zwei Elemente in diesem Kolimes, die durch $s_i \in M_i$ und $s_j \in M_j$ repräsentiert seien, mit ihren Bildern in M_k ($i, j \preceq k$) identifiziert werden können. Dann kann man dort die Gruppenoperation erklären. Siehe Aufgabe 15.7. Unser Hauptbeispiel für ein gerichtetes System ist das durch einen topologischen Filter gerichtete System der Ringe

$$\Gamma(U, \mathcal{O}), U \in F.$$

Der zugehörige Kolimes über dieses System bekommt einen eigenen Namen.

Definition 15.11. Sei (V, \mathcal{O}) eine quasiaffine Varietät und sei F ein topologischer Filter in V . Dann nennt man

$$\mathcal{O}_F = \operatorname{colim}_{U \in F} \Gamma(U, \mathcal{O})$$

den *Halm von \mathcal{O} in F* .

Den Halm im Umgebungfilter eines Punktes P nennt man auch den Halm in P und schreibt dafür \mathcal{O}_P .

Satz 15.12. (*Halm und Lokalisierung*) Sei R eine reduzierte kommutative Algebra von endlichem Typ über einem algebraisch abgeschlossenen Körper K . Es sei $P \in K\text{-Spek}(R)$ ein Punkt im K -Spektrum mit zugehörigem maximalen Ideal $\mathfrak{m} \subseteq R$. Dann gibt es eine natürliche Isomorphie (von R -Algebren)

$$R_{\mathfrak{m}} \longrightarrow \mathcal{O}_P.$$

Beweis. Der Halm \mathcal{O}_P hat eine eindeutige Struktur als R -Algebra, da ja die Gesamtmenge zum Filter gehört. Sei $F \in R$, $F \notin \mathfrak{m}$. Dann ist $1/F$ auf der offenen Umgebung $D(F)$ von P definiert. Dabei gilt dort $F \cdot 1/F = 1$, so dass F in dieser Menge und damit auch im Kolimes eine Einheit ist. Nach der universellen Eigenschaft der Nenneraufnahme gibt es also einen R -Algebra Homomorphismus

$$R_{\mathfrak{m}} \longrightarrow \mathcal{O}_P,$$

den wir als bijektiv nachweisen müssen. Sei zuerst $f \in \mathcal{O}_P$. Dieses Element ist repräsentiert durch eine algebraische Funktion $f \in \Gamma(U, \mathcal{O})$ mit $P \in U$. Insbesondere gibt es eine rationale Darstellung für f in P , d.h. $f = G/H$ auf $D(H)$ und $P \in D(H)$. Daher ist G/H ein Element in der Lokalisierung $R_{\mathfrak{m}}$, und dieses wird auf f geschickt.

Zur Injektivität sei G/H gegeben mit $H \notin \mathfrak{m}$ und vorausgesetzt, dass es als Element im Halm null ist. Dies bedeutet, dass es eine offene Umgebung U von P gibt, wo G/H die Nullfunktion ist. Wir können annehmen, dass diese offene Menge die Form $P \in D(H') \subseteq D(H)$ hat. Wegen Korollar 14.11 gibt es dann auch eine Beschreibung $G/H = G'/H' = 0$. Das heisst nach Lemma 14.8, dass $HH'H'G = 0$ in R ist. Dann ist auch $G/H = 0$ in der Lokalisierung. \square

Lemma 15.13. Sei K ein algebraisch abgeschlossener Körper und sei R eine integrale K -Algebra von endlichem Typ. Sei $U \subseteq K\text{-Spek}(R)$ eine offene Teilmenge. Dann ist

$$\Gamma(U, \mathcal{O}) = \bigcap_{P \in U} \mathcal{O}_P$$

(dabei wird der Durchschnitt im Quotientenkörper genommen).

Beweis. Zu jedem Punkt $P \in U$ gibt es Ringhomomorphismen $\Gamma(U, \mathcal{O}) \rightarrow \mathcal{O}_P$ und $\mathcal{O}_P \rightarrow Q(R)$, die jeweils injektiv sind. Damit gibt es auch einen injektiven Ringhomomorphismus

$$\Gamma(U, \mathcal{O}) \longrightarrow \bigcap_{P \in U} \mathcal{O}_P.$$

Sei $f \in Q(R)$ ein Element im Durchschnitt rechts. Dann gibt es zu jedem Punkt $P \in U$ eine Darstellung $f = G/H$ mit $P \in D(H) \subseteq U$. Dies bedeutet direkt, dass f eine algebraische Funktion auf U ist. \square

Definition 15.14. Sei V eine irreduzible quasiaffine Varietät. Dann ist der Halm von \mathcal{O} über alle nichtleeren offenen Mengen ein Körper, den man den *Funktionskörper* von V nennt.

16. VORLESUNG

16.1. Irreduzible Filter.

Wir haben in der letzten Vorlesung gesehen, dass zu einem Punkt P in einem K -Spektrum $K - \text{Spek}(R)$ der Umgebungsfilter gehört und dass der Halm in diesem Filter gleich der Lokalisierung von R an dem zugehörigen maximalen Ideal ist. Ebenfalls haben wir gesehen, dass bei integrem R der Halm über alle nichtleeren offenen Mengen den Quotientenkörper von R liefert, der wiederum die Lokalisierung am Nullideal ist. Dieser Zusammenhang wird mit dem Begriff des irreduziblen Filters verallgemeinert.



Einen Filter kann man mit dem, was in ihm hängen bleibt, identifizieren.

Definition 16.1. Ein topologischer Filter F heißt *irreduzibel*, wenn $\emptyset \notin F$ und folgendes gilt: Sind U, V zwei offene Mengen mit $U \cup V \in F$, so ist $U \in F$ oder $V \in F$.

Für Zariski-Filter (also topologische Filter in der Zariski-Topologie) gilt folgender Zusammenhang.

Satz 16.2. Sei K ein algebraisch abgeschlossener Körper und sei R eine kommutative K -Algebra von endlichem Typ mit K -Spektrum $X = K - \text{Spek}(R)$. Dann entsprechen sich folgende Objekte.

- (1) Primideale in R .
- (2) Irreduzible abgeschlossene Teilmengen von X .
- (3) Irreduzible Filter in X .

Dabei entspricht der irreduziblen abgeschlossenen Teilmenge $Y \subseteq X$ der Filter

$$F(Y) = \{U \subseteq X : U \cap Y \neq \emptyset\}.$$

Der Halm der Strukturgarbe an diesem Filter ist die Lokalisierung $R_{\mathfrak{p}}$, wobei \mathfrak{p} das zugehörige Primideal bezeichnet.

Beweis. Die Korrespondenz zwischen Primidealen und abgeschlossenen irreduziblen Teilmengen (zu einem Primideal \mathfrak{p} gehört die irreduzible abgeschlossene Teilmenge $V(\mathfrak{p})$) ist bekannt (siehe Lemma 4.3 und Proposition 11.10(3)). Die angegebene Konstruktion zu einer irreduziblen abgeschlossenen Menge Y liefert in der Tat einen irreduziblen Filter. Dabei ist die Irreduzibilität trivial, zu zeigen ist lediglich die Durchschnittseigenschaft eines

Filters. Seien $U, V \in F = F(Y)$, so dass also die Durchschnitte $Y \cap U$ und $Y \cap V$ nicht leer sind. Dann ist aber wegen der Irreduzibilität von Y auch der Durchschnitt

$$(Y \cap U) \cap (Y \cap V) = Y \cap (U \cap V)$$

nicht leer und daher ist $U \cap V \in F$.

Sei nun F irgendein irreduzibler topologischer Filter. Wir behaupten, dass das Komplement von

$$S = \{f \in R : D(f) \in F\}$$

ein Primideal ist. Es ist sofort ein saturiertes multiplikatives System. Es bleibt zu zeigen, dass das Komplement additiv abgeschlossen ist. Seien dazu $h, g \in R$ mit $g + h \in S$, also $D(g + h) \in F$. Dann gehört erst recht

$$D(g) \cup D(h) = D(g, h) \supseteq D(g + h)$$

zu F und wegen der Irreduzibilität von F ist $D(g) \in F$ oder $D(h) \in F$, woraus sich $g \in S$ oder $h \in S$ ergibt.

Diese drei Zuordnungen hintereinandergenommen führen dabei immer wieder zum Ausgangsobjekt zurück. Dazu muss man lediglich beachten, dass ein irreduzibler Zariski-Filter durch offene Mengen der Form $D(f)$ erzeugt wird, siehe Aufgabe 16.1.

Der Zusatz ist ein Spezialfall von Aufgabe 15.10. □

Den zu einer irreduziblen abgeschlossenen Menge gehörenden Filter nennen wir auch den zugehörigen *generischen Filter* zu Y und den Halm davon den *generischen Halm* zu Y . Ein Spezialfall der Korrespondenz von Satz 16.2 ist die Beziehung zwischen minimalen Primidealen, irreduziblen Komponenten und Ultrafiltern. Auf der anderen Seite hat man die Korrespondenz zwischen maximalen Idealen, Punkten und Umgebungfiltern.

16.2. Morphismen zwischen Varietäten.

Definition 16.3. Seien X und Y zwei quasiaffine Varietäten und sei

$$\psi : Y \longrightarrow X$$

eine stetige Abbildung. Dann nennt man ψ einen *Morphismus* (von quasiaffinen Varietäten), wenn für jede offene Teilmenge $U \subseteq X$ und jede algebraische Funktion $f \in \Gamma(U, \mathcal{O})$ gilt, dass die zusammengesetzte Funktion

$$f \circ \psi : \psi^{-1}(U) \longrightarrow U \xrightarrow{f} \mathbb{A}_K^1$$

zu $\Gamma(\psi^{-1}(U), \mathcal{O})$ gehört.

Bemerkung 16.4. Ein Morphismus

$$\psi : Y \longrightarrow X$$

induziert also nach Definition zu jeder offenen Teilmenge $U \subseteq X$ einen Ringhomomorphismus

$$\tilde{\psi} : \Gamma(U, \mathcal{O}) \longrightarrow \Gamma(\psi^{-1}(U), \mathcal{O}).$$

Insbesondere gibt es einen *globalen Ringhomomorphismus*

$$\tilde{\psi} : \Gamma(X, \mathcal{O}) \longrightarrow \Gamma(Y, \mathcal{O}).$$

Sind $U_1 \subseteq U_2$ offene Teilmengen in Y , so liegt ein kommutatives Diagramm von stetigen Abbildungen (wobei die senkrechten Pfeile offene Inklusionen sind)

$$\begin{array}{ccc} \psi^{-1}(U_1) & \longrightarrow & U_1 \\ \downarrow & & \downarrow \\ \psi^{-1}(U_2) & \longrightarrow & U_2, \end{array}$$

das wiederum zu dem kommutativen Diagramm

$$\begin{array}{ccc} \Gamma(\psi^{-1}(U_1), \mathcal{O}) & \longleftarrow & \Gamma(U_1, \mathcal{O}) \\ \uparrow & & \uparrow \\ \Gamma(\psi^{-1}(U_2), \mathcal{O}) & \longleftarrow & \Gamma(U_2, \mathcal{O}) \end{array}$$

von Ringhomomorphismen führt.

Wir fassen einige einfache Eigenschaften von Morphismen zusammen

Proposition 16.5. *Sei K ein algebraisch abgeschlossener Körper, und seien U, X, Y, Z quasiaffine Varietäten. Dann gelten folgende Aussagen.*

- (1) *Eine offene Einbettung $U \subseteq X$ ist ein Morphismus.*
- (2) *Sind $\theta : Z \rightarrow Y$ und $\psi : Y \rightarrow X$ Morphismen, so ist auch die Verknüpfung $\psi \circ \theta$ ein Morphismus.*

Beweis. Das ist trivial. □

Wichtiger sind die folgenden Eigenschaften.

Satz 16.6. *Sei K ein algebraisch abgeschlossener Körper und seien R und S kommutative K -Algebren vom endlichen Typ mit zugehörigen K -Spektren $X = K\text{-Spek}(R)$ und $Y = K\text{-Spek}(S)$. Dann ist die durch einen Ringhomomorphismus $\varphi : R \rightarrow S$ induzierte Spektrumsabbildung*

$$\varphi^* : Y \longrightarrow X$$

ein Morphismus.

Beweis. Wir wissen bereits nach Satz 12.7, das

$$Y = K\text{-Spek}(S) \longrightarrow X = K\text{-Spek}(R)$$

eine stetige Abbildung ist. Sei $U \subseteq X$ eine offene Teilmenge und $V = (\varphi^*)^{-1}(U)$ das Urbild. Sei $f : U \rightarrow K$ eine algebraische Funktion mit der Hintereinanderschaltung $f \circ \varphi^* : V \rightarrow K$. Wir haben zu zeigen, dass diese Abbildung ebenfalls algebraisch ist. Sei dazu $P \in V$ ein Punkt mit dem

Bildpunkt $Q = \varphi^*(P)$. Sei $Q \in D(H) \subseteq U$ und $f = G/H$ auf $D(H)$ mit $G, H \in R$. Es ist

$$P \in (\varphi^*)^{-1}(D(H)) = D(\varphi(H)).$$

Wir behaupten, dass auf $D(\varphi(H))$ die Gleichheit $f \circ \varphi^* = \frac{\varphi(G)}{\varphi(H)}$ gilt. Dies folgt für $\tilde{P} \in D(\varphi(H))$ aus

$$f \circ \varphi^*(\tilde{P}) = f(\varphi^*(\tilde{P})) = \frac{G(\varphi^*(\tilde{P}))}{H(\varphi^*(\tilde{P}))} = \frac{(\varphi(G))(\tilde{P})}{(\varphi(H))(\tilde{P})}.$$

□

Bemerkung 16.7. In der Situation von Satz 16.6 ist der zu $U = D(f)$ gehörende Ringhomomorphismus die natürliche Abbildung

$$\Gamma(D(f), \mathcal{O}) \cong R_f \longrightarrow \Gamma((\varphi^*)^{-1}(D(f)), \mathcal{O}) = \Gamma(D(\varphi(f)), \mathcal{O}) = S_{\varphi(f)}.$$

Lemma 16.8. Sei U eine quasiaffine Varietät über einem algebraisch abgeschlossenen Körper K und sei $f \in \Gamma(U, \mathcal{O})$ eine algebraische Funktion. Dann definiert f einen Morphismus

$$f : U \longrightarrow \mathbb{A}_K^1 \cong K.$$

Beweis. Sei $U \subseteq K\text{-Spek}(R)$. Es sei $V = D(t) \subseteq \mathbb{A}_K^1$ eine offene Teilmenge und $W = f^{-1}(V) \subseteq U$ das Urbild davon. Sei

$$s = \frac{r}{t^n} \in \Gamma(V, \mathcal{O}) = K[T]_t$$

eine algebraische Funktion auf V . Wir müssen zeigen, dass die Verknüpfung $s \circ f$ eine algebraische Funktion auf W ist. Sei dazu $P \in W$ und sei $f = G/H$ eine Beschreibung der nach Voraussetzung algebraischen Funktion f in der Umgebung $D(H) \ni P$. Dann ist

$$s \circ f(P) = s(f(P)) = \frac{r}{t^n} \left(\frac{G}{H}(P) \right) = \frac{r(G(P)/H(P))}{(t(G(P)/H(P)))^n}.$$

Dabei ist der Nenner $(t(G(P)/H(P)))^n$ nicht null, da $f(P) \in D(t)$ ist, so dass dies eine rationale Darstellung ist. □

Satz 16.9. Sei U eine quasiaffine Varietät über einem algebraisch abgeschlossenen Körper, und zwar sei $U \subseteq K\text{-Spek}(R)$, wobei R eine kommutative K -Algebra von endlichem Typ über einem algebraisch abgeschlossenen Körper K sei. Dann gibt es eine natürliche Bijektion

$$\text{Mor}(U, \mathbb{A}_K^1) \longrightarrow \Gamma(U, \mathcal{O}), \psi \longmapsto \tilde{\psi}(T),$$

wobei T die Variable in $K[T] = \Gamma(\mathbb{A}_K^1, \mathcal{O})$ bezeichnet. Insbesondere sind Morphismen von U nach der affinen Geraden durch den globalen Ringhomomorphismus

$$\tilde{\psi} : \Gamma(\mathbb{A}_K^1, \mathcal{O}) = K[T] \longrightarrow \Gamma(U, \mathcal{O})$$

eindeutig bestimmt.

Beweis. Die Abbildung ist wohldefiniert und surjektiv. Ist nämlich eine globale algebraische Funktion $f \in \Gamma(U, \mathcal{O})$ gegeben, so ist zunächst $f : U \rightarrow K$. Die Variable T , die auf $K = \mathbb{A}_K^1$ der identischen Abbildung entspricht, wird unter (der Verknüpfung mit) f auf das Element $f \in \Gamma(U, \mathcal{O})$ abgebildet. Nach Lemma 16.8 ist f ein Morphismus.

Die Injektivität ergibt sich, da sowohl der Morphismus als auch die algebraische Funktion durch die zugrunde liegende stetige Abbildung eindeutig festgelegt sind. \square

Satz 16.10. *Sei U eine quasiaffine Varietät, und zwar sei $U \subseteq K\text{-Spek}(R)$, wobei R eine kommutative K -Algebra von endlichem Typ über einem algebraisch abgeschlossener Körper K sei. Es sei S eine weitere kommutative K -Algebra von endlichem Typ. Dann gibt es eine natürliche Bijektion*

$$\text{Mor}(U, K\text{-Spek}(S)) \longrightarrow \text{Hom}_K^{\text{alg}}(S, \Gamma(U, \mathcal{O})), \psi \longmapsto \tilde{\psi},$$

wobei $\tilde{\psi}$ den zu ψ gehörigen globalen Ringhomomorphismus bezeichnet.

Beweis. Die Abbildung ist wohldefiniert. Aus Satz 16.9 folgt, dass die Aussage für $S = K[T]$ richtig ist. Daraus ergibt sich, dass die Aussage für jeden Polynomring $K[T_1, \dots, T_n]$ richtig ist, da ein Morphismus nach \mathbb{A}_K^n durch seine Komponenten und ein K -Algebra Homomorphismus durch die Einsetzungen für T_i gegeben ist. Sei nun $S = K[T_1, \dots, T_n]/\mathfrak{a}$ und

$$K\text{-Spek}(S) \cong V(\mathfrak{a}) = V \subseteq \mathbb{A}_K^n.$$

Zu einem Morphismus $U \rightarrow K\text{-Spek}(S)$ ist die Verknüpfung mit der abgeschlossenen Einbettung in den affinen Raum ebenfalls ein Morphismus. D.h. es liegt ein kommutatives Diagramm

$$\begin{array}{ccc} \text{Mor}(U, K\text{-Spek}(S)) & \longrightarrow & \text{Hom}_K^{\text{alg}}(S, \Gamma(U, \mathcal{O})) \\ \downarrow & & \downarrow \\ \text{Mor}(U, \mathbb{A}_K^n) & \longrightarrow & \text{Hom}_K^{\text{alg}}(K[T_1, \dots, T_n], \Gamma(U, \mathcal{O})) \end{array},$$

vor, wobei die untere Abbildung bereits als Bijektion nachgewiesen wurde. Die vertikalen Abbildungen sind injektiv. Wir müssen daher zeigen, dass die untere Abbildung die oberen Teilmengen ineinander überführt.

Ein Morphismus $U \rightarrow \mathbb{A}_K^n$, der (als Abbildung) durch V faktorisiert, ist auch ein Morphismus nach V . Die Morphismuseigenschaft ist nur für offene Mengen der Form $D(H)$ zu überprüfen, $H \in S$. Sei $\tilde{H} \in K[T_1, \dots, T_n]$ ein Repräsentant für H . Dann ist $K[T_1, \dots, T_n]_{\tilde{H}} \rightarrow S_H$ surjektiv und damit wird jedes Element aus S_H auf eine algebraische Funktion abgebildet.

Auf der rechten Seite des Diagramms gehört eine Algebra-Homomorphismus genau dann zur oberen Menge, wenn \mathfrak{a} zum Kern gehört. Damit folgt die Aussage aus Aufgabe 16.14. \square

Beispiel 16.11. Wir betrachten den Standardkegel, der als abgeschlossene Teilmenge

$$V = V(X^2 + Y^2 - Z^2) \subseteq \mathbb{A}_K^3.$$

gegeben sei. Es sei $U = D(X, Z - Y) \subseteq \mathbb{A}_K^3$ die offene Teilmenge mit dem Schnitt $V \cap U = D(X, Z - Y)$ (in V), der eine offene Menge in V ist. Wir behaupten, dass der zugehörige Ringhomomorphismus

$$\Gamma(U, \mathcal{O}) \longrightarrow \Gamma(U \cap V, \mathcal{O})$$

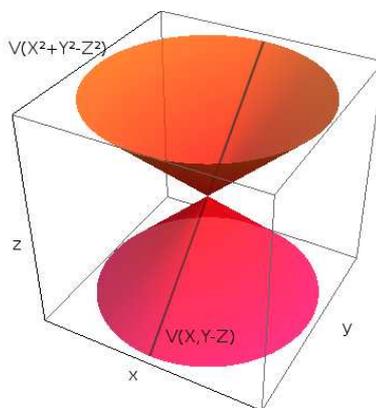
nicht surjektiv ist. Das liegt daran, dass rechts einfach der Polynomring in drei Variablen steht (vergleiche Aufgabe). Dagegen ergibt sich aus der Gleichung

$$X^2 = Z^2 - Y^2 = (Z - Y)(Z + Y),$$

dass es auf $U \cap V$ die algebraische Funktion

$$\frac{X}{Z - Y} = \frac{Z + Y}{X}$$

gibt, die nicht im Bild der Abbildung liegt, da es keine Funktion auf dem ganzen Kegel ist.

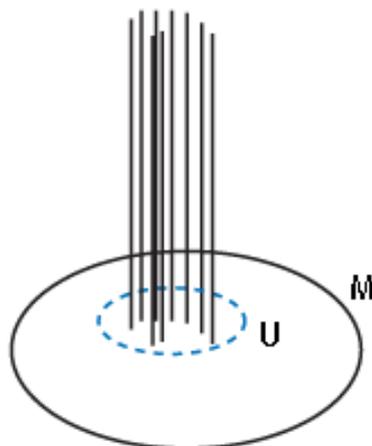


Nicht jede außerhalb der Gerade auf dem Kegel definierte Funktion lässt sich auf den affinen Raum ohne die Gerade fortsetzen.

Definition 16.12. Zu einem Morphismus $\psi : Y \rightarrow X$ zwischen affinen Varietäten bezeichnet man zu einem Punkt $P \in X$ das Urbild

$$\psi^{-1}(P) \subseteq Y$$

als die *Faser* über P . Als abgeschlossene Menge von Y ist sie selbst eine affine Varietät.



Die Fasern einer Abbildung (M ist der Zielbereich, der Definitionsbereich ist die Vereinigung aller Fasern; die Abbildung geht von oben nach unten).

17. VORLESUNG

17.1. Monoidringe.

Definition 17.1. Sei M ein kommutatives (additiv geschriebenes) Monoid und R ein kommutativer Ring. Dann wird der *Monoidring* $R[M]$ wie folgt konstruiert. Als R -Modul ist

$$R[M] = \bigoplus_{m \in M} R e_m,$$

d.h. $R[M]$ ist der freie Modul mit Basis e_m , $m \in M$. Die Multiplikation wird auf den Basiselementen durch

$$e_m \cdot e_k := e_{m+k}$$

definiert und auf ganz A distributiv fortgesetzt. Dabei definiert das neutrale Element $0 \in M$ das neutrale Element $1 = e_0$ der Multiplikation.

Bemerkung 17.2. (Erste Eigenschaften von Monoidringen) Ein Element in einem Monoidring lässt sich eindeutig schreiben als

$$f = \sum_{m \in \tilde{M}} a_m e_m,$$

wobei $\tilde{M} \subseteq M$ eine endliche Teilmenge ist und $a_m \in R$. Addiert wird komponentenweise und die Multiplikation ist explizit gegeben durch

$$f \cdot g = \left(\sum_{m \in \tilde{M}} a_m e_m \right) \left(\sum_{k \in \tilde{M}} b_k e_k \right) = \sum_{\ell \in M} \left(\sum_{m+k=\ell, m \in \tilde{M}, k \in \tilde{M}} a_m b_k \right) e_\ell.$$

Dies ist gemeint mit distributiver Fortsetzung. Die Menge der ℓ , über die hier summiert wird, ist endlich, und auch die inneren Summen sind jeweils endlich.

Es ist üblich, statt e_m suggestiver X^m zu schreiben, wobei X ein Symbol ist, das an eine Variable erinnern soll. Die Multiplikationsregel $X^m X^k = X^{m+k}$ erinnert dann an die entsprechende Regel für Polynomringe. In der Tat sind Polynomringe Spezialfälle von Monoidringen, und diese Notation stammt von dort. Auch ein exakter Beweis, dass in der Tat ein Ring mit assoziativer und distributiver Multiplikation vorliegt, funktioniert wie im Fall von Polynomringen. Meistens schreibt man ein Element einfach als $\sum_{m \in M} a_m X^m$, wobei fast alle $a_m = 0$ sind. Elemente der Form X^m nennt man *Monome*. Die Abbildung $M \rightarrow R[M]$, $m \mapsto X^m$, ist ein Monoidhomomorphismus, wobei rechts die multiplikative Monoidstruktur des Monoidringes genommen wird.

Ein Monoidring ist in natürlicher Weise eine R -Algebra, und zwar sind die Elemente f aus R aufgefasst in $R[M]$ gleich $f = f \cdot 1 = fX^0$. Man nennt daher auch R den Grundring des Monoidringes. Monoidringe sind bereits für Grundkörper interessant.

Beispiel 17.3. (Polynomring als Monoidring) Sei n eine natürliche Zahl und $M = \mathbb{N}^n$ das n -fache direkte Produkt der natürlichen Zahlen. Ein Element $k \in \mathbb{N}^n$ ist also ein n -Tupel (k_1, \dots, k_n) mit $k_i \in \mathbb{N}$. Dies kann man auch schreiben als

$$(k_1, \dots, k_n) = k_1(1, 0, 0, \dots, 0) + k_2(0, 1, 0, \dots, 0) + \dots + k_n(0, 0, 0, \dots, 1)$$

Damit lässt sich das zugehörige Monom X^k eindeutig schreiben als

$$X^k = X_1^{k_1} X_2^{k_2} \dots X_n^{k_n},$$

wobei wir $X_i = X^{e_i} = X^{(0, \dots, 0, 1, 0, \dots, 0)}$ für das Monom zum i -ten Basiselement geschrieben haben. Das bedeutet aber, dass der Monoidring zum Monoid \mathbb{N}^n über R genau der Polynomring in n Variablen ist. Insbesondere ist $R[\mathbb{N}^n] = R[X]$. Der Monoidring zum trivialen Monoid ist der Grundring selbst.

Beispiel 17.4. (Laurenttring als Monoidring) Sei n eine natürliche Zahl und $M = \mathbb{Z}^n$ das n -fache direkte Produkt der ganzen Zahlen. M ist also die freie Gruppe vom Rang n . Jedes Element $k \in \mathbb{Z}^n$ ist ein n -Tupel (k_1, \dots, k_n) mit $k_i \in \mathbb{Z}$. Dies kann man auch schreiben als

$$(k_1, \dots, k_n) = k_1(1, 0, 0, \dots, 0) + k_2(0, 1, 0, \dots, 0) + \dots + k_n(0, 0, 0, \dots, 1)$$

und das zugehörige Monom X^k kann man eindeutig schreiben als

$$X^k = X_1^{k_1} X_2^{k_2} \dots X_n^{k_n},$$

mit $k_i \in \mathbb{Z}$, wobei wir wieder $X_i = X^{e_i}$ geschrieben haben. Für diesen Monoidring schreibt man auch

$$R[M] = R[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}],$$

und dieser ist isomorph zur Nenneraufnahme des Polynomringes am Produkt der Variablen, also

$$R[M] = R[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}] = R[X_1, \dots, X_n]_{X_1 \dots X_n},$$

Diesen Ring nennt man auch den *Laurenttring* in n Variablen über R .

17.2. Universelle Eigenschaft der Monoidringe.

Satz 17.5. (*Universelle Eigenschaft der Monoidringe*) Sei R ein kommutativer Ring und sei M ein kommutatives Monoid. Sei B eine kommutative R -Algebra und $\varphi : M \rightarrow B$ ein Monoidhomomorphismus (bzgl. der multiplikativen Struktur von B .) Dann gibt es einen eindeutig bestimmten R -Algebra Homomorphismus $\tilde{\varphi} : R[M] \rightarrow B$ derart, dass das Diagramm

$$\begin{array}{ccc} M & \longrightarrow & R[M] \\ & \searrow & \downarrow \\ & & B \end{array}$$

kommutiert.

Beweis. Ein R -Modul-Homomorphismus $\tilde{\varphi} : R[M] \rightarrow B$ ist festgelegt durch die Bilder der Basiselemente X^m , $m \in M$. Das Diagramm kommutiert genau dann, wenn $\tilde{\varphi}(X^m) = \varphi(m)$ ist. Durch diese Bedingung ist die Abbildung also eindeutig festgelegt und ist bereits ein R -Modul-Homomorphismus. Es ist zu zeigen, dass dieser Homomorphismus auch die Multiplikation respektiert. Es ist $\tilde{\varphi}(1) = \tilde{\varphi}(X^0) = \varphi(0) = 1$. Ferner ist

$$\tilde{\varphi}(X^m X^k) = \tilde{\varphi}(X^{m+k}) = \varphi(m+k) = \varphi(m) \cdot \varphi(k) = \tilde{\varphi}(X^m) \cdot \tilde{\varphi}(X^k).$$

Auf der Ebene der Monome respektiert die Abbildung also die Multiplikation. Daraus folgen für zwei Elemente $f = \sum_{m \in M} a_m X^m$ und $g = \sum_{k \in M} b_k X^k$ die Identitäten

$$\begin{aligned} \tilde{\varphi}\left(\left(\sum_{m \in M} a_m X^m\right)\left(\sum_{k \in M} b_k X^k\right)\right) &= \tilde{\varphi}\left(\sum_{\ell \in M} \left(\sum_{m+k=\ell} a_m b_k\right) X^\ell\right) \\ &= \sum_{\ell \in M} \left(\sum_{m+k=\ell} a_m b_k\right) \varphi(\ell) \\ &= \sum_{m,k \in M} a_m b_k \varphi(m) \varphi(k) \\ &= \left(\sum_{m \in M} a_m \varphi(m)\right) \left(\sum_{k \in M} b_k \varphi(k)\right) \\ &= \tilde{\varphi}\left(\sum_{m \in M} a_m X^m\right) \tilde{\varphi}\left(\sum_{k \in M} b_k X^k\right), \end{aligned}$$

so dass die Abbildung ein Ringhomomorphismus ist. \square

Korollar 17.6. (*Funktorialität im Monoid*) Sei R ein kommutativer Ring. Seien M und N kommutative Monoide und sei $\varphi : M \rightarrow N$ ein Monoidhomomorphismus. Dann induziert dies einen R -Algebra-Homomorphismus zwischen den zugehörigen Monoidringen

$$\tilde{\varphi} : R[M] \rightarrow R[N] \text{ durch } X^m \longmapsto X^{\varphi(m)}.$$

Beweis. Dies folgt aus Satz 17.5 angewandt auf die R -Algebra $B = R[N]$ und den zusammengesetzten Monoidhomomorphismus $M \xrightarrow{\varphi} N \rightarrow R[N]$. \square

Bemerkung 17.7. Eine Familie von Elementen $m_i \in M$, $i \in I$, in einem Monoid M ergibt einen Monoidhomomorphismus $\mathbb{N}^{(I)} \rightarrow M$, indem das i -te Basiselement e_i auf m_i geschickt wird. Dies ist insbesondere für endliche Indexmengen $I = \{1, \dots, n\}$ relevant. Der Monoidhomomorphismus induziert dann nach Korollar 17.6 einen R -Algebra-Homomorphismus $R[\mathbb{N}^n] = R[X_1, \dots, X_n] \rightarrow R[M]$ von der Polynomalgebra in den Monoidring. Diese Abbildung ist der Einsetzungshomomorphismus, der durch $X_i \mapsto X^{m_i}$ gegeben ist.

Definition 17.8. Zu einem kommutativen Monoid M und einem kommutativen Ring R nennt man einen Monoidhomomorphismus

$$M \longrightarrow (R, \cdot, 1)$$

auch einen R -wertigen Punkt von M .

Bemerkung 17.9. Ein R -wertiger Punkt ist äquivalent zu einem R -Algebra-Homomorphismus von $R[M]$ nach R . Diese Sprechweise ist insbesondere im Fall eines Grundkörpers K üblich. Dann haben wir also

$$\begin{aligned} K\text{-Spek}(K[M]) &= \text{Hom}_K^{\text{alg}}(K[M], K) \\ &= \text{Mor}_{\text{mon}}(M, K) \\ &= \{K\text{-wertige Punkte von } M\}. \end{aligned}$$

Das bedeutet, dass hier das K -Spektrum bereits auf der Ebene des Monoids eine einfache Beschreibung besitzt, die rein multiplikativ ist. Das impliziert, wie wir sehen werden, dass es für die K -Spektren der Monoidringe im Allgemeinen eine viel übersichtlichere Beschreibung gibt als sonst. Man beachte allerdings, dass zur Definition der Zariski-Topologie und der Garbe der algebraischen Funktionen der Monoidring unverzichtbar ist.

Lemma 17.10. Sei R ein von null verschiedener kommutativer Ring. Seien M und N kommutative Monoide und sei $\varphi : M \rightarrow N$ ein Monoidhomomorphismus. Dann ist φ genau dann injektiv (surjektiv), wenn der zugehörige R -Algebra-Homomorphismus $\tilde{\varphi} : R[M] \rightarrow R[N]$ injektiv (surjektiv) ist.

Beweis. Sei φ injektiv, und angenommen, dass

$$\tilde{\varphi}\left(\sum_{m \in M} a_m X^m\right) = \sum_{m \in M} a_m X^{\varphi(m)} = 0.$$

Da die $\varphi(m)$, $m \in M$, alle verschieden sind, folgt daraus $a_m = 0$. Ist umgekehrt φ nicht injektiv, sagen wir $\varphi(m) = \varphi(k)$, $m \neq k$, so ist auch $\tilde{\varphi}(X^m) = \tilde{\varphi}(X^k)$, obwohl $X^m \neq X^k$ ist.

Ist φ surjektiv, so kann man für ein beliebiges Element $\sum_{n \in N} a_n X^n$ aus $R[N]$ sofort ein Urbild angeben, nämlich $\sum_{n \in N} a_n X^{m_n}$, wobei m_n ein beliebiges Urbild von n sei. Ist hingegen φ nicht surjektiv, so sei $n \in N$ ein Element, das nicht zum Bild gehört. Dann ist das Monom X^n von null verschieden und kann nicht im Bild des Algebra-Homomorphismus liegen. \square

Korollar 17.11. *Sei R ein von null verschiedener kommutativer Ring. Sei M ein kommutatives Monoid und $m_i \in M$, $i \in I$, eine Familie von Elementen aus M . Dann bilden die m_i genau dann ein Monoid-Erzeugendensystem für M , wenn die X^{m_i} , $i \in I$, ein R -Algebra-Erzeugendensystem für den Monoidring $R[M]$ bilden.*

Beweis. Die m_i , $i \in I$, bilden genau dann ein Monoid-Erzeugendensystem für M , wenn der Monoidhomomorphismus $\mathbb{N}^{(I)} \rightarrow M$ surjektiv ist. Dies ist nach Lemma 17.10 genau dann der Fall, wenn der zugehörige Homomorphismus

$$R[X_i, i \in I] \longrightarrow R[M], X_i \longmapsto X^{m_i},$$

surjektiv ist. Dies ist aber genau dann der Fall, wenn die X^{m_i} ein R -Algebra-Erzeugendensystem bilden. \square

Korollar 17.12. *(Funktorialität im Ring) Sei R ein kommutativer Ring und S eine R -Algebra. Es sei M ein kommutatives Monoid. Dann gibt es einen natürlichen R -Algebra-Homomorphismus*

$$R[M] \longrightarrow S[M], \sum_{m \in M} a_m X^m \longmapsto \sum_{m \in M} a_m X^m$$

(die Koeffizienten aus R werden also einfach in S aufgefasst).

Beweis. Dies folgt aus Satz 17.5, angewandt auf die R -Algebra $S[M]$ und den Monoidhomomorphismus $M \rightarrow S[M]$. \square

17.3. Differenzengruppe zu einem Monoid.

Wir interessieren uns nun für die Frage, wann ein Monoidring ein Integritätsbereich ist (was nur bei integrem Grundring sein kann) und wie man dann den Quotientenkörper beschreiben kann. Da im Quotientenkörper jedes von null verschiedene Element invertierbar sein muss, gilt das insbesondere für die Monome T^m , $m \in M$, und es liegt nahe, nach einer additiven Gruppe zu suchen, die M umfasst.

Definition 17.13. Sei M ein kommutatives Monoid. Dann nennt man die Menge der *formalen Differenzen*

$$\Gamma(M) = \{m - n : m, n \in M\}$$

mit der Addition

$$m_1 - n_1 + m_2 - n_2 := (m_1 + m_2) - (n_1 + n_2)$$

und der Identifikation

$$m_1 - n_1 = m_2 - n_2 \text{ falls es } m \in M \text{ gibt mit } m + m_1 + n_2 = m + m_2 + n_1.$$

die *Differenzengruppe* zu M .

Wir überlassen es dem Leser als Aufgabe, zu zeigen, dass die Differenzengruppe wirklich eine Gruppe ist. Die vorstehende Konstruktion ist natürlich der Konstruktion von Quotientenkörpern bzw. Quotientenringen nachempfunden, man muss nur die multiplikative Schreibweise dort additiv umdeuten. Die Konstruktion der Differenzengruppe ist eigentlich elementarer. Die Differenzengruppe zum additiven Monoid \mathbb{N} ist natürlich \mathbb{Z} . Die Elemente in einem Monoid kann man direkt im Differenzenmonoid auffassen, und zwar durch den Monoidhomomorphismus

$$M \longrightarrow \Gamma(M), m \longmapsto m - 0,$$

wobei wir statt $m - 0$ einfach m schreiben. Völlig unproblematisch ist dieser Übergang aber doch nicht, da diese Abbildung im Allgemeinen nicht injektiv sein muss. Das hat damit zu tun, dass in der obigen Definition bei der Identifizierung links und rechts ein m auftreten darf (und das lässt sich auch nicht vermeiden). Natürlich will man auch diejenigen Monoide charakterisieren, für die man dieses Extra- m nicht braucht.

Definition 17.14. Man sagt, dass in einem kommutativen Monoid M die *Kürzungsregel* gilt (oder dass M ein *Monoid mit Kürzungsregel* ist), wenn aus einer Gleichung

$$m + n = m + k \text{ mit } m, n, k \in M,$$

stets folgt, dass $n = k$ ist.

Für ein solches Monoid ist die Abbildung in die Differenzengruppe injektiv, siehe Aufgabe 17.8.

18. VORLESUNG

18.1. Monomiale Kurven.

Wir spezialisieren nun die Theorie der Monoidringe auf den eindimensionalen Fall und gelangen zu denjenigen Ringen, die monomiale Kurven beschreiben.

Definition 18.1. Eine *monomiale Kurve* ist das Bild der affinen Geraden \mathbb{A}_K^1 unter einer Abbildung der Form

$$\mathbb{A}_K^1 \longrightarrow \mathbb{A}_K^n, t \longmapsto (t^{e_1}, \dots, t^{e_n}),$$

mit $e_i \geq 1$ für alle i .

Wir werden gleich sehen, dass das Bild einer solchen monomialen Abbildung Zariski-abgeschlossen ist, d.h., dass eine monomiale Kurve wirklich eine algebraische Kurve ist. Eine monomiale Kurve ist insbesondere eine parametrisierte und damit eine rationale Kurve. Manchmal bezeichnet man auch die Abbildung selbst als monomiale Kurve. Häufig beschränkt man sich auf den Fall, wo die Exponenten e_i insgesamt teilerfremd sind. Dies ist keine wesentliche Einschränkung, da man andernfalls stets schreiben kann $e_i = m f_i$ mit

dem gemeinsamen Teiler m und teilerfremden Zahlen f_i . Dann kann man die Gesamtabbildung auffassen als Hintereinanderschaltung

$$\mathbb{A}_K^1 \longrightarrow \mathbb{A}_K^1 \longrightarrow \mathbb{A}_K^n \text{ mit } t \longmapsto t^m = s \text{ und } s \longmapsto (s_1^{f_1}, \dots, s_n^{f_n}),$$

wobei vorne ein einfaches Potenzieren und hinten eine monomiale Kurvenabbildung mit teilerfremden Exponenten vorliegt.

Bemerkung 18.2. Eine monomiale Abbildung $t \mapsto (t^{e_1}, \dots, t^{e_n})$ ist nichts anderes als die zum Monoidmorphismus $\mathbb{N}^n \rightarrow \mathbb{N}$, die den i -ten Basisvektor auf e_i schickt, gehörende Abbildung der zugehörigen K -Spektra. Diese Monoidabbildung faktorisiert

$$\mathbb{N}^n \longrightarrow M \longrightarrow \mathbb{N},$$

wobei M das von den e_i erzeugte Untermonoid der natürlichen Zahlen ist. Ein solches Untermonoid heißt *numerisches Monoid*. Die erste Abbildung ist dabei eine Surjektion. Es liegen also insgesamt Ringhomomorphismen

$$K[\mathbb{N}^n] = K[X_1, \dots, X_n] \longrightarrow K[M] \longrightarrow K[\mathbb{N}] = K[T]$$

und geometrisch die Spektrumsabbildungen

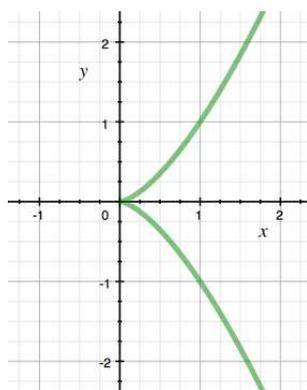
$$\mathbb{A}_K^1 \longrightarrow K\text{-Spek}(K[M]) \subseteq \mathbb{A}_K^n$$

vor. Das Bild der affinen Geraden liegt also im K -Spektrum des Monoidringes $K[M]$. Wir werden weiter unten sehen, dass die Abbildung $\mathbb{A}_K^1 \rightarrow K\text{-Spek}(K[M])$ stets surjektiv ist und im Fall, dass die Exponenten e_i teilerfremd sind, auch injektiv.

Beispiel 18.3. Die *Neilsche Parabel* C ist das Bild unter der monomialen Abbildung

$$\mathbb{A}_K^1 \longrightarrow \mathbb{A}_K^2, t \longmapsto (t^2, t^3) = (x, y).$$

Die zugehörige Gleichung ist $y^2 = x^3$, d.h. es ist $C = V(Y^2 - X^3)$.



Das Besondere an monomialen Kurven ist, dass sie zwar allein durch das Exponententupel (e_1, \dots, e_n) bzw. das davon erzeugte numerische Monoid gegeben sind, also durch einen sehr kleinen Betrag an (kombinatorischer) Information, aber zugleich ein reichhaltiges Beispielmaterial an algebraischen

Kurven liefern (dies gilt allgemein für Monoidringe und die dadurch definierten algebraischen Varietäten).

Lemma 18.4. *Sei $M \subseteq \mathbb{N}$ ein numerisches Monoid, das von teilerfremden natürlichen Zahlen e_1, \dots, e_n erzeugt sei. Dann gibt es zu jedem $m \in \mathbb{N}$ eine Darstellung*

$$m = a_1 e_1 + \dots + a_n e_n \text{ mit } 0 \leq a_i < e_{i+1} \text{ für } 1 \leq i \leq n-1.$$

Für m hinreichend groß kann man zusätzlich noch $a_n \geq 0$ erreichen, so dass es dann eine Darstellung mit nichtnegativen Koeffizienten gibt.

Beweis. Wegen der Teilerfremdheit gibt es natürlich eine Darstellung

$$m = b_1 e_1 + \dots + b_n e_n$$

mit ganzzahligen Koeffizienten b_i . Wir werden sie schrittweise auf die gewünschte Gestalt bringen. Wir schreiben $b_1 = c_1 e_2 + a_1$ mit $0 \leq a_1 < e_2$ (Division mit Rest). Dies setzt man in die Gleichung für m ein und schlägt den Term $c_1 e_2 e_1$ zu $b_2 e_2$ dazu. Ebenso bringt man den (neuen) zweiten Koeffizienten auf die gewünschte Form, in dem man ihn mit dem dritten Erzeuger verarbeitet. So kann man alle ersten $n-1$ Koeffizienten auf die gewünschte Gestalt bringen.

Sei die Darstellung nun in der gewünschten Form. Dann ist die Summe der ersten $n-1$ Summanden beschränkt. Wenn m größer als diese Schranke ist, so muss der letzte Summand und damit auch der letzte Koeffizient nichtnegativ sein. \square

Zu einem von teilerfremden Elementen erzeugten Untermonoid gehören also ab einer gewissen Stelle alle natürlichen Zahlen. Diese bekommt sogar einen eigenen Namen.

Definition 18.5. Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde Erzeuger definiertes numerisches Monoid. Dann nennt man die minimale Zahl f mit $\mathbb{N}_{\geq f} \subseteq M$ die *Führerzahl* von M .

Wir geben noch einige weitere Definitionen von numerischen Invarianten von monomialen Kurven, die man diskret, also auf der Ebene des numerischen Monoids berechnen kann. Wir werden später sehen, dass diese Invarianten allgemeiner für beliebige algebraische Kurven definiert werden können, dort aber im allgemeinen schwieriger zu berechnen sind.

Definition 18.6. Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde Erzeuger definiertes numerisches Monoid. Dann nennt man die Anzahl der Lücken, d.h. der natürlichen Zahlen $\mathbb{N} - M$, den *Singularitätsgrad* von M , geschrieben $\delta(M)$.

Definition 18.7. Sei $M \subseteq \mathbb{N}$ ein numerisches Monoid mit teilerfremden Erzeugern. Dann nennt man die minimale Anzahl von Elementen in einem Erzeugendensystem für M die *Einbettungsdimension* von M .

Definition 18.8. Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde Erzeuger definiertes numerisches Monoid. Dann nennt man das minimale (positive) Element $e \in M$, $e \geq 1$, die *Multiplizität* von M , geschrieben $e(M)$.

Beispiel 18.9. Wir betrachten das durch 5, 8 und 11 erzeugte numerische Monoid M . M besteht also aus allen Summen $5a_1 + 8a_2 + 11a_3$ mit nichtnegativen Koeffizienten a_1, a_2, a_3 . Es lässt sich einfach überlegen, dass M die folgenden Elemente enthält:

$$0, 5, 8, 10, 11, 13, 15, 16, 18, 19, 20, 21, 22, 23, 24, 25, \dots$$

Da es insbesondere fünf Zahlen hintereinander enthält (von 18 bis 22), muss jede weitere Zahl auch dazu gehören, da man ja einfach $5 \in M$ dazuaddieren kann. Damit ist die Führerzahl 18, die Multiplizität ist 5, der Singularitätsgrad ist 10 und die Einbettungsdimension ist 3.

Satz 18.10. Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde natürliche Zahlen e_1, \dots, e_n erzeugtes Untermonoid. Dann ist die monomiale Abbildung

$$\mathbb{A}_K^1 \longrightarrow K\text{-Spek}(K[M])$$

eine Bijektion.

Beweis. Die Abbildung kann man auffassen als die natürliche Abbildung

$$\mathbb{A}_K^1 = \text{Mor}_{\text{mon}}(\mathbb{N}, K) \longrightarrow \text{Mor}_{\text{mon}}(M, K),$$

die durch die Inklusion von Monoiden $M \subseteq \mathbb{N}$ induziert ist. Zur Injektivität seien $a, b \in K$ gegeben und sei angenommen, dass für alle $m \in M$ gilt: $a^m = b^m$. Bei $b = 0$ folgt sofort $a = 0$, sei also $b \neq 0$. Dann gilt $\left(\frac{a}{b}\right)^m = 1$ für alle $m \in M$. Da es für M ein teilerfremdes Erzeugendensystem gibt, gehören nach Lemma 18.4 ab einem gewissen f alle natürlichen Zahlen zu M . Es ist also insbesondere $a^m = b^m$ für alle $m \geq f$. Daraus folgt aber $\frac{a}{b} = 1$ (und $a = b$): seien nämlich m und $k \geq f$ und teilerfremd, und sei $s^m = s^k = 1$. Wegen der Teilerfremdheit gibt es (nach dem Lemma von Bezout) ganze Zahlen p, q mit $pk + qm = 1$. Dann ist

$$s = s^{pk+qm} = (s^k)^p \cdot (s^m)^q = 1.$$

Zur Surjektivität. Es sei ein Monoidmorphismus $\varphi : M \rightarrow K$ gegeben, und wir müssen ihn zu einem Monoidmorphismus auf ganz \mathbb{N} fortsetzen. Es sei $\varphi(e_i) = a_i \in K$. Zwischen diesen Werten gilt die Beziehung

$$a_j^{e_i} = \varphi(e_j)^{e_i} = \varphi(e_i e_j) = \varphi(e_i)^{e_j} = a_i^{e_j}.$$

Wenn eines der $a_i = 0$ ist, so müssen alle $= 0$ sein und die Nullabbildung ist eine Fortsetzung. Wir können also annehmen, dass alle a_i Einheiten sind. Wegen der Teilerfremdheit der e_i gibt es eine Darstellung der Eins, d.h. es gibt ganze Zahlen m_1, \dots, m_n mit $m_1 e_1 + \dots + m_n e_n = 1$. Wir behaupten, dass durch $1 \mapsto a = a_1^{m_1} \dots a_n^{m_n}$ eine Fortsetzung auf \mathbb{N} gegeben ist. Dazu müssen wir zeigen, dass der durch $1 \mapsto a$ (also $k \mapsto a^k$) definierte Monoidmorphismus

mit φ übereinstimmt, was man nur für die e_i überprüfen muss. Betrachten wir also e_1 . Dann ist

$$\begin{aligned}
 a^{e_1} &= (a_1^{m_1} \cdots a_n^{m_n})^{e_1} \\
 &= a_1^{e_1 m_1} \cdot a_2^{e_1 m_2} \cdots a_n^{e_1 m_n} \\
 &= a_1^{1 - \sum_{i=2}^n m_i e_i} (a_2^{e_1 m_2} \cdots a_n^{e_1 m_n}) \\
 &= a_1 \cdot (a_1^{-m_2 e_2} a_2^{e_1 m_2}) \cdots (a_1^{-m_n e_n} a_n^{e_1 m_n}) \\
 &= a_1 \cdot (a_1^{-e_2} a_2^{e_1})^{m_2} \cdots (a_1^{-e_n} a_n^{e_1})^{m_n} \\
 &= a_1,
 \end{aligned}$$

da die Faktoren rechts in der vorletzten Zeile alle 1 nach der Vorüberlegung (oberes Display) sind. \square

Bemerkung 18.11. Den vorstehenden Satz kann man auch über die universelle Eigenschaft der Differenzgruppe beweisen. Wir skizzieren dies kurz für die Surjektivität. Die Differenzgruppe eines numerischen Monoids mit teilerfremden Erzeugern ist \mathbb{Z} . Der Fall, dass ein Erzeuger auf null geht, wird wie im Beweis abgehandelt. Dann kann man davon ausgehen, dass ein Monoidhomomorphismus $\varphi : M \rightarrow K^\times$ in die Einheitengruppe des Körpers vorliegt. Dann gibt es nach der universellen Eigenschaft der Monoidringe eine (eindeutig bestimmte) Fortsetzung $\tilde{\varphi} : \mathbb{Z} \rightarrow K^\times$, die das Urbild liefert (diese Bemerkung verdanken wir Herrn Hebestreit.)

Die folgenden beiden Aussagen zeigen, dass es für ein numerisches Monoid ein kanonisches Erzeugendensystem gibt und dass damit die Einbettungsdimension eine neue Interpretation erhält, die sich später auf beliebige noethersche lokale Ringe übertragen lässt (ein Monoidring ist natürlich nicht lokal, wohl aber die Lokalisierung an der Singularität eines numerischen Monoids).

Lemma 18.12. *Sei $M \subseteq \mathbb{N}$ ein numerisches Monoid mit teilerfremden Erzeugern, und es sei $M_+ = \{m \in M : m \geq 1\}$ und $M_+ + M_+ = \{m + m' : m, m' \in M_+\}$. Dann ist*

$$M_+ - (M_+ + M_+)$$

ein Erzeugendensystem für M , und jedes andere Erzeugendensystem enthält dieses.

Beweis. Ein Element $m \in M_+ - (M_+ + M_+)$ lässt sich nicht als Summe von anderen Elementen darstellen, daher gehören sie zu jedem Erzeugendensystem. Umgekehrt ist es aber schon ein Erzeugendensystem. Wäre das nicht der Fall, so gäbe es ein minimales Element $x \in M$, das nicht von diesen Elementen erzeugt würde. Insbesondere gehört dann x nicht zu diesen Elementen und daher ist $x = x_1 + x_2$ mit $x_1, x_2 \in M_+ + M_+$. Diese beiden Summanden sind aber kleiner als x und deshalb gibt es für sie eine Summendarstellung aus diesen Elementen, was sofort ein Widerspruch ist. \square

Korollar 18.13. Sei $M \subseteq \mathbb{N}$ ein numerisches Monoid mit teilerfremden Erzeugern, und es sei $M_+ = \{m \in M : m \geq 1\}$ und $M_+ + M_+ = \{m + m' : m, m' \in M_+\}$. Dann ist die Einbettungsdimension von M gleich der Anzahl von $M_+ - (M_+ + M_+)$.

Beweis. Dies folgt direkt aus Lemma 18.12. \square

19. VORLESUNG

19.1. Restklassendarstellung für monomiale Kurven.

Sei M ein numerisches Monoid, das von den teilerfremden natürlichen Zahlen e_1, \dots, e_n erzeugt werde. Die zugehörige Surjektion $\mathbb{N}^n \rightarrow M \subseteq \mathbb{N}$ führt zu einer Surjektion

$$K[X_1, \dots, X_n] \longrightarrow K[M], X_i \longmapsto T^{e_i},$$

und einer abgeschlossenen Einbettung $C = K - \text{Spek}(K[M]) \hookrightarrow \mathbb{A}_K^n$. Durch welche Gleichungen lässt sich C beschreiben?

Satz 19.1. Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde Elemente e_1, \dots, e_n erzeugtes Untermonoid und sei $\mathbb{N}^n \rightarrow M$ die zugehörige surjektive Abbildung mit dem zugehörigen Restklassenhomomorphismus $\varphi : K[X_1, \dots, X_n] \rightarrow K[M]$. Dann wird das Kernideal durch

$$\ker \varphi = \left(\prod_{i \in I_1} X_i^{r_i} - \prod_{i \in I_2} X_i^{s_i} : I_1, I_2 \subseteq \{1, \dots, n\} \text{ disjunkt}, \sum_{i \in I_1} r_i e_i = \sum_{i \in I_2} s_i e_i \right)$$

(mit $r_i, s_i \geq 1$) beschrieben.

Beweis. Dass die angegebenen Elemente zum Kernideal gehören folgt direkt aus

$$\varphi\left(\prod_{i \in I_1} X_i^{r_i}\right) = \prod_{i \in I_1} (t^{e_i})^{r_i} = t^{\sum_{i \in I_1} r_i e_i}.$$

Für die Umkehrung sei $F \in K[X_1, \dots, X_n]$ ein Polynom mit $\varphi(F) = 0$. Wir schreiben

$$F = \sum_{\nu} a_{\nu} X^{\nu}$$

(mit $\nu = (\nu_1, \dots, \nu_n)$). Daher ist

$$\varphi(F) = \sum_{\nu} a_{\nu} t^{\sum_{i=1}^n \nu_i e_i} = \sum_{k=0} \left(\sum_{\nu: \sum_{i=1}^n \nu_i e_i = k} a_{\nu} \right) t^k.$$

Da dieses Polynom null ist müssen alle Koeffizienten null sein, d.h. zu jedem k gehört auch

$$F_k = \sum_{\nu: \sum_{i=1}^n \nu_i e_i = k} a_{\nu} X^{\nu}$$

zum Kern. Wir können also annehmen, dass in F nur Monome X^{ν} vorkommen mit gleichem Wert $\sum_{i=1}^n \nu_i e_i = k$. Betrachten wir ein solches Monom aus

F , sagen wir X^ν (mit $a_\nu \neq 0$). Es muss in F mindestens noch ein weiteres Monom, sagen wir X^μ , vorkommen, da ein einzelnes Monom nicht auf null abgebildet wird. Wir schreiben

$$F = a_\nu(X^\nu - X^\mu) + (F - a_\nu X^\nu + a_\nu X^\mu).$$

Im Summand rechts kommt X^ν nicht mehr vor, und es kommt auch kein neues Monom hinzu. In $X^\nu - X^\mu$ können wir diejenigen Variablen, die beidseitig auftreten, so weit ausklammern, dass sich ein Ausdruck der Form

$$X^\nu - X^\mu = X_1^{b_1} \cdots X_n^{b_n} \left(\prod_{i \in I_1} X_i^{r_i} - \prod_{i \in I_2} X_i^{s_i} \right)$$

mit disjunkten I_1 und I_2 und mit $\sum_{i \in I_1} e_i r_i = \sum_{i \in I_2} e_i s_i$ ergibt. Der linke Summand in obiger Beschreibung von F gehört also zu dem von den angegebenen Binomen erzeugten Ideal und wir können mit dem rechten Summand, in dem ein Monom weniger vorkommt, fortfahren. \square

Die einfachsten Gleichungen sind von der Bauart ($i \neq j$)

$$X_i^{e_j / \text{ggT}(e_i, e_j)} - X_j^{e_i / \text{ggT}(e_i, e_j)}.$$

Im Fall von ebenen monomialen Kurven ist das auch die einzige Gleichung.

Korollar 19.2. *Sei C die durch $t \mapsto (t^{e_1}, t^{e_2}) = (x, y)$ (mit e_1, e_2 teilerfremd) gegebene monomiale ebene Kurve. Dann ist*

$$C = V(X^{e_2} - Y^{e_1}).$$

Beweis. Dies folgt sofort aus Satz 19.1. \square

Bei monomialen Raumkurven lassen sich die beschreibenden Gleichungen auch noch einigermaßen einfach bestimmen, da man immer eine Variable isolieren kann.

Beispiel 19.3. Sei C die durch

$$t \mapsto (t^3, t^4, t^5) = (x, y, z)$$

gegebene monomiale Kurve. Für jede der drei Variablen müssen wir schauen, welche Potenzen davon sich, wenn man die t -Potenz substituiert, auch als Monom in den beiden anderen Variablen ausdrücken lassen.

Zunächst haben wir die Beziehungen, in denen jeweils nur zwei Variablen vorkommen. Das sind

$$Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5.$$

Hier kann es, wie im ebenen Fall, immer nur eine Beziehung geben.

In den Relationen, wo alle drei Variablen beteiligt sind, kommt eine der Variablen allein vor. Starten wir mit X . Zunächst lassen sich X und X^2 nicht durch die anderen Variablen ausdrücken, dafür haben wir $X^3 = T^9 = YZ$. Eine andere Kombination ist nicht möglich. Grundsätzlich impliziert eine mehrfache Darstellung $X^k = Y^i Z^j = Y^a Z^b$, dass man zwischen Potenzen von Y und

von Z eine Beziehung hat, da man ja die kleineren Potenzen rauskürzen kann. Da wir alle Relationen mit nur zwei Variablen schon aufgelistet haben, liefert eine Potenz von X immer nur maximal eine neue Relation. Wir behaupten, dass wir für X allein stehend schon fertig sind. Ist nämlich $X^k = Y^i Z^j$, so ist $k \geq 3$. Bei $i = 0$ oder $j = 0$ haben wir die Gleichungen schon aufgelistet. Sei also $i, j \geq 1$. Dann kann man aber mittels der Gleichung $X^3 = YZ$ die Exponenten in der Gleichung kleiner machen (in dem man den Exponenten von X um 3 reduziert und die Exponenten von Y und von Z um 1.)

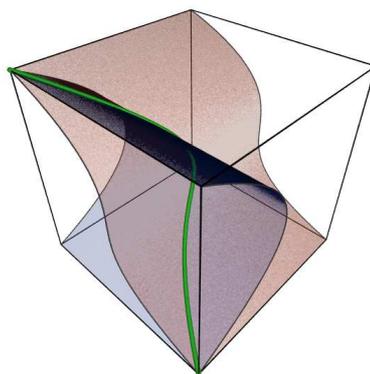
Für Y hat man sofort die Gleichung $Y^2 = ZX$, mit der man wieder alle anderen Gleichungen reduzieren kann.

Für Z hat man $Z^2 = X^2 Y$ und $Z^3 = XY^3$. Es gibt keine kleineren Monome in X und Y , die man als Potenz von Z ausdrücken kann. Daher kann man jede andere Relation mittels einer von diesen auf eine frühere zurückführen.

Insgesamt haben wir also für die Kurve C die Gleichungen

$$C = V(Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5, X^3 - YZ, Y^2 - XZ, Z^2 - X^2 Y, Z^3 - XY^3)$$

Beispiel 19.4. (Die gedrehte Kubik)



Sei $C \subset \mathbb{A}_K^3$ die „gedrehte Kubik“, also das Bild der monomialen Abbildung, die durch $t \mapsto (t, t^2, t^3)$ gegeben ist. Diese Kurve ist isomorph zu einer affinen Geraden und insbesondere glatt. Das beschreibende Ideal ist nach Satz 19.1 gleich

$$\mathfrak{a} = (Y - X^2, Z - X^3, Y^3 - Z^2, Z - XY) = (Y - X^2, Z - X^3).$$

Die zwei letzten Gleichungen sind dabei überflüssig, da sie sich durch die beiden anderen ausdrücken lassen. Insgesamt ist also

$$C = V(Y - X^2, Z - X^3).$$

Die Bilder von C unter den drei verschiedenen Projektionen sind

$$C_1 = V(Z^2 - Y^3), C_2 = V(Z - X^3), C_3 = V(Y - X^2).$$

Dabei sind C_2 und C_3 glatt und isomorph zur affinen Geraden (als Graph einer Abbildung), während C_1 die singuläre Neilsche Parabel ist.

19.2. Ganzheit.

Definition 19.5. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1x + r_0 = 0,$$

wobei die Koeffizienten r_i , $i = 0, \dots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x .

Definition 19.6. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz*, wenn x eine Ganzheitsgleichung mit Koeffizienten aus R erfüllt.

Definition 19.7. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann nennt man die Menge der Elemente $x \in S$, die ganz über R sind, den *ganzen Abschluss* von R in S .

Definition 19.8. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R , wenn jedes Element $x \in S$ ganz über R ist.

S ist genau dann ganz über R , wenn der ganze Abschluss von R in S gleich S ist.

Lemma 19.9. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ sind folgende Aussagen äquivalent.

- (1) x ist ganz über R .
- (2) Es gibt eine R -Unteralgebra T von S mit $x \in T$ und die ein endlicher R -Modul ist.
- (3) Es gibt einen endlichen R -Untermodule M von S , der einen Nichtnullteiler aus S enthält, mit $xM \subseteq M$.

Beweis. (1) \Rightarrow (2). Wir betrachten die von den Potenzen von x erzeugte R -Unteralgebra $R[x]$ von S , die aus allen polynomialen Ausdrücken in x mit Koeffizienten aus R besteht. Aus einer Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1x + r_0 = 0$$

ergibt sich

$$x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \dots - r_1x - r_0.$$

Man kann also x^n durch einen polynomialen Ausdruck von einem kleineren Grad ausdrücken. Durch Multiplikation dieser letzten Gleichung mit x^i kann man jede Potenz von x mit einem Exponenten $\geq n$ durch einen polynomialen Ausdruck von einem kleineren Grad ersetzen. Insgesamt kann man dann aber all diese Potenzen durch polynomiale Ausdrücke vom Grad $\leq n-1$ ersetzen. Damit ist

$$R[x] = R + Rx + Rx^2 + \dots + Rx^{n-2} + Rx^{n-1}$$

und die Potenzen $x^0 = 1, x^1, x^2, \dots, x^{n-1}$ bilden ein endliches Erzeugendensystem von $T = R[x]$.

(2) \Rightarrow (3). Sei $x \in T \subseteq S$, T eine R -Unteralgebra, die als R -Modul endlich erzeugt sei. Dann ist $xT \subseteq T$, und T enthält den Nichtnullteiler 1.

(3) \Rightarrow (1). Sei $M \subseteq S$ ein endlich erzeugter R -Untermodul mit $xM \subseteq M$. Seien y_1, \dots, y_n erzeugende Elemente von M . Dann ist insbesondere xy_i für jedes i eine R -Linearkombination der y_j , $j = 1, \dots, n$. Dies bedeutet

$$xy_i = \sum_{j=1}^n r_{ij}y_j$$

mit $r_{ij} \in R$ oder als Matrix geschrieben

$$x \begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ y_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} & \cdot & \cdot & r_{1,n} \\ r_{2,1} & r_{2,2} & \cdot & \cdot & r_{2,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ r_{n,1} & r_{n,2} & \cdot & \cdot & r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ y_n \end{pmatrix}.$$

Dies schreiben wir als

$$0 = \begin{pmatrix} x - r_{1,1} & -r_{1,2} & \cdot & \cdot & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & \cdot & \cdot & -r_{2,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ -r_{n,1} & -r_{n,2} & \cdot & \cdot & x - r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ y_n \end{pmatrix}.$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{adj}Ay = 0$ (y bezeichne den Vektor (y_1, \dots, y_n)) und nach der Cramerschen Regel ist $A^{adj}A = (\det A)E_n$, also gilt $((\det A)E_n)y = 0$. Es ist also $(\det A)y_j$ für alle j und damit $(\det A)z$ für alle z . Da M nach Voraussetzung einen Nichtnullteiler enthält, muss $\det A = 0$ sein. Die Determinante ist aber ein normierter polynomialer Ausdruck in x vom Grad n , so dass eine Ganzheitsgleichung vorliegt. \square

Korollar 19.10. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringweiterung. Dann ist der ganze Abschluss von R in S eine R -Unteralgebra von S .*

Beweis. Die Ganzheitsgleichungen $X - r$, $r \in R$, zeigen, dass jedes Element aus R ganz über R ist. Seien $x_1 \in S$ und $x_2 \in S$ ganz über R . Nach der Charakterisierung der Ganzheit (Lemma 19.5) gibt es endliche R -Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Sei y_1, \dots, y_n ein R -Erzeugendensystem von T_1 und z_1, \dots, z_m ein R -Erzeugendensystem von T_2 . Wir können annehmen, dass $y_1 = z_1 = 1$ ist. Betrachte den endlich erzeugten R -Modul

$$T = T_1 \cdot T_2 = \langle y_i z_j, i = 1, \dots, n, j = 1, \dots, m \rangle,$$

der offensichtlich $x_1 + x_2$ und x_1x_2 (und 1) enthält. Dieser R -Modul T ist auch wieder eine R -Algebra, da für zwei beliebige Elemente gilt

$$\left(\sum r_{ij}y_iz_j\right)\left(\sum s_{kl}y_kz_l\right) = \sum r_{ij}s_{kl}y_iz_jy_kz_l,$$

und für die Produkte gilt $y_iz_j \in T_1$ und $y_kz_l \in T_2$ so dass diese Linearkombination zu T gehört. Dies zeigt, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Deshalb ist der ganze Abschluss ein Unterring von S , der R enthält. Also liegt eine R -Unteralgebra vor. \square

Definition 19.11. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Man nennt R *ganz-abgeschlossen* in S , wenn der ganze Abschluss von R in S gleich R ist.

20. VORLESUNG

20.1. Normale Ringe und Normalisierung.

Definition 20.1. Ein Integritätsbereich heißt *normal*, wenn er ganz-abgeschlossen in seinem Quotientenkörper ist.

Definition 20.2. Sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann nennt man den ganzen Abschluss von R in $Q(R)$ die *Normalisierung* von R .

Es ist eine nichttriviale Tatsache, dass falls R von endlichem Typ ist, dann auch die Normalisierung davon von endlichem Typ ist. Wichtige Beispiele für normale Ringe werden durch faktorielle Ringe geliefert.

Satz 20.3. (*Normalität faktorieller Bereiche*) Sei R ein faktorieller Integritätsbereich. Dann ist R normal.

Beweis. Sei $K = Q(R)$ der Quotientenkörper von R und $q \in K$ ein Element, das die Ganzheitsgleichung

$$q^n + r_{n-1}q^{n-1} + r_{n-2}q^{n-2} + \dots + r_1q + r_0 = 0$$

mit $r_i \in R$ erfüllt. Wir schreiben $q = a/b$ mit $a, b \in R$, wobei wir annehmen können, dass die Darstellung gekürzt ist, dass also a und $b \in R$ keinen gemeinsamen Primteiler besitzen. Wir haben zu zeigen, dass b eine Einheit in R ist, da dann $q = ab^{-1}$ zu R gehört.

Wir multiplizieren obige Ganzheitsgleichung mit b^n und erhalten in R

$$a^n + (r_{n-1}b)a^{n-1} + (r_{n-2}b^2)a^{n-2} + \dots + (r_1b^{n-1})a + (r_0b^n) = 0.$$

Wenn b keine Einheit ist, dann gibt es auch einen Primteiler p von b . Dieser teilt alle Summanden $(r_{n-i}b^i)a^{n-i}$ für $i \geq 1$ und daher auch den ersten, also a^n . Das bedeutet aber, dass a selbst ein Vielfaches von p ist im Widerspruch zur vorausgesetzten Teilerfremdheit. \square

Satz 20.4. Sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Dann ist auch die Nenneraufnahme R_S normal.

Beweis. Siehe Aufgabe 20.1. □

20.2. Normalisierung von Monoidringen.

Wir wollen besprechen, wann Monoidringe normal sind und wie gegebenenfalls die Normalisierung eines Monoidrings aussieht. Hierzu brauchen wir zunächst Bedingungen, die sicherstellen, dass ein Monoidring über einem Integritätsbereich wieder integer ist.

Definition 20.5. Ein kommutatives Monoid M heißt *torsionsfrei*, wenn für $m, n \in M$ aus $rm = rn$ für eine positive Zahl $r \in \mathbb{N}_+$ stets $m = n$ folgt.

Satz 20.6. (*Integrität von Monoidringen*) Sei R ein Integritätsbereich und sei M ein torsionsfreies kommutatives Monoid, das die Kürzungsregel erfüllt. Dann ist der Monoidring $R[M]$ ein Integritätsbereich.

Beweis. Zunächst ist $M \subseteq \Gamma(M)$, wobei $\Gamma(M)$ die Differenzengruppe zu M bezeichnet. Damit ist $R[M] \subseteq R[\Gamma(M)]$ ein Unterring, und es genügt die Aussage für $R[\Gamma(M)]$ zu beweisen. Da M torsionsfrei ist, ist nach Aufgabe 20.9 auch $\Gamma(M)$ torsionsfrei. Wir können also annehmen, dass M eine torsionsfreie kommutative Gruppe ist. Sei nun

$$\sum_{n \in M} a_n X^n \cdot \sum_{n \in M} b_n X^n = 0.$$

Da hier fast alle Koeffizienten null sind, spielt sich dies in einer endlich erzeugten Untergruppe U der torsionsfreien Gruppe M ab. Nach dem Hauptsatz über endlich erzeugte torsionsfreie kommutative Gruppen ist dann $U \cong \mathbb{Z}^n$. Wir können also sogar $M = \mathbb{Z}^n$ annehmen. Dann ist aber $R[M]$ eine Nenneraufnahme eines Polynomringes über einem Integritätsbereich und damit integer. □

Für ein Monoid ohne Kürzungsregel kann der zugehörige Monoidring über einem Integritätsbereich Nullteiler besitzen.

Beispiel 20.7. Sei M ein Monoid, in dem es zwei verschiedene Elemente m und n gebe mit $m + n = n + n$. Daraus folgt ohne die Kürzungsregel eben nicht $m = n$. Im Monoidring über einem beliebigen Integritätsbereich R und für ein beliebiges Element $a \neq 0$ ist dann $aX^m - aX^n \neq 0$ und $X^n \neq 0$, aber

$$(aX^m - aX^n)X^n = aX^{m+n} - aX^{n+n} = a(X^{2n} - X^{2n}) = 0.$$

Definition 20.8. Sei M ein torsionsfreies kommutatives Monoid mit Kürzungsregel und mit zugehöriger Differenzengruppe $\Gamma(M)$. Dann heißt das Untermonoid

$$\tilde{M} = \{m \in \Gamma(M) : \text{es gibt } r \in \mathbb{N}_+ \text{ mit } rm \in M\}$$

die Normalisierung von M .

Satz 20.9. (Normalisierung von Monoidringen) Sei M ein torsionsfreies kommutatives Monoid mit Kürzungsregel und mit zugehöriger Differenzengruppe $\Gamma(M)$ und mit Normalisierung \tilde{M} , $M \subseteq \tilde{M} \subseteq \Gamma(M)$. Sei R ein normaler Ring. Dann ist die Normalisierung des Monoidringes $R[M]$ der Monoidring $R[\tilde{M}]$. Insbesondere ist der Monoidring zu einem normalen Monoid über einem normalen Ring selbst wieder normal.

Beweis. Zunächst ist

$$R[M] \subseteq R[\tilde{M}] \subseteq R[\Gamma] \subseteq Q(R)[M] \subseteq Q(R[M]).$$

Sei $m \in \tilde{M}$ mit $m = n - k$, $n, k \in M$, und mit $rm = m + m + \dots + m \in M$ (r mal). Damit ist $T^m = T^n/T^k$ ein Element im Quotientenkörper und nach der zweiten Eigenschaft ist $(T^m)^r \in R[M]$. Dies bedeutet, dass eine (reine) Ganzheitsgleichung für T^m vorliegt und damit T^m zur Normalisierung von $R[M]$ gehört.

Für die Umkehrung kann man M durch \tilde{M} ersetzen und sich somit auf den Fall beschränken, wo M normal ist. Man beweist zuerst, dass für eine torsionsfreie Gruppe G der Gruppenring $R[G]$ normal ist, was daraus folgt, dass der Polynomring über einem normalen Bereich wieder normal ist (siehe Aufgabe 20.6). Dann muss man zeigen, dass $R[M]$ in $R[\Gamma(M)]$ ganz abgeschlossen ist. Eine solche Ganzheitsgleichung spielt sich in einer endlich erzeugten Untergruppe $U \subseteq \Gamma(M)$ ab, so dass man $\Gamma(M) = \mathbb{Z}^n$ annehmen darf.

Hier kommt nun etwas konvexe Geometrie ins Spiel, was wir nicht ausführen. Jedenfalls lässt sich ein normales Untermonoid $M \subseteq \mathbb{Z}^n$ darstellen als der Durchschnitt (innerhalb von \mathbb{Q}^n oder \mathbb{R}^n) von \mathbb{Z}^n und einem polyhedrischen Kegel. Ein solcher Kegel ist selbst wiederum der Durchschnitt von endlich vielen Halbräumen H_i (Lemma von Gordan). Dabei ist ein Halbraum H gegeben durch eine lineare Abbildung $p: V = \mathbb{R}^n \rightarrow \mathbb{R}$ mit $H = p^{-1}(\mathbb{R}_+)$. Daraus folgt, dass M ein endlicher Durchschnitt $M = \bigcap_{i \in I} M_i$ ist mit $M_i = p_i^{-1}(\mathbb{N})$. Daraus ergibt sich, dass die M_i eine Form $M_i \cong \mathbb{N} \times \mathbb{Z}^{n-1}$ haben. Damit ist $R[M] = \bigcap_{i \in I} R[M_i]$ normal, da die einzelnen $R[M_i] \cong R[\mathbb{N} \times \mathbb{Z}^{n-1}]$ normal sind. \square

Beispiel 20.10. Wir betrachten die algebraische Fläche, die durch die Gleichung

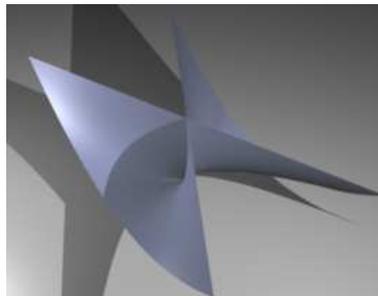
$$X^2Z = Y^2$$

gegeben ist. Wir wollen sie als die Fläche zu einem Monoidring verstehen. Dazu sei

$$M = \{(1, 0), (1, 1), (0, 2) \subset \mathbb{N}^2\}.$$

Wegen $(1, 1) - (1, 0) = (0, 1)$ ist \mathbb{Z}^2 das Quotientengitter (Differenzgruppe). Da $2(0, 1) = (0, 2) \in M$ ist, muss \mathbb{N}^2 die Normalisierung von M sein. Die drei Erzeuger ergeben einen surjektiven Monoidhomomorphismus

$$\mathbb{N}^3 \longrightarrow M, e_i \longmapsto m_i, i = 1, 2, 3.$$



Diese monomiale Abbildung $\mathbb{N}^3 \longrightarrow M \subset \mathbb{N}^2$ bedeutet geometrisch die Abbildung

$$\mathbb{A}_K^2 \longrightarrow K\text{-Spek}(K[M]) \hookrightarrow \mathbb{A}_K^3, (s, t) \longmapsto (s, st, t^2).$$

Dabei gehen (monomial gesehen) $2e_1 + e_3$ und $2e_2$ beide auf das Element $(1, 1)$, und das liefert die Gleichung $X^2Z = Y^2$, die man natürlich auch direkt ablesen kann.

Man kann die definierende Gleichung auch als $Z = \left(\frac{Y}{X}\right)^2$ ansehen. Von $K[X, Y]$ ausgehend wird also ein Quadrat zu $\frac{Y}{X}$ adjungiert.

Beispiel 20.11. Wir betrachten das durch $(1, 0), (-1, 2)$ und $(0, 1)$ erzeugte Untermonoid $M \subseteq \mathbb{Z}^2$. Für den zugehörigen Monoidring gilt $K[M] \cong K[X, Y, Z]/(Z^2 - XY)$. Wir behaupten, dass das Monoid normal ist, also mit seiner Normalisierung übereinstimmt. Die beiden Erzeuger $(1, 0)$ und $(-1, 2)$ definieren je eine Gerade in \mathbb{R}^2 , und das Monoid besteht aus allen Gitterpunkten (Punkte im \mathbb{Z}^2) innerhalb des durch diese Geraden definierten Kegels. Dies sieht man so: die Gitterpunkte in diesem Kegel sind gegeben durch die zwei Bedingungen

$$\{(s, t) \in \mathbb{Z}^2 : t \geq 0 \text{ und } t \geq -2s\}.$$

Ein Punkt daraus mit $s \geq 0$ gehört offensichtlich zu M . Sei also (s, t) ein Punkt daraus mit $s < 0$. Wegen der zweiten linearen Bedingung kann man dann schreiben $(s, t) = (s, -2s) + (t - 2s)(0, 1)$, was wegen $t - 2s \geq 0$ zu M gehört.

Mit den zwei Geraden lässt sich M auch sofort beschreiben als $M = H_1 \cap H_2$ mit $H_1 = \{(s, t) : t \geq 0\} \cong \mathbb{Z} \times \mathbb{N}$ und $H_2 = \{(s, t) : t \geq -2s\} \cong \mathbb{Z} \times \mathbb{N}$, wobei die zweite Identifizierung von der \mathbb{Z} -Basis $(-1, 2), (0, 1)$ herrührt. Aus dieser expliziten Beschreibung folgt, dass der zugehörige Monoidring normal ist.

20.3. Monomiale Kurven und Normalisierung.

Wir werden später sehen, dass eine algebraische Kurve genau dann normal ist, wenn sie nichtsingulär ist. Im Fall einer monomilaen Kurve lässt sich die Normalisierung einfach beschreiben.

Satz 20.12. (Normalisierung von monomialen Kurven) Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde e_1, \dots, e_n erzeugtes Untermonoid, und $K[M] \subseteq K[T]$ die zugehörige Ringerweiterung von Monoidringen. Dann ist $K[T]$ die Normalisierung von $K[M]$. Mit anderen Worten: Die monomiale Abbildung

$$\mathbb{A}_K^1 \longrightarrow K\text{-Spek}(K[M])$$

ist eine Normalisierung.

Beweis. Wir haben $K[M] = K[T^{e_1}, \dots, T^{e_n}] \subseteq K[T]$. Da die Exponenten teilerfremd sind, erzeugen sie die Eins und das bedeutet (multiplikativ betrachtet), dass es ein Monom in diesen Potenzen (auch mit negativen Exponenten) gibt, das gleich T ist. D.h. T ist ein Quotient von Elementen aus $K[M]$ und daher sind die Quotientenkörper gleich. Andererseits erfüllt T eine Ganzheitsgleichung über $K[M]$, bspw. $T^{e_1} - T^{e_1} = 0$. Da $K[T]$ normal ist (sogar faktoriell, da es ja ein Hauptidealbereich ist), muss es sich um die Normalisierung handeln. \square

Monomiale Kurven liefern also eine Vielzahl an Beispielen, wo die Normalisierung auf der Ebene der K -Spektren eine Bijektion ist. Es handelt sich auch um eine Homöomorphie bzgl. der Zariski-Topologie, die ja im Kurvenfall sehr einfach ist. Dennoch wäre es falsch, die beiden Kurven als identisch anzusehen. Die Normalisierung ist (bei $e_i \neq 1$ für alle i) auf der Ringebene keine Bijektion, und in der algebraischen Geometrie darf man nicht nur die mengentheoretische oder topologische Gestalt des Nullstellengebildes anschauen, man darf die Ringe (und die Gleichungen selbst) im Hintergrund nicht völlig vergessen. Den Unterschied sieht man auch in der eingebetteten Situation, wo die Neilsche Parabel eine Spitze besitzt.

Mit der Normalisierung bekommt der Singularitätsgrad einer monomialen Kurve eine neue Interpretation.

Lemma 20.13. Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde Erzeuger definiertes numerisches Monoid. Es sei $R = K[M]$ der zugehörige Monoidring und $R^{\text{norm}} = K[T]$ die Normalisierung davon. Dann gilt für den Singularitätsgrad von M die Gleichung

$$\delta(M) = \dim_K(R^{\text{norm}}/R).$$

Beweis. Die Normalisierung besitzt die K -Basis T^m , $m \in \mathbb{N}$, und der Monoidring $K[M]$ besitzt die K -Basis T^m , $m \in M$. Daher besitzt der Restraum $K[T]/K[M]$ die K -Basis T^m , $m \in \mathbb{N} - M$. Die Dimension des Restraumes ist die Anzahl der Elemente einer Basis, und diese Anzahl ist die Anzahl der Lücken, also der Singularitätsgrad von M . \square

21. VORLESUNG

21.1. Diskrete Bewertungsringe.

Wir setzen nun die lokale Untersuchung von algebraischen Kurven fort und werden im weiteren Verlauf verschiedene Charakterisierungen dafür finden, dass ein Punkt einer Kurve nichtsingulär (oder glatt) ist. Zu dem Punkt P auf der Kurve gehört der lokale Ring in P , der die Lokalisierung des affinen Koordinatenringes der Kurve am maximalen Ideal ist, das zu P gehört. Wenn $P = (a, b) \in C = V(F) \subset \mathbb{A}_K^2$ ist, so lässt sich der lokale Ring in doppelter Weise beschreiben, nämlich als

$$K[X, Y]_{(X-a, Y-b)}/(F) \cong (K[X, Y]/(F))_{\mathfrak{m}}$$

(dabei ist \mathfrak{m} das maximale Ideal aufgefasst im Restklassenring). Dieser Ring beschreibt die wesentlichen algebraischen Eigenschaften des Punktes auf der Kurve. Wichtig ist zunächst der Begriff des diskreten Bewertungsringes.

Definition 21.1. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Lemma 21.2. *Ein diskreter Bewertungsring ist ein lokaler, noetherscher Hauptidealbereich mit genau zwei Primidealen, nämlich 0 und dem maximalen Ideal \mathfrak{m} .*

Beweis. Ein diskreter Bewertungsring ist kein Körper. In einem Hauptidealbereich, der kein Körper ist, wird jedes maximale Ideal von einem Primelement erzeugt, und die Primerzeuger zu verschiedenen maximalen Idealen können nicht assoziiert sein. Also gibt es genau ein maximales Ideal. Ebenso wird jedes von null verschiedene Primideal durch ein Primelement erzeugt, so dass es neben dem maximalen Ideal nur noch das Nullideal gibt. \square

Definition 21.3. Zu einem Element $f \in R$, $f \neq 0$, in einem diskreten Bewertungsring mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichne, die *Ordnung* von f . Sie wird mit $\text{ord}(f)$ bezeichnet.

Die Ordnung ist also nichts anderes als der Exponent zum (bis auf Assoziiertheit) einzigen Primelement in der Primfaktorzerlegung. Sie hat folgende Eigenschaften.

Lemma 21.4. *Sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Dann hat die Ordnung*

$$R - \{0\} \longrightarrow \mathbb{N}, f \longmapsto \text{ord}(f),$$

folgende Eigenschaften.

- (1) $\text{ord}(fg) = \text{ord}(f) + \text{ord}(g)$.
- (2) $\text{ord}(f + g) \geq \min\{\text{ord}(f), \text{ord}(g)\}$.
- (3) $f \in \mathfrak{m}$ genau dann, wenn $\text{ord}(f) \geq 1$.
- (4) $f \in R^\times$ genau dann, wenn $\text{ord}(f) = 0$.

Beweis. Siehe Aufgabe 21.1. □

Wir wollen eine wichtige Charakterisierung für diskrete Bewertungsringe beweisen, die insbesondere beinhaltet, dass ein normaler lokaler Integritätsbereich mit genau zwei Primidealen bereits ein diskreter Bewertungsring ist. Dazu benötigen wir einige Vorbereitungen.

Lemma 21.5. *Sei R ein kommutativer Ring und sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal \mathfrak{p} in R mit $f \notin \mathfrak{p}$.*

Beweis. Wir betrachten die Menge der Ideale

$$M = \{ \mathfrak{a} \text{ Ideal} : f^r \notin \mathfrak{a} \text{ für alle } r \}.$$

Diese Menge ist nicht leer, da sie das Nullideal enthält. Ferner ist sie induktiv geordnet (bzgl. der Inklusion): ist nämlich \mathfrak{a}_i eine total geordnete Teilmenge, so ist deren Vereinigung ebenfalls ein Ideal, das keine Potenz von f enthält. Nach dem Lemma von Zorn gibt es daher maximale Elemente in M .

Wir behaupten, dass ein solches maximales Element \mathfrak{p} ein Primideal ist. Sei dazu $g, h \in R$ und $g, h \in \mathfrak{p}$, und sei $g, h \notin \mathfrak{p}$ angenommen. Dann hat man echte Inklusionen

$$\mathfrak{p} \subset \mathfrak{p} + (g), \mathfrak{p} + (h).$$

Wegen der Maximalität können die beiden Ideale rechts nicht zu M gehören, und das bedeutet, dass es Exponenten $r, s \in \mathbb{N}$ gibt mit

$$f^r \in \mathfrak{p} + (g) \text{ und } f^s \in \mathfrak{p} + (h).$$

Dann ergibt sich der Widerspruch

$$f^r f^s \in \mathfrak{p} + (gh) \subseteq \mathfrak{p}.$$

□

Lemma 21.6. *Sei R ein noetherscher lokaler kommutativer Ring. Es sei vorausgesetzt, dass das maximale Ideal \mathfrak{m} das einzige Primideal von R ist. Dann gibt es einen Exponenten $n \in \mathbb{N}$ mit*

$$\mathfrak{m}^n = 0.$$

Beweis. Wir behaupten zunächst, dass jedes Element in R eine Einheit oder nilpotent ist. Sei hierzu $f \in R$ keine Einheit. Dann ist $f \in \mathfrak{m}$. Angenommen, f ist nicht nilpotent. Dann gibt es nach 21.5 ein Primideal \mathfrak{p} mit $f \notin \mathfrak{p}$. Damit ergibt sich der Widerspruch $\mathfrak{p} \neq \mathfrak{m}$.

Es ist also jedes Element im maximalen Ideal nilpotent. Insbesondere gibt es für ein endliches Erzeugendensystem f_1, \dots, f_k von \mathfrak{m} eine natürliche Zahl m mit $f_i^m = 0$ für alle $i = 1, \dots, k$. Sei $n = km$. Dann ist ein beliebiges Element aus \mathfrak{m}^n von der Gestalt

$$\left(\sum_{i=1}^k a_{i1} f_i \right) \left(\sum_{i=1}^k a_{i2} f_i \right) \cdots \left(\sum_{i=1}^k a_{in} f_i \right).$$

Ausmultiplizieren ergibt eine Linearkombination mit Monomen $f_1^{r_1} \cdots f_k^{r_k}$ und $\sum_{i=1}^k r_i = n$, so dass ein f_i mit einem Exponenten $\geq n/k = m$ vorkommt. Daher ist das Produkt 0. \square

Satz 21.7. *Sei R ein noetherscher lokaler Integritätsbereich mit der Eigenschaft, dass es genau zwei Primideale $0 \subset \mathfrak{m}$ gibt. Dann sind folgende Aussagen äquivalent.*

- (1) R ist ein diskreter Bewertungsring.
- (2) R ist ein Hauptidealbereich.
- (3) R ist faktoriell.
- (4) R ist normal.
- (5) \mathfrak{m} ist ein Hauptideal.

Beweis. (1) \Rightarrow (2) folgt direkt aus der Definition 21.1.

(2) \Rightarrow (3) folgt aus der allgemeinen Aussage, dass jeder Hauptidealbereich faktoriell ist.

(3) \Rightarrow (4) folgt aus Satz 20.4.

(4) \Rightarrow (5). Sei $f \in \mathfrak{m}, f \neq 0$. Dann ist $R/(f)$ ein noetherscher lokaler Ring mit nur einem Primideal (nämlich $\tilde{\mathfrak{m}} = \mathfrak{m}R/(f)$). Daher gibt es nach Lemma 21.5 ein $n \in \mathbb{N}$ mit $\tilde{\mathfrak{m}}^n = 0$. Zurückübersetzt nach R heißt das, dass $\mathfrak{m}^n \subseteq (f)$ gilt. Wir wählen n minimal mit den Eigenschaften

$$\mathfrak{m}^n \subseteq (f) \text{ und } \mathfrak{m}^{n-1} \not\subseteq (f).$$

Wähle $g \in \mathfrak{m}^{n-1}$ mit $g \notin (f)$ und betrachte

$$h := \frac{f}{g} \in Q(R) \text{ (es ist } g \neq 0 \text{)}.$$

Das Inverse, also $h^{-1} = \frac{g}{f}$, gehört nicht zu R , sonst wäre $g \in (f)$. Da R nach Voraussetzung normal ist, ist h^{-1} auch nicht ganz über R . Nach dem Modulkriterium Lemma 19.9 für die Ganzheit gilt insbesondere für das maximale Ideal $\mathfrak{m} \subset R$ die Beziehung

$$h^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$$

ist. Nach Wahl von g ist aber auch

$$h^{-1}\mathfrak{m} = \frac{g}{f}\mathfrak{m} \subseteq \frac{\mathfrak{m}^n}{f} \subseteq R.$$

Daher ist $h^{-1}\mathfrak{m}$ ein Ideal in R , das nicht im maximalen Ideal enthalten ist. Also ist $h^{-1}\mathfrak{m} = R$. Das heißt einerseits $h \in \mathfrak{m}$ und andererseits gilt für ein beliebiges $x \in \mathfrak{m}$ die Beziehung $h^{-1}x \in R$, also $x = h(h^{-1}x)$, also $x \in (h)$ und somit $(h) = \mathfrak{m}$.

(5) \Rightarrow (1). Sei $\mathfrak{m} = (\pi)$. Dann ist π ein Primelement und zwar bis auf Assoziiertheit das einzige. Sei $f \in R, f \neq 0$ keine Einheit. Dann ist $f \in \mathfrak{m}$ und daher $f = \pi g_1$. Dann ist g_1 eine Einheit oder $g_1 \in \mathfrak{m}$. Im zweiten Fall ist wieder $g_1 = \pi g_2$ und $f = \pi^2 g_2$.

Wir behaupten, dass man $f = \pi^k u$ mit einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Lemma 21.5 gibt es ein $m \in \mathbb{N}$ mit $(\pi^m) = \mathfrak{m}^m \subseteq (f)$. Bei $n \geq m + 1$ ergibt sich $\pi^m = af = a\pi^{m+1}b$ und der Widerspruch $1 = ab\pi$.

Es lässt sich also jede Nichteinheit $\neq 0$ als Produkt einer Potenz des Primelements mit einer Einheit schreiben. Insbesondere ist R faktoriell. Für ein beliebiges Ideal $\mathfrak{a} = (f_1, \dots, f_s)$ ist $f_i = \pi^{n_i} u_i$ mit Einheiten u_i . Dann sieht man leicht, dass $\mathfrak{a} = (\pi^n)$ ist mit $n = \min_i \{n_i\}$. \square

21.2. Das Lemma von Nakayama.

Nach dem vorangehenden Überlegungen liegt ein diskreter Bewertungsring genau dann vor, wenn der lokale Integritätsbereich die Eigenschaft hat, dass das maximale Ideal durch ein Element erzeugt wird. Es ist von daher naheliegend, generell die lokalen Ringe zu Punkten auf einer algebraischen Kurve dahingehend zu studieren, wie viele Erzeuger das maximale Ideal benötigt. Dies führt zum Begriff der Einbettungsdimension, den wir schon im Zusammenhang mit monomialen Kurven erwähnt haben. Diese Einbettungsdimension ist auch die Dimension des R/\mathfrak{m} -Vektorraumes $\mathfrak{m}/\mathfrak{m}^2$, für diesen Zusammenhang brauchen wir aber einige Vorbereitungen und insbesondere das Lemma von Nakayama.

Im Lemma von Nakayama wird folgende Konstruktion betrachtet: zu einem R -Modul V , einem Untermodul $U \subseteq V$ und einem Ideal $I \subseteq R$ bezeichnet man mit IU den R -Untermodul von V , der von allen Elementen der Form fv , $f \in I$, $v \in U$, erzeugt wird (dies ist auch ein R -Untermodul von U). Ist U ebenfalls ein Ideal (also ein R -Untermodul von R), so fällt dieses Konzept mit dem Produkt von Idealen zusammen. Der Restklassenmodul V/IV ist dabei in natürlicher Weise nicht nur ein R -Modul, sondern auch ein R/I -Modul. Wenn I ein maximales Ideal ist, so bedeutet dies, dass der Restklassenmodul sogar ein Vektorraum über dem Restklassenkörper ist.

Lemma 21.8. (*Lemma von Nakayama*) Sei (R, \mathfrak{m}) ein lokaler Ring und sei V ein endlich erzeugter R -Modul. Es sei $\mathfrak{m}V = V$ vorausgesetzt. Dann ist $V = 0$.

Beweis. Sei v_1, \dots, v_n ein Erzeugendensystem von V . Nach Voraussetzung gibt es wegen $v_i \in \mathfrak{m}V$ zu jedem v_i eine Darstellung

$$v_i = a_{i1}v_1 + \dots + a_{in}v_n$$

mit $a_{ij} \in \mathfrak{m}$. Daraus ergibt sich für jedes i eine Darstellung

$$(1 - a_{ii})v_i = a_{i1}v_1 + \dots + a_{i,i-1}v_{i-1} + a_{i,i+1}v_{i+1} + \dots + a_{in}v_n.$$

Da $a_{ii} \in \mathfrak{m}$ ist, ist der Koeffizient $1 - a_{ii}$ eine Einheit. Dies bedeutet aber, dass man nach v_i auflösen kann, so dass also v_i überflüssig ist. So kann man sukzessive auf alle Erzeuger verzichten, was bedeutet, dass der Nullmodul vorliegen muss. \square

22. VORLESUNG

22.1. Die Einbettungsdimension.

Definition 22.1. Es sei R ein lokaler kommutativer noetherscher Ring mit maximalem Ideal \mathfrak{m} . Dann heißt die minimale Idealerzeugendenzahl für \mathfrak{m} die *Einbettungsdimension* von R , geschrieben

$$\text{embdim}(R).$$

Ein noetherscher lokaler Integritätsbereich der Dimension eins (d.h. die einzigen Primideale sind das Nullideal und das maximale Ideal) ist genau dann ein diskreter Bewertungsring, wenn seine Einbettungsdimension 1 ist. Wir erwähnen, dass die Einbettungsdimension immer zumindest so groß ist wie die Dimension eines lokalen Ringes. Die Ringe, bei denen Gleichheit gilt, spielen eine besondere Rolle und heißen *reguläre Ringe*. Wir sind der Einbettungsdimension schon im Fall von monomialen Kurven begegnet und müssen zeigen, dass die dortige Definition (18.7) mit der neuen verträglich ist.

Wir beweisen zunächst eine andere Charakterisierung, die sich aus dem Lemma von Nakayama ergibt.

Lemma 22.2. *Sei (R, \mathfrak{m}, K) ein lokaler Ring und sei V ein endlich erzeugter R -Modul. Dann stimmt die minimale Erzeugendenzahl $\mu(V)$ mit der Dimension des K -Vektorraums $V/\mathfrak{m}V$ überein.*

Beweis. Wir zeigen etwas allgemeiner, dass Elemente $v_1, \dots, v_n \in V$ genau dann ein R -Erzeugendensystem für V bilden, wenn deren Restklassen in $V/\mathfrak{m}V$ ein R/\mathfrak{m} -Erzeugendensystem von $V/\mathfrak{m}V$ bilden. Dabei ist die eine Richtung trivial, seien also Elemente $v_1, \dots, v_n \in V$ gegeben, die modulo \mathfrak{m} erzeugen. Es sei $U \subseteq V$ der von den v_i erzeugte R -Untermodul von V . Die Voraussetzung übersetzt sich zu $V = U + \mathfrak{m}V$. Wir betrachten den Restklassenmodul V/U . Dort gilt dann $(V/U)\mathfrak{m} = V/U$, woraus nach dem Lemma von Nakayama die Gleichheit $V/U = 0$ und $V = U$ folgt. \square

Korollar 22.3. *Sei (R, \mathfrak{m}, K) ein noetherscher lokaler Ring. Dann ist die Einbettungsdimension gleich*

$$\mu(\mathfrak{m}) = \dim_K(\mathfrak{m}/\mathfrak{m}^2).$$

Beweis. Dies folgt sofort aus Lemma 22.2 angewandt auf das Ideal \mathfrak{m} und den endlich erzeugten R -Modul \mathfrak{m} . \square

Den in der vorstehenden Aussage auftretenden R -Modul $\mathfrak{m}/\mathfrak{m}^2$, der ein Vektorraum über R/\mathfrak{m} ist, nennt man auch den *Kotangentenraum* des lokalen Ringes.

Lemma 22.4. *Sei R ein noetherscher kommutativer Ring und \mathfrak{n} ein maximales Ideal. Es sei $S = R_{\mathfrak{n}}$ die Lokalisierung an \mathfrak{n} mit dem maximalen Ideal*

$\mathfrak{m} = \mathfrak{n}R_{\mathfrak{n}}$. Dann ist

$$\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{n}/\mathfrak{n}^2.$$

Insbesondere ist die Einbettungsdimension der Lokalisierung gleich $\dim_{R/\mathfrak{n}}(\mathfrak{n}/\mathfrak{n}^2)$.

Beweis. Bekanntlich ist $R/\mathfrak{n} \cong R_{\mathfrak{m}}/\mathfrak{m}$, so dass der gleiche Körper zugrunde liegt. Der natürliche R -Modul-Homomorphismus $\mathfrak{n} \rightarrow \mathfrak{m}$ induziert einen K -Vektorraum-Homomorphismus

$$\mathfrak{n}/\mathfrak{n}^2 \longrightarrow \mathfrak{m}/\mathfrak{m}^2,$$

der surjektiv ist, da R -Modul-Erzeuger von \mathfrak{n} auf $R_{\mathfrak{n}}$ -Erzeuger von \mathfrak{m} abbilden, und diese modulo \mathfrak{m}^2 ein K -Vektorraum-Erzeugendensystem ergeben. Sei also $f \in \mathfrak{n}$ ein Element, das rechts auf null abgebildet wird. D.h. es gilt $f \in \mathfrak{m}^2$ in der Lokalisierung $R_{\mathfrak{n}}$. Dies bedeutet wiederum, dass es Elemente $g_1, \dots, g_n \in \mathfrak{n}$ und $h_1, \dots, h_n \in \mathfrak{n}$ und ein Element $s \notin \mathfrak{n}$ (im integren Fall - allgemein ist das Argument unwesentlich komplizierter) gibt mit

$$sf = g_1h_1 + \dots + g_nh_n.$$

Da s nicht zum maximalen Ideal gehört, gibt es $r \in R$ und $g \in \mathfrak{n}$ mit $g + rs = 1$. Wir multiplizieren die obige Gleichung mit r und erhalten

$$(1 - g)f = r(g_1h_1 + \dots + g_nh_n)$$

bzw.

$$f = r(g_1h_1 + \dots + g_nh_n) + gf.$$

Dabei gehört die rechte Seite offensichtlich zu \mathfrak{n}^2 , und damit definiert f das Nullelement in $\mathfrak{n}/\mathfrak{n}^2$. \square

Lemma 22.5. *Sei K ein Körper und M ein numerisches Monoid, das von teilerfremden natürlichen Zahlen erzeugt sei. Es sei $R = K[M]$ der zugehörige Monoidring mit dem maximalen Ideal $\mathfrak{n} = (M_+)$ und der Lokalisierung $R_{\mathfrak{n}}$. Dann ist die numerische Einbettungsdimension von M (bzw. $K[M]$) gleich der Einbettungsdimension des lokalen Rings $R_{\mathfrak{n}}$.*

Beweis. Es ist $\mathfrak{n} = (M_+) = \bigoplus_{m \in M_+} K T^m$ und $\mathfrak{n}^2 = (2M_+) = \bigoplus_{m \in 2M_+} K T^m$. Der Restklassenraum ist daher

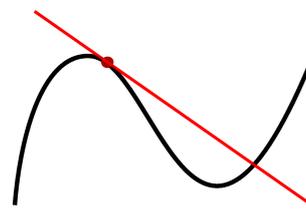
$$\mathfrak{n}/\mathfrak{n}^2 = \bigoplus_{m \in M_+ - 2M_+} K T^m.$$

Dessen K -Dimension ist also gleich der Anzahl der Elemente aus $M_+ - 2M_+$. Nach Korollar 18.13 ist $M_+ - 2M_+$ das minimale Monoiderzeugendensystem von M , sodass die Dimension gleich der numerischen Einbettungsdimension ist.

Andererseits ist nach Lemma 22.4 die Dimension von $\mathfrak{n}/\mathfrak{n}^2$ gleich der Einbettungsdimension des zugehörigen lokalen Rings $R_{\mathfrak{n}}$. \square

22.2. Glatte und singuläre Punkte.

Sei K ein Körper und $F \in K[X, Y], F \neq 0$, ein Polynom ohne mehrfache Faktoren (da wir uns nur für die zugehörige Kurve interessieren, ist dies bei einem algebraisch abgeschlossenen Körper aufgrund des Hilbertschen Nullstellensatzes keine Einschränkung).



Für jeden Punkt $(a, b) \in \mathbb{A}_K^2$, kann man zu den Variablen $X - a$ und $Y - b$ übergehen. Das bedeutet, dass man den Punkt in den Ursprung verschiebt. Für das Verhalten eines Polynoms an einem Punkt kann man sich also stets auf den Ursprungspunkt beschränken.

Sei also $P = (0, 0)$. Wir schreiben F mit homogenen Komponenten als

$$F = F_d + F_{d-1} + \dots + F_1 + F_0.$$

Hier sind die F_i homogen vom Grad i . Was kann man an den einzelnen homogenen Komponenten ablesen? Zunächst gilt trivialerweise die Beziehung

$$P \in V(F) \text{ genau dann, wenn } F_0 = 0.$$

Wenn man die Koordinaten von P , also $(0, 0)$, in F einsetzt, so werden ja alle höheren Komponenten zu null gemacht, und lediglich die konstante Komponente F_0 bleibt übrig. Da wir uns hauptsächlich für das Verhalten der Kurve in einem Kurvenpunkt interessieren, werden wir uns häufig auf die Situation $F_0 = 0$ beschränken. Was ist dann die erste homogene Komponente F_i , die nicht null ist? Welche Rolle spielt dieses i und welche Rolle spielen dessen Linearfaktoren?

Nehmen wir zunächst an, dass $F_0 = 0$ und $F_1 = aX + bY$ ist. Diese Linearform (die null sein kann) lässt sich auch mit partiellen Ableitungen charakterisieren, es ist nämlich

$$\frac{\partial F}{\partial x}(P) = a \text{ und } \frac{\partial F}{\partial y}(P) = b.$$

Hier und im Folgenden werden Polynome einfach *formal abgeleitet*. Damit ist auch $F_1 = 0$ genau dann, wenn $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0$ ist. Wenn dies nicht der Fall ist, so ist es naheliegend, die durch die Gleichung $F_1(X, Y) = 0$ definierte Gerade als Tangente an die Kurve im Punkt P anzusehen. Ein erstes Indiz dafür ist, dass im linearen Fall $F = F_1$ die Gerade mit ihrer Tangente zusammenfallen soll.

Definition 22.6. Sei K ein Körper und $F \in K[X, Y]$ ein von null verschiedenes Polynom. Es sei $P \in C = V(F) \subset \mathbb{A}_K^2$ ein Punkt der zugehörigen affinen ebenen Kurve. Dann heißt P ein *glatter Punkt* von C , wenn gilt

$$\frac{\partial F}{\partial X}(P) \neq 0 \text{ oder } \frac{\partial F}{\partial Y}(P) \neq 0.$$

Andernfalls heißt der Punkt *singulär*.

Definition 22.7. Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X, Y]$ ein von null verschiedenes Polynom. Es sei $P \in C = V(F) \subset \mathbb{A}_K^2$ ein Punkt der zugehörigen affinen ebenen Kurve, der (nach linearer Variablentransformation) der Nullpunkt sei. Es sei

$$F = F_d + F_{d-1} + \dots + F_m$$

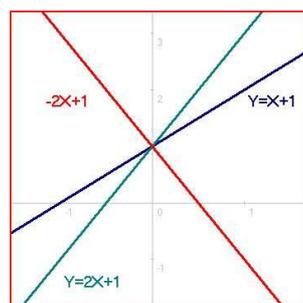
die homogene Zerlegung von F mit $F_d \neq 0$ und $F_m \neq 0$, $d \geq m$. Dann heißt m die *Multiplizität* der Kurve im Punkt P . Sei $F_m = G_1 \cdots G_m$ die Zerlegung in lineare Faktoren. Dann nennt man jede Gerade $V(G_i)$, $i = 1, \dots, m$, eine *Tangente* an C im Punkt P . Die Vielfachheit von G_i in F_m nennt man auch die *Multiplizität* der Tangente.

Der Punkt ist genau dann glatt, wenn die Multiplizität eins ist. In diesem Fall gibt es genau eine Tangente durch den Punkt, deren Steigung man über die partiellen Ableitungen berechnen kann.

Beispiel 22.8. Seien d verschiedene Geraden L_1, \dots, L_d in der affinen Ebene gegeben, die alle durch den Nullpunkt laufen mögen. Es seien $a_i X + b_i Y = 0$, $i = 1, \dots, d$, die zugehörigen Gleichungen (die nur bis auf einen Skalar definiert sind). Die Vereinigung dieser Geraden wird dann durch das Produkt

$$F = (a_1 X + b_1 Y) \cdots (a_d X + b_d Y)$$

beschrieben. Insbesondere ist $F = F_d$ homogen vom Grad d . Hier definiert jeder Linearfaktor eine Tangente durch den Nullpunkt.



Geraden, die sich im Punkt $(0,1)$ schneiden

Bemerkung 22.9. Für einen glatten Punkt $P \in C = V(F)$ einer ebenen algebraischen Kurve ist die Multiplizität $m = 1$. Bei $P = (0,0)$ ist also der lineare Term der Kurvengleichung $F_1 = uX + vY \neq 0$ und es ist

$$\frac{\partial F}{\partial X}(P) = u \text{ und } \frac{\partial F}{\partial Y}(P) = v$$

(da die höheren homogenen Komponenten von F keinen Beitrag zu den partiellen Ableitungen im Nullpunkt leisten). Diese lineare Gleichung ist also die Tangentengleichung. Auch für einen beliebigen glatten Punkt $P = (a, b) \in C$ kann man aus den partiellen Ableitungen von F in P direkt die Tangentengleichung ablesen, und zwar ist die Tangente gegeben durch

$$\frac{\partial F}{\partial X}(P)(X - a) + \frac{\partial F}{\partial Y}(P)(Y - b) = 0.$$

Bemerkung 22.10. Sei $F \in K[X, Y]$ mit zugehöriger ebener algebraischer Kurve C und sei $P \in C = V(F)$ ein glatter Punkt der Kurve. Zu $F : \mathbb{A}_K^2 \rightarrow \mathbb{A}_K^1$ und dem Punkt P gehört die durch die partiellen Ableitungen definierte lineare *Tangentialabbildung* (das *totale Differential*) zwischen den zugehörigen Tangentialräumen, also

$$T_P F = \left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P) \right) : T_P \mathbb{A}_K^2 \cong \mathbb{A}_K^2 \longrightarrow T_{F(P)} \mathbb{A}_K^1 = T_0 \mathbb{A}_K^1 \cong \mathbb{A}_K^1$$

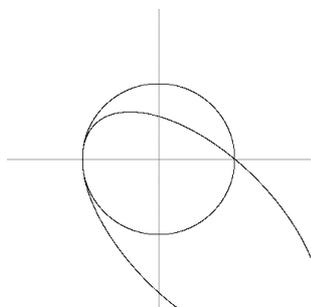
$$\text{mit } (s, t) \longmapsto \frac{\partial F}{\partial X}(P)s + \frac{\partial F}{\partial Y}(P)t$$

Da P ein glatter Punkt ist, ist diese lineare Abbildung nicht die Nullabbildung. Die (Richtung der) Tangente von C an P ist der Kern dieser Tangentialabbildung (wobei man bei der Identifizierung der Tangentialebene in P mit der umgebenden affinen Ebene den Punkt P mit dem Nullpunkt identifizieren muss. Die Tangente muss ja durch den Punkt gehen, der Kern gibt nur eine lineare Richtung vor.)

Die folgenden beiden Aussagen zeigen, dass ein Kreuzungspunkt zweier irreduzibler Komponenten niemals glatt sein kann.

Lemma 22.11. *Sei $C = V(F)$ eine ebene algebraische Kurve und $F = F_1 \cdots F_n$ die Zerlegung in verschiedene Primfaktoren. Es sei $P \in C$ ein glatter Punkt der Kurve. Dann liegt P auf nur einer Komponente $C_i = V(F_i)$ der Kurve.*

Beweis. Siehe Aufgabe 22.5. □



Bei einer algebraischen Kurve sind die Schnittpunkte von irreduziblen Komponenten niemals glatt.

Korollar 22.12. *Sei $C \subseteq \mathbb{A}_K^2$ eine ebene glatte algebraische Kurve über einem algebraisch abgeschlossenen Körper. Dann ist C irreduzibel.*

Beweis. Aufgrund von Lemma 22.11 sind die irreduziblen Komponenten der Kurve disjunkt. Dies sind dann aber auch die Zusammenhangskomponenten der Kurve. Also gibt es nur eine irreduzible Komponente und daher ist die Kurve irreduzibel. □

Satz 22.13. *Sei K ein Körper und R eine K -Algebra von endlichem Typ, und sei $P \in K - \text{Spek}(R)$ ein Punkt mit zugehörigem maximalem Ideal \mathfrak{m} . Dann ist die Abbildung*

$$d : R \longrightarrow \mathfrak{m}/\mathfrak{m}^2, f \longmapsto df := \overline{f - f(P)}$$

eine Derivation, d.h. d ist K -linear und es gilt $d(fg) = f dg + g df$.

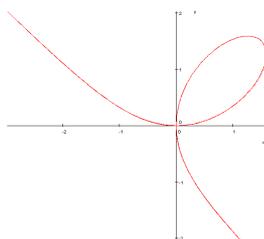
Beweis. Zunächst ist die Abbildung wohldefiniert, da wegen $(f - f(P))(P) = 0$ die Funktion $f - f(P)$ zum maximalen Ideal gehört. Die K -Linearität ist trivial. Die Produktregel folgt aus (im dritten Schritt wird ein Element aus \mathfrak{m}^2 addiert)

$$\begin{aligned}
 d(fg) &= fg - (fg)(P) \\
 &= fg - f(P)g(P) \\
 &= fg - f(P)g(P) + (f - f(P))(g - g(P)) \\
 &= 2fg - fg(P) - gf(P) \\
 &= f(g - g(P)) + g(f - f(P)) \\
 &= fdg + gdf.
 \end{aligned}$$

□

23. VORLESUNG

Beispiel 23.1. (Kartesisches Blatt)



Das Kartesische Blatt wird durch die Gleichung $F = X^3 + Y^3 - 3XY = 0$ beschrieben (die 3 ist dabei nicht wichtig, und könnte durch eine andere Zahl $\neq 0$ ersetzt werden). Die homogenen Bestandteile der Kurvengleichung sind $F_3 = X^3 + Y^3$ und $F_2 = -3XY$. Damit hat der Nullpunkt des Kartesischen Blattes die Multiplizität zwei und ist singulär, und sowohl die X - als auch die Y -Achse sind Tangenten (mit einfacher Multiplizität). An den übrigen Punkten ist die Kurve glatt (der Grundkörper habe nicht die Charakteristik

3): aus

$$\frac{\partial F}{\partial X} = 3X^2 - 3Y = 0 \text{ und } \frac{\partial F}{\partial Y} = 3Y^2 - 3X = 0$$

folgt $Y = X^2$ und $X = Y^2$, also auch $Y = Y^4$ (ebenso für X). Dann ist $Y = X = 0$ oder X und Y sind beide eine dritte Einheitswurzel (und zwar sind beide 1 oder es sind die beiden anderen dritten Einheitswurzeln). An diesen anderen Verschwindungsstellen der beiden partiellen Ableitungen hat aber F den Wert -1 , diese sind also keine Punkte der Kurve.

23.1. Glatte und normale Punkte.

Wir wollen zeigen, dass ein Punkt auf einer ebenen algebraischen Kurve genau dann glatt ist, wenn der zugehörige lokale Ring ein diskreter Bewertungsring ist. Dabei ist die Glattheit in einem Punkt extrinsisch unter Bezug auf die umgebende Ebene definiert worden, während die Eigenschaft, ein diskreter Bewertungsring zu sein, nur vom Koordinatenring der Kurve abhängt. Das folgende Lemma erledigt die eine Richtung, für die andere Richtung müssen wir zuerst eine intrinsische Multiplizität für einen lokalen Ring entwickeln.

Lemma 23.2. *Sei K ein Körper, $F \in K[X, Y]$ ein Polynom $\neq 0$ ohne mehrfache Faktoren und sei $P \in C = V(F)$ ein glatter Punkt der Kurve. Es sei R der lokale Ring der Kurve im Punkt P . Dann ist R ein diskreter Bewertungsring.*

Beweis. Zunächst ist R ein noetherscher lokaler Ring, der aufgrund von Korollar 22.12 ein Integritätsbereich ist. Daher sind die einzigen Primideale das Nullideal und das maximale Ideal \mathfrak{m}_P . Wir werden zeigen, dass das maximale Ideal ein Hauptideal ist.

Wir können annehmen, dass P der Nullpunkt ist, und schreiben F als

$$F = F_d + \dots + F_1$$

mit $F_1 \neq 0$. Da P glatt ist, liegt eine solche Gestalt vor. Durch eine Variablentransformation können wir erreichen, dass $F_1 = Y$ ist. Wir können in F die isoliert stehenden Potenzen von X (die Monome, wo kein Y vorkommt) zusammenfassen und bei den anderen Y ausklammern. Dann lässt sich die Gleichung $F = 0$ schreiben als

$$Y(1 + G) = XH(X),$$

wobei $G \in (X, Y)$ ist. Es ist dann $1 + G$ eine Einheit in $K[X, Y]_{(X, Y)}$ und erst recht im lokalen Ring $R = K[X, Y]_{(X, Y)}/(F)$ der Kurve. Daher gilt in R die Beziehung

$$Y = \frac{H}{1 + G}X.$$

Also wird das maximale Ideal im lokalen Ring R von X allein erzeugt, so dass nach Satz 21.7 ein diskreter Bewertungsring vorliegt. \square

23.2. Die Hilbert-Samuel Multiplizität.

Lemma 23.3. *Sei R ein noetherscher lokaler Ring mit maximalem Ideal \mathfrak{m} und Restklassenkörper $K = R/\mathfrak{m}$. Dann besitzen die Restklassenmoduln $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ endliche Dimension über K . Wenn R einen Körper K enthält, der isomorph auf den Restklassenkörper abgebildet wird, so sind auch die Restklassenringe R/\mathfrak{m}^n von endlicher Dimension über K .*

Beweis. Wir schreiben den Restklassenmodul $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ als

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong \mathfrak{m}^n/(\mathfrak{m}^n)\mathfrak{m}.$$

Damit sind wir in der Situation von Lemma 22.2. Da \mathfrak{m}^n ein endlich erzeugtes Ideal ist, folgt, dass dieser Restklassenmodul endliche Dimension über dem Restklassenkörper besitzt.

Für die Restklassenringe betrachten wir die kurze exakte Sequenz von R -Moduln,

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow R/\mathfrak{m}^{n+1} \longrightarrow R/\mathfrak{m}^n \longrightarrow 0.$$

Dies ist nach unserer Voraussetzung auch eine kurze exakte Sequenz von K -Vektorräumen, so dass sich die K -Dimensionen addieren. Nach dem bereits bewiesenen steht links ein endlichdimensionaler Raum. Die Aussage folgt nun durch Induktion über n aus dieser Sequenz, wobei der Induktionsanfang durch $R/\mathfrak{m} = K$ gesichert ist. \square

Im Fall einer ebenen algebraischen Kurve $V = V(F) \subset \mathbb{A}_K^2$ und einem Punkt $P = (a, b) \in V$ ist der lokale Ring gegeben durch $K[X, Y]_{(X-a, Y-b)}/(F)$. Der Restklassenkörper dieses lokalen Ringes ist K selbst. Daher sind die Voraussetzungen, die im vorstehenden Lemma auftauchen, alle erfüllt, und alle Dimensionen sind Dimensionen über dem Grundkörper.

Satz 23.4. *(Intrinsische Charakterisierung der Multiplizität) Sei $P \in V = V(F) \subset \mathbb{A}_K^2$ ein Punkt auf einer ebenen affinen Kurve. Es sei $R = \mathcal{O}_{V,P}$ der zugehörige lokale Ring mit maximalem Ideal \mathfrak{m} . Dann gilt für die Multiplizität m_P von P die Gleichung*

$$m_P = \dim_K (\mathfrak{m}^n/\mathfrak{m}^{n+1}) \text{ für } n \text{ hinreichend groß.}$$

Beweis. Wir betrachten die kurze exakte Sequenz

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow R/\mathfrak{m}^{n+1} \longrightarrow R/\mathfrak{m}^n \longrightarrow 0$$

von K -Vektorräumen. Nach Lemma 23.3 sind die Dimensionen endlich. Dass die Dimensionen von $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ konstant gleich der Multiplizität sind (für n hinreichend groß) ist äquivalent dazu, dass die Differenz zwischen den Dimensionen von R/\mathfrak{m}^{n+1} und R/\mathfrak{m}^n konstant gleich der Multiplizität ist für n hinreichend groß. Dies ist durch Induktion äquivalent dazu, dass

$$\dim(R/\mathfrak{m}^n) = nm_P + c$$

gilt für eine Konstante c und n hinreichend groß. Wir können durch Verschieben der Situation annehmen, dass P der Nullpunkt in der Ebene ist. Sei $\mathfrak{a} = (X, Y)$ das zugehörige maximale Ideal in $S = K[X, Y]$. Dann ist $K[X, Y]/(\mathfrak{a}^n + (F)) = R/\mathfrak{m}^n$, so dass die Aussage dafür zu zeigen ist.

Nach Voraussetzung hat F die Gestalt $F = F_m + F_{m+1} \dots$ mit $m = m_P$. Damit ist insbesondere $F \in \mathfrak{a}^m$. Für ein weiteres Polynom $G \in \mathfrak{a}^{n-m}$ (mit $n \geq m$) ist $GF \in \mathfrak{a}^n$. Daher liegt eine kurze exakte Sequenz

$$0 \longrightarrow S/\mathfrak{a}^{n-m} \xrightarrow{F} S/\mathfrak{a}^n \longrightarrow S/(\mathfrak{a}^n, F) = R/\mathfrak{m}^n \longrightarrow 0$$

vor. Dabei folgt die Injektivität links aus einer direkten Gradbetrachtung. Bekanntlich ist die Dimension von S/\mathfrak{a}^n gleich $n(n+1)/2$. Daher ergibt sich für $n \geq m$ die Gleichheit

$$\begin{aligned} \dim(R/\mathfrak{m}^n) &= \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} \\ &= \frac{n^2+n-(n-m)^2-n+m}{2} \\ &= \frac{2nm-m^2+m}{2} \\ &= nm - \frac{m(m-1)}{2}. \end{aligned}$$

Dies ist die Behauptung. \square

Bemerkung 23.5. Satz 23.3 besagt insbesondere, dass die Multiplizität eines Punktes auf einer ebenen Kurve eine Invariante des lokalen Ringes der Kurve in dem Punkt ist, und damit insbesondere nur von intrinsischen Eigenschaften der Kurve abhängt, nicht von der Realisierung in einer umgebenden Ebene. Es gibt für jeden noetherschen lokalen Ring die sogenannte *Hilbert-Samuel Multiplizität*, die über die R/\mathfrak{m} -Dimensionen der Restklassenmoduln $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ definiert wird. Im eindimensionalen Fall ist sie definiert als

$$\lim_{n \rightarrow \infty} (\dim_{R/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1})),$$

wobei diese Funktion konstant wird (was nicht trivial ist). Wenn R einen Körper K enthält, der isomorph zum Restkörper ist (was bei lokalen Ringen zu einer Kurve der Fall ist), so ist diese Zahl auch gleich

$$\lim_{n \rightarrow \infty} (\dim_K(R/\mathfrak{m}^n)).$$

Satz 23.6. (*Glattheit und Normalität*) Sei K ein Körper und sei $F \in K[X, Y]$ nichtkonstant ohne mehrfachen Faktor mit zugehöriger algebraischer Kurve $C = V(F)$. Es sei $P = (a, b) \in C$ ein Punkt der Kurve mit maximalem Ideal $\mathfrak{m} = (X - a, Y - b)$ und mit lokalem Ring $R = (K[X, Y]_{\mathfrak{m}})/(F)$. Dann sind folgende Aussagen äquivalent.

- (1) P ist ein glatter Punkt der Kurve.
- (2) R ist ein diskreter Bewertungsring.
- (3) R ist ein normaler Integritätsbereich.
- (4) Die Multiplizität von P ist eins.

Beweis. Die Implikation (1) \Rightarrow (2) wurde in Lemma 23.1 bewiesen. Die Äquivalenz (2) \Leftrightarrow (3) wurde in Satz 21.7 bewiesen. Die Äquivalenz (1) \Leftrightarrow (4) folgt

aus der Definition 22.7 der Multiplizität. Es bleibt also (2) \Rightarrow (4) zu zeigen, wobei wir unter Verwendung von Satz 23.3 mit der Hilbert-Samuel Multiplizität arbeiten können. Es genügt also zu zeigen, dass für einen lokalen Ring einer ebenen algebraischen Kurve, der ein diskreter Bewertungsring ist, die Restklassenmoduln $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong \mathfrak{m}^n/\mathfrak{m}^n\mathfrak{m}$ alle eindimensional über dem Restklassenkörper $R/\mathfrak{m} \cong K$ sind. Dies folgt aber wegen $\mathfrak{m}^n = (\pi^n)$ direkt aus dem Lemma von Nakayama 21.8. \square

23.3. Monomiale Kurven und Multiplizität.

Zu einem numerischen Monoid $M \subseteq \mathbb{N}$ das von teilerfremden natürlichen Zahlen $e_1 < e_2 < \dots < e_r$ erzeugt werde, wird der minimale Erzeuger, also e_1 , auch als *Multiplizität* bezeichnet. Es ist zu zeigen, dass dies die richtige Multiplizität ergibt. Dazu sei

$$M_+ = \{m \in M : m \geq 1\}$$

und

$$nM_+ = \{m \in M : \text{es gibt eine Darstellung } m = m_1 + \dots + m_n \text{ mit } m_i \in M_+\}.$$

Dies sind offensichtlich Monoid-Ideale von M . Es folgt, dass die zugehörigen Mengen $K[nM_+] = \bigoplus_{m \in nM_+} K T^m$ Ideale im Monoidring sind. Und zwar ist $\mathfrak{m} = K[M_+]$ ein maximales Ideal, und die Potenzen davon sind $\mathfrak{m}^n = K[nM_+]$.

Lemma 23.7. *Sei $M \subseteq \mathbb{N}$ ein numerisches Monoid mit (numerischer) Multiplizität e_1 und sei ℓ eine Zahl mit $\mathbb{N}_{\geq \ell} \subseteq M$. Dann gelten für die Mächtigkeit der Differenzmenge $M - nM_+$ die Abschätzungen*

$$ne_1 - \ell \leq \#(M - nM_+) \leq (n - 1)e_1 + \ell.$$

Beweis. Die Abschätzung nach unten folgt daraus, dass die kleinste Zahl in nM_+ genau ne_1 ist, die natürlichen Zahlen $0, 1, \dots, ne_1 - 1$ liegen also außerhalb davon. Dabei liegen die Zahlen $\geq \ell$ in M , so dass von diesen ne_1 Zahlen mindestens $ne_1 - \ell$ zu M gehören.

Zur Abschätzung nach oben behaupten wir, dass alle Zahlen $\geq (n - 1)e_1 + \ell$ zu nM_+ gehören. Sei $x \geq (n - 1)e_1 + \ell$. Dann ist $x = (n - 1)e_1 + \ell'$ mit $\ell' \geq \ell$ und daher ist $\ell' \in M$. Also liegt direkt eine Zerlegung von x in n Summanden aus M vor. \square

Korollar 23.8. *Es sei $M \subseteq \mathbb{N}$ ein von teilerfremden Zahlen erzeugtes numerisches Monoid mit numerischer Multiplizität e_1 . Es sei $\mathfrak{m} = (M_+)$ das maximale Ideal des Monoidringes $K[M]$, das dem Nullpunkt entspricht. Dann gilt*

$$\lim_{n \rightarrow \infty} \frac{\dim_K(K[M]/\mathfrak{m}^n)}{n} = e_1.$$

Das heißt, dass die numerische Multiplizität mit der Hilbert-Samuel Multiplizität übereinstimmt.

Beweis. Der Restklassenring $K[M]/\mathfrak{m}^n = K[M]/(nM_+)$ hat die Elemente aus $M - nM_+$ als K -Basis. Deren Anzahl ist also die Dimension davon. Aufgrund der in Lemma 23.6 bewiesenen Abschätzungen konvergiert der Ausdruck $\frac{\#(M - nM_+)}{n}$ für $n \mapsto \infty$ gegen e_1 . Daher gilt diese Konvergenz auch für die Dimensionen. \square

24. VORLESUNG

24.1. Tangenten bei Parametrisierungen.

Satz 24.1. *Es sei K ein unendlicher Körper und $\varphi : \mathbb{A}_K^1 \rightarrow \mathbb{A}_K^n$ eine durch n Polynome $\varphi = (\varphi_1(t), \dots, \varphi_n(t))$ in einer Variablen gegebene Abbildung, deren Bild in der Kurve $C = V(F_1, \dots, F_m)$ liege. Es sei $P = \varphi(Q) \in C$. Dann liegt der Vektor $(\frac{\partial \varphi_1}{\partial t}(Q), \dots, \frac{\partial \varphi_n}{\partial t}(Q))$ im Kern der durch die Jacobi-Matrix*

$$\left(\frac{\partial F_i}{\partial X_j}(P) \right)_{ij}$$

definierten linearen Tangentialabbildung $(TF)_P : \mathbb{A}_K^n \rightarrow \mathbb{A}_K^m$. Ist $n = 2$ und verschwinden nicht beide Ableitungen von φ und ist P ein glatter Punkt von C , so definiert der Vektor $(\frac{\partial \varphi_1}{\partial t}(Q), \frac{\partial \varphi_2}{\partial t}(Q))$ die Richtung der Tangente von C in P .

Beweis. Wegen $\varphi(\mathbb{A}_K^1) \subseteq V(F_1, \dots, F_m)$ ist die Hintereinanderschaltung $F \circ \varphi$ die konstante Abbildung auf den Nullpunkt. Über einem unendlichen Körper sind dann auch die beschreibenden Komponentenpolynome null. Daher ist auch

$$0 = (T(F \circ \varphi))_Q = (TF)_P \circ (T\varphi)_Q = 0,$$

und das ist die Behauptung. Daraus folgt auch der Zusatz, da unter den angegebenen Bedingungen der Kern der Jacobi-Matrix und das Bild der Tangentialabbildung eindimensional sind, also wegen der Inklusion übereinstimmen müssen. \square

Beispiel 24.2. Wir knüpfen an Beispiel 6.3 an, d.h. wir betrachten die Kurve $V(y^2 - x^2 - x^3)$ mit der Parametrisierung

$$(\varphi(t), \psi(t)) = (t^2 - 1, t(t^2 - 1)) = (x, y).$$

Die partiellen Ableitungen von F sind

$$\frac{\partial F}{\partial x} = -2x - 3x^2 \quad \text{und} \quad \frac{\partial F}{\partial y} = 2y.$$

Die Jacobimatrix der Parametrisierung ist

$$\left(\frac{\partial \varphi}{\partial t}, \frac{\partial \psi}{\partial t} \right) = (2t, 3t^2 - 1).$$

Damit ist in der Tat (mit $P = (\varphi(t), \psi(t))$)

$$\begin{aligned}
 & \left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P) \right) \begin{pmatrix} 2t \\ 3t^2 - 1 \end{pmatrix} \\
 &= (-2(t^2 - 1) - 3(t^2 - 1)^2, 2(t^3 - t)) \begin{pmatrix} 2t \\ 3t^2 - 1 \end{pmatrix} \\
 &= -4t(t^2 - 1) - 6t(t^2 - 1)^2 + 2(t^3 - t)(3t^2 - 1) \\
 &= -4t^3 + 4t - 6t^5 + 12t^3 - 6t + 6t^5 - 2t^3 - 6t^3 + 2t \\
 &= 0.
 \end{aligned}$$

Für $t = 2$ ergibt sich beispielsweise der Bildpunkt $P = (3, 6)$. Für diesen Wert hat der Tangentialvektor die Richtung $(4, 11)$. Die partiellen Ableitungen an P ergeben den Gradienten $(-33, 12)$, der senkrecht zum Tangentialvektor steht. Die Tangente selbst wird durch

$$\{(3, 6) + s(4, 11), s \in K\} \text{ oder als } V(-11x + 4y + 9)$$

beschrieben.

24.2. Tangenten bei Raumkurven.

Wir beschränken uns zwar hauptsächlich auf den Fall von ebenen Kurven, dennoch kann man auch für Kurven in einer höherdimensionalen Umgebung und überhaupt für beliebige Varietäten mit der Hilfe von Ableitungen die Begriffe glatt und singular definieren. Wir demonstrieren dies kurz für Raumkurven, die durch zwei Polynome $F, G \in K[X, Y, Z]$ in drei Variablen ohne gemeinsame Komponenten gegeben seien (nicht jede Raumkurve lässt sich so beschreiben!). In diesem Fall betrachtet man zu einem Punkt $P \in C = V(F, G)$ wieder die *Jacobi-Matrix*

$$\begin{pmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} & \frac{\partial F}{\partial z} \\ \frac{\partial G}{\partial x} & \frac{\partial G}{\partial y} & \frac{\partial G}{\partial z} \end{pmatrix}_P : \mathbb{A}_K^3 \longrightarrow \mathbb{A}_K^2.$$

Dann ist P ein glatter Punkt der Kurve genau dann, wenn diese Matrix den Rang zwei hat. Der eindimensionale Kern definiert dann die *Tangente*.

Beispiel 24.3. Wir knüpfen an an das Beispiel 4.6, also den Schnitt C der beiden Zylinder, die durch

$$F = X^2 + Y^2 - 1 \text{ und } G = Y^2 + Z^2 - 1$$

gegeben sind. Die partiellen Ableitungen sind

$$\partial F = (2X, 2Y, 0) \text{ und } \partial G = (0, 2Y, 2Z).$$

Ein singularer Punkt liegt vor, wenn diese durch die Jacobi-Matrix definierte Abbildung einen Rang ≤ 1 hat, und dies ist genau dann der Fall, wenn die beiden partiellen Ableitungstupel linear abhängig sind (und es ein Punkt der

zugehörigen Varietät ist). Wegen den beiden Nullen kann lineare Abhängigkeit nur bei $x = z = 0$ vorliegen, und dort liegt sie für beliebiges y auch vor. Bei $x = z = 0$ ergibt allerdings nur $y = \pm 1$ ein Punkt der Kurve, und das sind die zwei singulären Punkte von C . Dies sind natürlich genau die beiden Schnittpunkte der beiden Kreise, die nach Beispiel 4.6 die irreduziblen Komponenten von C sind. Wenn die Radien der beiden Zylinder nicht gleich groß sind, sagen wir $r_1 \neq r_2$, so funktioniert die Bestimmung der singulären Punkte zunächst genau gleich, und man gelangt zur Bedingung $y^2 = r_1$ und $y^2 = r_2$, die nicht beide zugleich erfüllt sein können. Bei unterschiedlichen Radien ist die Schnittkurve also glatt.

24.3. Potenzreihenringe.

Definition 24.4. Sei R ein kommutativer Ring und T_1, \dots, T_n eine Menge von Variablen. Eine *formale Potenzreihe* ist ein Ausdruck der Form

$$F = \sum_{\nu} a_{\nu} T^{\nu} = \sum_{\nu} a_{\nu} T_1^{\nu_1} \cdots T_n^{\nu_n},$$

wobei $a_{\nu} \in R$ ist für alle $\nu = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n$.

Man addiert zwei Potenzreihen komponentenweise und multipliziert sie in der gleichen Weise wie Polynome. In einer Variablen hat man

$$F \cdot G = \left(\sum_{i=0}^{\infty} a_i T^i \right) \left(\sum_{j=0}^{\infty} b_j T^j \right) = \sum_{k=0}^{\infty} c_k T^k \quad \text{mit} \quad c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Definition 24.5. Sei R ein kommutativer Ring. Dann bezeichnet man mit

$$R[[X_1, \dots, X_n]]$$

den *Potenzreihenring in n Variablen* (oder den *Ring der formalen Potenzreihen in n Variablen*).

Wir interessieren uns hauptsächlich für den Potenzreihenring $K[[T]]$ in einer Variablen über einem Körper K . Mit Hilfe von Potenzreihenringen kann man „formale Parametrisierungen“ für beliebige algebraische Kurven in jedem Punkt finden, was wir in der nächsten Vorlesung behandeln werden. Zunächst müssen wir einige grundlegende Eigenschaften der Potenzreihenringe verstehen.

Satz 24.6. Sei K ein Körper und sei $K[[T]]$ der Ring der formalen Potenzreihen. Dann ist eine formale Potenzreihe $F = \sum_{n=0}^{\infty} a_n T^n$ genau dann eine Einheit, wenn der konstante Term $a_0 \neq 0$ ist.

Beweis. Die angegebene Bedingung ist notwendig, da die Abbildung $K[[T]] \rightarrow K, T \mapsto 0$, die eine Potenzreihe auf den konstanten Term schickt, ein Ringhomomorphismus ist. Für die Umkehrung müssen wir eine Potenzreihe $G = \sum_{j=0}^{\infty} b_j T^j$ angeben mit

$$FG = \left(\sum_{i=0}^{\infty} a_i T^i \right) \left(\sum_{j=0}^{\infty} b_j T^j \right) = 1.$$

Für b_0 ergibt sich daraus die Bedingung $a_0 b_0 = 1$, die wegen $a_0 \neq 0$ eine eindeutige Lösung besitzt, nämlich $b_0 = a_0^{-1}$. Nehmen wir induktiv an, dass die Koeffizienten b_j für $j < n$ schon konstruiert seien derart, dass sämtliche Koeffizienten c_k , $1 \leq k < n$, der Produktreihe FG gleich null sind. Für den n -ten Koeffizienten ergibt sich die Bedingung

$$c_n = 0 = a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0.$$

Dabei sind bis auf b_n alle Werte festgelegt, und wegen $a_0 \neq 0$ ergibt sich eine eindeutige Lösung für b_n . \square

Korollar 24.7. *Sei K ein Körper und $R = K[[T]]$ der Potenzreihenring in einer Variablen. Dann ist R ein diskreter Bewertungsring.*

Beweis. Zunächst ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = (T)$. Wenn nämlich eine Potenzreihe F keine Einheit ist, so muss nach Satz 24.6 der konstante Term von F null sein. Dann kann man aber schreiben $F = T\tilde{F}$ mit der umindizierten Potenzreihe \tilde{F} . Die Nullteilerfreiheit folgt durch Betrachten der Anfangsterme: sind F und G von null verschiedene Potenzreihen, so ist

$$F = a_k T^k + a_{k+1} T^{k+1} + \dots \quad \text{und} \quad G = b_\ell T^\ell + a_{\ell+1} T^{\ell+1} + \dots \quad \text{mit} \quad a_k, b_\ell \neq 0.$$

Für die Produktreihe ist dann der Koeffizient $c_{k+\ell} = a_k b_\ell \neq 0$, da die kleineren Koeffizienten alle null sind. Es bleibt also noch noethersch zu zeigen. Es ergibt sich aber direkt, dass ein Hauptidealbereich vorliegt, und zwar wird jedes Ideal $\neq 0$ von T^j erzeugt, wobei j das Minimum über alle Indizes von Koeffizienten $\neq 0$ von Potenzreihen in dem Ideal ist. \square

Man kann Potenzreihen nicht nur addieren und multiplizieren, sondern auch, unter gewissen Zusatzbedingungen, Potenzreihen in andere Potenzreihen einsetzen. Diese Operation entspricht der Hintereinanderschaltung von Abbildungen.

Definition 24.8. Es sei K ein Körper und $F = \sum_{i=0}^{\infty} a_i T^i \in K[[T]]$ eine Potenzreihe. Es sei $G = \sum_{j=0}^{\infty} b_j T^j$ eine weitere Potenzreihe mit konstantem Term null. Dann nennt man die Potenzreihe

$$\begin{aligned} F(G) &= a_0 + a_1 \left(\sum_{j=0}^{\infty} b_j T^j \right) + a_2 \left(\sum_{j=0}^{\infty} b_j T^j \right)^2 + a_3 \left(\sum_{j=0}^{\infty} b_j T^j \right)^3 + \dots \\ &= \sum_{k=0}^{\infty} c_k T^k \end{aligned}$$

die *eingesetzte Potenzreihe*. Ihre Koeffizienten sind folgendermaßen festgelegt.

$$c_k = \sum_{s=0}^k \left(\sum_{j_1 + \dots + j_s = k} a_s b_{j_1} \cdots b_{j_s} \right).$$

Hierbei wird summiert über alle geordneten s -Tupel $(j_1, \dots, j_s) \in \mathbb{N}_+^s$.

Man beachte in der vorstehenden Definition, dass wegen $b_0 = 0$ nur über $j \geq 1$ summiert wird, so dass alle beteiligten Summen endlich sind. Die

Formeln für das Einsetzen sind derart, dass sie bei Polynomen das übliche Einsetzen von Polynomen in Polynome ergeben. Einsetzen von Potenzreihen in Potenzreihen liefert wieder einen Einsetzungshomomorphismus der Potenzreihenringe.

Lemma 24.9. *Sei K ein Körper mit dem Potenzreihenring $K[[T]]$. Es sei $G \in K[[S]]$ eine Potenzreihe mit konstantem Term null. Dann definiert G durch Einsetzen einen K -Algebra-Homomorphismus*

$$K[[T]] \longrightarrow K[[S]], F \longmapsto F(G).$$

Beweis. Die Abbildung ist wohldefiniert. Um zu zeigen, dass ein Ringhomomorphismus vorliegt, muss man lediglich gewisse Koeffizienten vergleichen. Diese hängen immer nur von endlich vielen Koeffizienten der beteiligten Potenzreihen an, so dass sich diese Aussage aus dem polynomialen Fall ergibt. \square

Lemma 24.10. *Sei K ein Körper, $K[[T]]$ der Potenzreihenring über K und $G = \sum_{j=0}^{\infty} b_j T^j$ mit $b_0 = 0$ und $b_1 \neq 0$. Dann definiert der durch $T \mapsto G$ definierte Einsetzungshomomorphismus einen K -Algebra-Automorphismus auf $K[[T]]$.*

Beweis. Wir zeigen zunächst, dass es eine Potenzreihe $F = \sum_{i=0}^{\infty} a_i T^i$ gibt mit $F(G) = T$. Dabei muss $a_0 = 0$ und $a_1 = b_1^{-1}$ sein. Sei nun die Potenzreihe F mit der gewünschten Eigenschaft bis zum $(k-1)$ -Koeffizienten bereits konstruiert. Für den Koeffizienten c_k hat man nach Definition 24.8 die Bedingung

$$0 = c_k = \sum_{s=0}^k \left(\sum_{j_1+\dots+j_s=k} a_s b_{j_1} \cdots b_{j_s} \right) = \sum_{s=0}^{k-1} \left(\sum_{j_1+\dots+j_s=k} a_s b_{j_1} \cdots b_{j_s} \right) + a_k b_1^k.$$

Daraus ergibt sich eine eindeutig lösbare Bedingung an a_k .

Wir betrachten nun die Hintereinanderschaltung

$$K[[T]] \xrightarrow{T \mapsto F} K[[T]] \xrightarrow{T \mapsto G} K[[T]].$$

Dabei ist die Gesamtabbildung der Einsetzungshomomorphismus $T \mapsto T$, und das ist die Identität. Insbesondere ist die hintere Abbildung surjektiv. Da $K[[T]]$ nach Korollar 24.7 ein diskreter Bewertungsring, sind die Ideale darin bekannt, und nur das Nullideal kommt als Kern der Abbildung in Frage. Die Abbildung ist also auch injektiv und damit bijektiv. \square

25. VORLESUNG

25.1. Lösung in Potenzreihen für algebraische Kurven.

Sei $F \neq 0$ ein Polynom, das die ebene algebraische Kurve C beschreibe, und sei $P = (0, 0) \in C$ vorausgesetzt (was keine Einschränkung ist, und durch Verschiebung immer erreicht werden kann). Wie kann man die Kurve im

Nullpunkt mittels Potenzreihen beschreiben, wann gibt es also einen durch nichtkonstante Potenzreihen G und H mit konstantem Term 0 definierten Ringhomomorphismen

$$K[X, Y] \longrightarrow K[[T]] \text{ mit } X \longmapsto G \text{ und } Y \longmapsto H$$

mit $F(G, H) = 0$ (also einen Ringhomomorphismus $K[X, Y]/(F) \rightarrow K[[T]]$). Es geht also um Lösungen der Gleichung

$$F(X, Y) = 0$$

in Potenzreihen, die das Verhalten der Kurve um die Punktlösung 0 herum genauer beschreiben.

Der grundsätzliche Ansatz ist hier ein *Potenzreihenansatz*, wie er bspw. auch in der Theorie der Differentialgleichungen verwendet wird. Man setzt

$$G = \sum_{k=0}^{\infty} a_k T^k \text{ und } H = \sum_{\ell=0}^{\infty} b_\ell T^\ell$$

mit zunächst unbestimmten Koeffizienten a_k und b_ℓ an. Das direkte Einsetzen in die beschreibende Gleichung $F = 0$ und Ausmultiplizieren ergibt dann einen prinzipiell unendlichen Ausdruck. Allerdings ist für jedes T^k der zugehörige Ausdruck für den Koeffizienten nur durch endlich viele Daten bestimmt, und zwar sind dafür nur die Koeffizienten von F, G und H unterhalb des Grades k relevant. Da $F(G, H) = 0$ sein soll, müssen die Koeffizienten von F, G, H so sein, dass sich als Koeffizient zu T^k stets null ergibt.

Man sucht dann nach Bedingungen, wann es dafür Lösungen gibt, wie sie aussehen und ob sie eindeutig sind. Die Bedingung $a_0 = b_0 = 0$ ist dabei eine *Anfangsbedingung*, die wiedergibt, dass die Potenzreihenlösung durch den Nullpunkt gehen soll.

Es ergibt sich schnell eine Bedingung an die linearen Terme der Potenzreihen (also an a_1 und b_1), die man als eine weitere Rechtfertigung dafür ansehen kann, dass wir die Linearfaktoren des ersten homogenen Bestandteiles F_m in der homogenen Zerlegung von F als Tangentengleichungen interpretiert haben.

Lemma 25.1. *Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X, Y]$ ein Polynom mit homogener Zerlegung $F = F_d + \dots + F_m$ mit $d \geq m \geq 1$ und $F_m \neq 0$. Es sei*

$$F_m = \prod_{\lambda=1}^m (u_\lambda X + v_\lambda Y)$$

die Faktorzerlegung in Linearfaktoren (diese Linearfaktoren definieren also die Tangenten von $C = V(F)$ an $P = (0, 0)$). Es seien

$$G = \sum_{n=0}^{\infty} a_n T^n \text{ und } H = \sum_{\ell=0}^{\infty} b_\ell T^\ell \in K[[T]]$$

Potenzreihen, die eine Lösung der Kurvengleichung $F = 0$ durch den Nullpunkt beschreiben (d.h. $a_0 = b_0 = 0$.) Dann ist $u_\lambda a_1 + v_\lambda b_1 = 0$ für ein λ , d.h. der lineare Term der Potenzreihen ist durch eine der Tangenten vorgegeben.

Beweis. Wir setzen

$$G = a_1 T + a_2 T^2 + \dots \text{ und } H = b_1 T + b_2 T^2 + \dots$$

in F ein. In einem homogenen Bestandteil F_k , der ja eine Summe von Ausdrücken der Form $c_{ij} X^i Y^j$ mit $i + j = k$ ist, kann man sofort T^k ausklammern, und zwar ergibt sich ein Ausdruck der Form

$$F_k(G, H) = \left(\sum_{i+j=k} c_{ij} a_1^i b_1^j \right) T^k + \left(\sum_{i+j=k} c_{ij} (i a_1^{i-1} a_2 b_1^j + j a_1^i b_1^{j-1} b_2) \right) T^{k+1} + \dots$$

In den Koeffizienten von T^k gehen also a_1, b_1 in einer übersichtlichen Form über F_k ein, aber auch kompliziertere Terme, die von F_ℓ , $\ell < k$, herrühren. Auf F_m angewandt, wo ja keine kleineren homogenen Komponenten mitberücksichtigt werden müssen, heißt dies, dass

$$\sum_{i+j=m} c_{ij} a_1^i b_1^j = 0$$

die entscheidende Gleichung für a_1 und b_1 ist. Dies ist aber nichts anderes als die Bedingung $F_m(a_1, b_1) = 0$. Da F_m ein Produkt von Linearfaktoren ist, muss (a_1, b_1) einen der Linearfaktoren annullieren, was die behauptete Aussage ist. \square

Man beachte, dass im vorstehenden Lemma die Möglichkeit $a_1 = b_1 = 0$ nicht ausgeschlossen ist. In der Tat gibt es nur unter zusätzlichen Bedingungen eine Realisierung einer Kurve mittels Potenzreihen entlang einer vorgegebenen Tangente, siehe Satz 25.2 und die Beispiele weiter unten.

Der Rechenaufwand zur Bestimmung einer Potenzreihenlösung lässt sich wesentlich verringern, wenn man sich auf „Graphlösungen“ beschränkt, wo die eine Potenzreihe einfach ein lineares Polynom ist (und zwar eines, das durch eine Tangente gegeben ist), und die zweite eine zu bestimmende Potenzreihe. Das ist häufig keine wesentliche Einschränkung, wie aus Lemma 24.10 folgt. Mit diesem Lemma können wir nämlich die Potenzreihen $G, H \in K[[T]]$ einfach transformieren, wenn nicht beide lineare Terme verschwinden. Sei hierzu $G = a_1 T + \dots$, $a_1 \neq 0$ angenommen. Mit einer geeigneten Potenzreihe $U(T)$ ist $U(G(T)) = T$ und $U(H(T)) = \tilde{H}(T)$. Man schaltet also einen Potenzreihenautomorphismus dahinter, damit die Hintereinanderschaltung

$$K[X, Y] \xrightarrow{X \mapsto G, Y \mapsto H} K[[T]] \xrightarrow{T \mapsto U(T)} K[[T]]$$

die besonders einfache Gestalt $X \mapsto T$, $Y \mapsto \tilde{H}$ bekommt. Dies bedeutet, dass man die Kurve als Graph zu einer formalen Funktion in einer Variablen realisieren möchte.

Satz 25.2. Sei K ein Körper und sei $F \in K[X, Y]$ ein Polynom $\neq 0$ mit $(0, 0) \in C = V(F)$ und sei $F = F_d + \dots + F_m$ die homogene Zerlegung von F mit $d \geq m$ und mit $F_m \neq 0$. Es sei $uX + vY$ ein einfacher Linearfaktor von F_m (also ein lineares Polynom, das eine Tangente definiert). Dann gibt es Potenzreihen

$$G = \sum_{n=0}^{\infty} a_n T^n, H = \sum_{\ell=0}^{\infty} b_\ell T^\ell \in KT$$

mit $F(G, H) = 0$ und mit konstantem Term $a_0, b_0 = 0$ und mit $a_1 u + b_1 v = 0$. Dabei kann eine der Potenzreihen als ein lineares Polynom gewählt werden.

Beweis. Durch eine lineare Variablentransformation können wir annehmen, dass $uX + vY = Y$ ist. Wir zeigen, dass es dann eine Potenzreihenlösung mit $G = T$ und mit (zu konstruierendem) $H = b_2 T^2 + b_3 T^3 + \dots$ gibt. Wegen $a_1 = 1$ und $b_1 = 0$ erfüllt das die angegebene lineare (Tangenten-)Bedingung.

Sei $F = \sum_{i,j} c_{ij} X^i Y^j$. Es ist $c_{m,0} = 0$, da andernfalls Y kein Linearfaktor von F_m sein könnte, und es ist $c_{m-1,1} \neq 0$, da sonst Y ein Linearfaktor mit einer Multiplizität ≥ 2 wäre.

Wir zeigen, dass es bei diesen Anfangsdaten eine eindeutig bestimmte Potenzreihe $H = b_2 T^2 + b_3 T^3 + \dots$ gibt. Einsetzen von G und H in F ergibt für jedes k eine Bedingung, da der resultierende Koeffizient zu T^k gleich null sein muss. Der k -te Koeffizient ist eine Summe von Ausdrücken der Form

$$c_{ij} b_{\ell_1} \cdots b_{\ell_j} \text{ mit } i + \sum_{\rho=1}^j \ell_\rho = k.$$

(Diese Ausdrücke kommen mehrfach vor, bzw. mit einem Multinomialkoeffizient.) Da $\ell_\rho \geq 2$ ist, kommt für $k < m + \ell - 1$ der Term b_ℓ nicht vor. Der Term b_ℓ kommt erstmalig im $k = (m + \ell - 1)$ -ten Koeffizienten vor, und zwar in der einzigen Weise

$$c_{m-1,1} b_\ell.$$

Ansonsten kommen in diesem Koeffizienten nur die c_{ij} und b_r mit $r < \ell$ vor. Da nach Voraussetzung $c_{m-1,1} \neq 0$ ist, ist dadurch der Wert von b_ℓ eindeutig festgelegt. Die Koeffizienten b_ℓ werden also induktiv konstruiert, wobei die Werte jeweils eindeutig durch die Bedingung an die Koeffizienten festgelegt sind. \square

Beispiel 25.3. Wir betrachten die ebene affine Kurve vom Grad drei, die durch die Gleichung $F = X^3 + XY + Y = 0$ gegeben ist. Die partiellen Ableitungen sind

$$\frac{\partial F}{\partial X} = 3X^2 + Y \text{ und } \frac{\partial F}{\partial Y} = X + 1.$$

Die zweite Ableitung ist nur bei $X = -1$ null, dort hat aber F den Wert -1 , d.h. die Kurve ist glatt. Im Nullpunkt haben die partiellen Ableitungen den Wert $(0, 1)$. Die zugehörige Tangente ist also die X -Achse, was dazu passt, dass der lineare Term der Kurvengleichung Y ist.

Wir berechnen die Potenzreihe $Y = H(T) = \sum_{\ell=0}^{\infty} b_{\ell} T^{\ell}$, die die Kurve im Nullpunkt als Graph beschreibt (es ist $X = T$). Die Anfangsbedingungen sind $b_0 = b_1 = 0$. Für die folgenden Koeffizienten von H müssen wir aus der Gleichung $F(T, H) = T^3 + TH + H = 0$, also

$$T^3 + T(b_2 T^2 + b_3 T^3 + \dots) + (b_2 T^2 + b_3 T^3 + \dots) = 0$$

über die Koeffizienten der T^k die Bedingungen an b_{ℓ} herauslesen.

b_2 . Der zweite Koeffizient liefert sofort $b_2 = 0$.

b_3 . Der dritte Koeffizient liefert die Bedingung $1 + b_3 = 0$, woraus $b_3 = -1$ folgt.

Die folgenden Koeffizienten liefern die Bedingung $b_{\ell-1} + b_{\ell} = 0$, so dass also die folgenden b_{ℓ} abwechselnd 1 und -1 sind. Man hat also eine einfache Rekursionsformel und es ist

$$H = -T^3 + T^4 - T^5 + T^6 - T^7 + \dots$$

Die Umformung der Kurvengleichung in

$$Y = \frac{-X^3}{1+X}$$

zeigt, dass hier der Graph einer rationalen Funktion (mit einem Pol bei $X = -1$) vorliegt. Die angegebene Potenzreihe beschreibt also den Graph einer rationalen Funktion als Graph einer formal-analytischen Funktion.

Beispiel 25.4. (Potenzreihe für Kartesisches Blatt) Wir betrachten das Kartesische Blatt, das durch $X^3 + Y^3 - 3XY = 0$ gegeben ist, im Nullpunkt und bzgl. der durch $Y = 0$ gegebenen Tangente und wollen die Potenzreihe bestimmen, mit der sich der „Zweig“ der Kurve, der diese Tangente definiert, als Graph beschreiben lässt. Wir setzen also $X = T$ und $H = b_2 T^2 + b_3 T^3 + b_4 T^4 + \dots$ an und haben diese Koeffizienten zu bestimmen (die Charakteristik von K sei nicht 3). Die Koeffizienten b_{ℓ} sind durch die Bedingung

$$0 = T^3 + H^3 - 3TH = T^3 + (b_2 T^2 + b_3 T^3 + \dots)^3 - 3T(b_2 T^2 + b_3 T^3 + \dots)$$

festgelegt. Das Einsetzen bzw. Ausmultiplizieren dieser Potenzreihe liefert zum ersten Mal für $k = 3$ eine Bedingung. Der Summand X^3 (bzw. T^3) muss überhaupt nur einmal berücksichtigt werden, nämlich für $k = 3$. Der Summand Y^3 muss erst ab $k \geq 6$ berücksichtigt werden, da ja $Y = H$ ein Vielfaches von T^2 ist. Der Summand XY muss ab $k = 3$ berücksichtigt werden.

b_2 . Hier hat man die Bedingung

$$1 - 3b_2 = 0,$$

woraus sich $b_2 = \frac{1}{3}$ ergibt.

b_3 . Dies taucht erstmals in der Bedingung für den vierten Koeffizienten auf. Dort steht es aber isoliert, so dass $b_3 = 0$ sein muss.

b_4 . Aus dem gleichen Grund ist $b_4 = 0$.

b_5 . Hierfür ist der sechste Koeffizient entscheidend, und dabei ist jetzt auch Y^3 zu berücksichtigen. Es ergibt sich die Bedingung

$$b_2^3 - 3b_5 = 0,$$

also $b_5 = \frac{1}{81}$.

b_6, b_7, b_8 . Der Summand

$$Y^3 = (b_2T^2 + b_5T^5 + \dots)(b_2T^2 + b_5T^5 + \dots)(b_2T^2 + b_5T^5 + \dots)$$

leistet erstmalig wieder für den neunten Koeffizienten einen Beitrag, und zwar ist dieser $3b_2^2b_5$. Dies bedeutet, dass b_6 und b_7 isoliert stehen und daher null sein müssen. Für b_8 ergibt sich die Bedingung

$$3b_2^2b_5 - 3b_8 = 0$$

und daher ist $b_8 = \frac{1}{729}$.

Die Anfangsglieder der Potenzreihe H , die den einen Kurvenzweig im Nullpunkt als Graph beschreibt, ist also

$$H = \frac{1}{3}T^2 + \frac{1}{81}T^5 + \frac{1}{729}T^8 + \dots$$

Beispiel 25.5. Wir betrachten die durch $X^3 - Y^2 = 0$ definierte Neilsche Parabel. Hier ist der Nullpunkt singular, und es gibt nur eine Tangente, nämlich $Y = 0$, diese hat aber die Multiplizität zwei, d.h. Satz 25.2 ist hier nicht anwendbar. Wir werden zeigen, dass es überhaupt keine Potenzreihenlösung im Nullpunkt mit nicht verschwindendem linearen Term gibt.

Seien dazu $X = G = a_1T + a_2T^2 + \dots$ und $Y = H = b_1T + b_2T^2 + \dots$ Potenzreihen, die die Kurvengleichung erfüllen. Wir setzen in die Kurvengleichung ein und erhalten für den zweiten Koeffizienten die Bedingung $-b_1^2 = 0$, woraus $b_1 = 0$ folgt. Für den dritten Koeffizienten ergibt sich hingegen $a_1^3 = 0$, also wieder $a_1 = 0$. Dennoch gibt es Potenzreihenlösungen für die Neilsche Parabel durch den Nullpunkt. Hierzu kann man einfach die monomiale Lösung $G = T^2$ und $H = T^3$ nehmen (die ja sogar eine Bijektion zwischen der affinen Geraden und der Neilschen Parabel stiftet). Der lineare Term davon ist freilich null.

Bemerkung 25.6. (Der Satz über implizite Funktionen) Sei $K = \mathbb{R}$ oder \mathbb{C} und $F \in K[X, Y]$. Bei $(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P)) \neq (0, 0)$, wenn also P ein regulärer Punkt der Funktion F ist (oder, äquivalent, ein glatter Punkt von $C = V(F - F(P))$), so sichert der *Satz über implizite Funktionen*, dass sich die Kurve in einer (metrischen) Umgebung des Punktes als Graph einer differenzierbaren Funktion darstellen lässt.

26. VORLESUNG

26.1. Die Schnittmultiplizität.

Es seien zwei ebene algebraische Kurven $C, D \subset \mathbb{A}_K^2$ gegeben, die keine Komponente gemeinsam haben. Dann besteht der Durchschnitt $C \cap D$ nach Satz 4.8 nur aus endlich vielen Punkten. Wir wollen das Schnittverhalten der beiden Kurven in einem Punkt $P \in C \cap D$ quantitativ erfassen. Dabei empfiehlt es sich, eine etwas allgemeinere Situation zu betrachten, und zwar schreiben wir $C = V(F)$ und $D = V(G)$ und berücksichtigen, dass in F und in G Primfaktoren (jeweils) mehrfach vorkommen können. D.h. wir unterscheiden von nun an zwischen den Kurven $V(F)$ und $V(F^n)$, obwohl es sich geometrisch um das gleiche Objekt handelt.

Lemma 26.1. *Sei K ein Körper und seien $F, G \in K[X, Y]$ Polynome ohne gemeinsamen Primteiler. Es sei $P \in V(F, G)$ und $R = K[X, Y]_{\mathfrak{m}_P}$ die zugehörige Lokalisierung. Dann besitzt der Restklassenring $R/(F, G)$ eine endliche K -Dimension.*

Beweis. Sei \mathfrak{m} das maximale Ideal in R . Da F und G keinen gemeinsamen Teiler haben, gibt es in R zwischen (F, G) und \mathfrak{m} kein weiteres Primideal. Daher ist in $R/(F, G)$ jede Nichteinheit nilpotent. Daher gilt in R die Beziehung $\mathfrak{m}^s \subseteq (F, G) \subseteq \mathfrak{m}$ für ein s . Es liegt daher eine Surjektion $R/\mathfrak{m}^s \rightarrow R/(F, G)$ vor. Nach Lemma 23.3 besitzt der Restklassenring links eine endliche K -Dimension, so dass dies auch für den Restklassenring rechts gilt. \square

Aufgrund von diesem Lemma ist die folgende Definition sinnvoll.

Definition 26.2. Sei K ein Körper und seien $F, G \in K[X, Y]$ zwei nicht-konstante Polynome ohne gemeinsame Komponente und sei

$$P \in V(F) \cap V(G) = V(F, G).$$

Dann nennt man die Dimension

$$\dim_K(K[X, Y]_P/(F, G))$$

die *Schnittmultiplizität* der beiden Kurven $V(F)$ und $V(G)$ im Punkt P . Sie wird mit

$$\text{mult}_P(F, G) \text{ oder mit } \text{mult}_P(V(F), V(G))$$

bezeichnet.

Beispiel 26.3. Sei $C = V(F)$ und eine Gerade $G = V(cX + dY)$ in der affinen Ebene \mathbb{A}_K^2 gegeben, die keine Komponente von C sei. Es sei $P = (a, b) \in C \cap G$ ein Punkt des Durchschnitts. Den Restklassenring

$$K[X, Y]_P/(F, cX + dY)$$

berechnet man, indem man mittels des linearen Terms nach einer der Variablen X oder Y auflöst. Damit kann man eine Variable eliminieren und

der Restklassenring ist isomorph zu $K[X]_P/(\tilde{F})$, wobei man \tilde{F} erhält, indem man in F die Variable Y durch $-\frac{c}{d}X$ ersetzt. Dies kann man auch so sehen, dass man zuerst $K[X]/(\tilde{F})$ berechnet und dann an dem Punkt lokalisiert. Das Polynom \tilde{F} hat in $K[X]$ eine Faktorisierung in Linearfaktoren

$$\tilde{F} = (X - \lambda_1)^{\nu_1} \cdots (X - \lambda_k)^{\nu_k}.$$

Da der Punkt P eine Nullstelle ist, muss $a = \lambda_i$ sein für ein i . Bei der Lokalisierung werden die anderen Linearfaktoren zu Einheiten gemacht und „übrig“ bleibt

$$K[X]/(X - \lambda_i)^{\nu_i}.$$

Dieser Ring hat die Dimension ν_i .

Lemma 26.4. *Sei K ein algebraisch abgeschlossener Körper, sei $F = F_d + \dots + F_m \in K[X, Y]$, $d \geq m$, ein Polynom in homogener Zerlegung und $L = V(aX + bY)$ eine Gerade durch den Nullpunkt P , die keine Komponente von $V(F)$ sei. Dann ist $\text{mult}_P(L, V(F)) \geq m_P(F) = m$, d.h. die Schnittmultiplizität einer Kurve mit einer Geraden ist mindestens so groß wie die Multiplizität der Kurve im Schnittpunkt. Wenn L keine Tangente der Kurve ist, so gilt hierbei Gleichheit.*

Beweis. Wir setzen $R = K[X, Y]_{(X, Y)}$ und $H = aX + bY$, und wir nehmen $b \neq 0$ an, so dass wir $Y = cX$ schreiben können. Es sei zunächst die Gerade L keine Tangente von $V(F)$ in P , also keine Komponente von $V(F_m)$. Es ist dann

$$R/(F, H) = K[X]_{(X)}/(F_d(X, cX) + \dots + F_m(X, cX)).$$

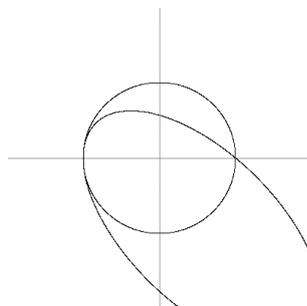
Hierbei ist $F_m(X, cX) \neq 0$ und es wird $X^m u$ mit einer Einheit u rausdividiert, so dass der Restklassenring die Dimension m besitzt. Im allgemeinen Fall gibt es ein minimales i , $m \leq i \leq d$, mit $F_i(X, cX) \neq 0$ (sonst wäre L eine Komponente von $V(F)$). Dann ist mit dem gleichen Argument die Dimension des Restklassenringes $= i \geq m$. \square

Proposition 26.5. *Sei K ein algebraisch abgeschlossener Körper und seien $F, G \in K[X, Y]$ Polynome ohne gemeinsame Komponente und sei $P \in \mathbb{A}_K^2$ ein Punkt. Dann gelten folgende Aussagen.*

- (1) *Es ist $\text{mult}_P(F, G) = 0$ genau dann, wenn $P \notin V(F, G)$ ist.*
- (2) *Es ist $\text{mult}_P(F, G) = \text{mult}_P(G, F)$.*
- (3) *Die Schnittmultiplizität ändert sich nicht bei einer affinen Variablentransformation.*
- (4) *Wenn $F = F_1 F_2$ ist mit $F_2(P) \neq 0$, so ist $\text{mult}_P(F, G) = \text{mult}_P(F_1, G)$.*
- (5) *Es ist $\text{mult}_P(F, G) = \text{mult}_P(F, G + HF)$ für jedes $H \in K[X, Y]$.*

Beweis. Das ist trivial. \square

Teil (4) der letzten Aussage kann man auch so formulieren, dass die Schnittmultiplizität nur von den Komponenten von F und G abhängen, die durch P gehen.



Ein transversaler und ein nichttransversaler Schnitt

Definition 26.6. Es seien $F, G \in K[X, Y]$ und $P \in V(F, G)$. Dann sagt man, dass sich $V(F)$ und $V(G)$ im Punkt P *transversal schneiden*, wenn P sowohl auf $V(F)$ als auch auf $V(G)$ ein glatter Punkt ist und wenn die Tangenten der beiden Kurven im Punkt P verschieden sind.

Lemma 26.7. Sei K ein Körper und seien $F, G \in K[X, Y]$ Polynome ohne gemeinsame Komponente. Es sei $P \in V(F, G) \subseteq \mathbb{A}_K^2$ ein Schnittpunkt. Dann schneiden sich $V(F)$ und $V(G)$ in P transversal genau dann, wenn die Schnittmultiplizität $\text{mult}_P(V(F), V(G)) = 1$ ist.

Beweis. Es sei $R = K[X, Y]_{\mathfrak{m}}$ der lokale Ring zum (Null-)Punkt P in der Ebene. Sei zunächst der Schnitt als transversal vorausgesetzt. Dann sind insbesondere beide Kurven in P glatt, und $B = R/(F)$ ist ein diskreter Bewertungsring nach Lemma 23.2. Da die Tangenten verschieden sind, können wir annehmen, dass die Tangente an $V(F)$ durch $V(Y)$ und die Tangente an $V(G)$ durch $V(X)$ gegeben ist. Nach dem Beweis zu Lemma 23.2 ist dann X eine Ortsuniformisierende von B . Da G die Form hat $G = X + H$ mit $H \in \mathfrak{m}^2$ ist G ebenfalls eine Ortsuniformisierende in B und daher ist $B/(G) = K$. Daher ist die Schnittmultiplizität eins.

Für die Rückrichtung folgt aus Lemma 26.4, dass die Multiplizität der beiden Kurven in P eins sein muss und daher beide Kurven in P glatt sind. Nehmen wir an, dass die Tangenten übereinstimmen. Dann können wir annehmen, dass sowohl F als auch G die Form $Y + \text{Terme von größerem Grad}$ besitzen. Man kann die Idealerzeuger (F, G) durch $(F, F - G)$ ersetzen, und dabei ist $F - G \in \mathfrak{m}^2$. Dann erzeugt aber $F - G$ in $B = R/(F)$ nicht das maximale Ideal, und die Schnittmultiplizität kann nicht eins sein. \square

Satz 26.8. (*Summenformel*) Seien $F, G \in K[X, Y]$ Polynome ohne gemeinsamen Primteiler mit Faktorzerlegungen

$$F = \prod_{i=1}^m F_i^{\nu_i} \quad \text{und} \quad G = \prod_{j=1}^n G_j^{\mu_j}$$

Dann ist

$$\text{mult}_P(F, G) = \sum_{i,j} \nu_i \mu_j \text{mult}_P(F_i, G_j).$$

Beweis. Diese Aussage folgt durch Induktion aus dem Spezialfall $F = F_1 F_2$ (und $G = G$). Sei $R = K[X, Y]_P$. Wegen $(F_1 F_2, G) \subseteq (F_2, G)$ hat man eine surjektive Abbildung $R/(F_1 F_2, G) \rightarrow R/(F_2, G)$. Andererseits induziert die Multiplikation mit F_2 einen R -Modul Homomorphismus $R/(F_1, G) \rightarrow R/(F_1 F_2, G)$. Wir behaupten, dass eine kurze exakte Sequenz

$$0 \longrightarrow R/(F_1, G) \xrightarrow{\cdot F_2} R/(F_1 F_2, G) \longrightarrow R/(F_2, G) \longrightarrow 0$$

vorliegt. Dabei ist die Surjektivität klar und ebenso, dass die hintereinander geschalteten Abbildungen die Nullabbildung sind. Sei $z \in R/(F_1 F_2, G)$ ein Element, das rechts auf null abgebildet wird. Dann kann man in R schreiben: $z = AF_2 + BG$. Dann wird $AF_2 \in R/(F_1 F_2, G)$ ebenfalls auf diese Klasse abgebildet, und dieses kommt von links. Sei nun $w \in R/(F_1, G)$, dass durch Multiplikation mit F_2 auf null abgebildet wird, also $wF_2 = CF_1 F_2 + DG$. Wir schreiben dies als $(w - CF_1)F_2 = DG$. Da F und G keinen gemeinsamen Primteiler besitzen, gilt dies erst recht für F_2 und G . Also muss F_2 ein Teiler von D sein und es ergibt sich eine Beziehung $(w - CF_1) = \tilde{D}G$, woraus folgt, dass bereits $w = 0$ ist.

Aus der Additivitätseigenschaft von kurzen exakten Sequenzen folgt die gewünschte Identität

$$\begin{aligned} \text{mult}_P(F_1 F_2, G) &= \dim_K (R/(F_1 F_2, G)) = \dim_K (R/(F_1 F_2, G)) \\ &= \dim_K (R/(F_1, G)) + \dim_K (R/(F_2, G)). \end{aligned}$$

□

Satz 26.9. *Sei R ein noetherscher kommutativer Ring mit nur endlich vielen Primidealen $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, die alle maximal seien. Dann gibt es eine kanonische Isomorphie*

$$R \cong R_{\mathfrak{m}_1} \times \cdots \times R_{\mathfrak{m}_n}.$$

Beweis. Die maximalen Ideale sind zugleich die minimalen Primideale. Daher besteht der Durchschnitt $\mathfrak{a} = \bigcap_i \mathfrak{m}_i$ aller maximaler Ideale nur aus nilpotenten Elementen. Da der Ring noethersch ist, gibt es dann auch ein s mit $\mathfrak{a}^s = 0$. Zu jedem maximalen Ideal \mathfrak{m}_i betrachten wir die Lokalisierung $R \rightarrow R_{\mathfrak{m}_i}$. Wir behaupten, dass diese Lokalisierung isomorph zum Restklassenring

$$R/\mathfrak{a}_i \text{ mit } \mathfrak{a}_i := \mathfrak{m}_i^s$$

ist. Wegen $\prod \mathfrak{m}_i \subseteq \bigcap \mathfrak{m}_i$ ist $(\prod \mathfrak{m}_i)^s \subseteq (\bigcap \mathfrak{m}_i)^s$ und daher ist auch $\mathfrak{a}_1 \cdots \mathfrak{a}_n = 0$. Sei $i = 1$. Zu jedem $j \neq 1$ gibt es ein $g_j \in \mathfrak{m}_j$ mit $g_j \notin \mathfrak{m}_1$. Daher gilt für jedes Element $f \in \mathfrak{a}_1$ die Beziehung

$$f g_2^s \cdots g_n^s = 0.$$

Wegen $g_2^s \cdots g_n^s \notin \mathfrak{m}_1$ bedeutet dies, dass f unter der Lokalisierungsabbildung auf null geht. Wir erhalten also einen Ringhomomorphismus

$$R/\mathfrak{a}_1 \longrightarrow R_{\mathfrak{m}_1}.$$

Damit ist die Lokalisierung rechts auch eine Lokalisierung des Restklassenringes links. Die maximalen Ideale erzeugen paarweise das Einheitsideal. Dies gilt dann auch für beliebige Potenzen davon. Daraus folgt zunächst, dass das Ideal \mathfrak{a}_1 nur in \mathfrak{m}_1 enthalten ist. Daher ist der Restklassenring links selbst ein lokaler Ring. Also muss die Abbildung ein Isomorphismus sein.

Die gegebene Abbildung kann man also auch schreiben als

$$R \longrightarrow \prod_{i=1}^n R/\mathfrak{a}_i.$$

Hierbei erzeugen die \mathfrak{a}_i paarweise das Einheitsideal, so dass nach einer Form des Chinesischen Restsatzes eine Isomorphie vorliegt. \square

Korollar 26.10. *Sei K ein algebraisch abgeschlossener Körper und seien $F, G \in K[X, Y]$ Polynome ohne gemeinsamen Primteiler. Es seien $P_1, \dots, P_n \in \mathbb{A}_K^2$ die endlich vielen Punkte aus $V(F, G)$ mit den zugehörigen maximalen Idealen $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ in $K[X, Y]$. Dann gibt es eine kanonische Isomorphie*

$$K[X, Y]/(F, G) \cong (K[X, Y]_{\mathfrak{m}_1})/(F, G) \times \cdots \times (K[X, Y]_{\mathfrak{m}_n})/(F, G).$$

Beweis. Da F und G keinen gemeinsamen Primteiler haben, umfasst das Ideal (F, G) nur endlich viele Primideale, die alle maximal sind. Daher erfüllt Der Restklassenring $R/(F, G)$ die Bedingungen aus Satz 26.9. Da der Körper algebraisch abgeschlossen ist, entsprechen die maximalen Ideale eindeutig den Punkten im Schnitt der beiden zugehörigen Kurven $V(F)$ und $V(G)$, so dass sich die Aussage ergibt. \square

Satz 26.11. *Sei K ein algebraisch abgeschlossener Körper und seien $F, G \in K[X, Y]$ Polynome ohne gemeinsamen Primteiler. Dann ist*

$$\dim_K (K[X, Y]/(F, G)) = \sum_P \text{mult}_P(F, G).$$

Beweis. Dies folgt direkt aus der in Korollar 26.10 bewiesenen Isomorphie. \square

Wir erwähnen noch abschließend ohne Beweis folgenden Satz, der eine Abschätzung zwischen der Schnittmultiplizität und den Multiplizitäten der beiden Kurven angibt.

Satz 26.12. *(Multiplizitätsabschätzung) Es seien $F, G \in K[X, Y]$ und $P \in V(F, G)$. Dann gilt die Abschätzung*

$$\text{mult}_P(F, G) \geq m_P(F) \cdot m_P(G).$$

Beweis. Siehe Fulton, Algebraic Curves, Chapter III.3. \square

27. VORLESUNG

27.1. Der projektive Raum.

Definition 27.1. Sei K ein Körper. Der *projektive n -dimensionale Raum* \mathbb{P}_K^n besteht aus allen Geraden des \mathbb{A}_K^{n+1} durch den Nullpunkt, wobei diese Geraden als Punkte aufgefasst werden. Ein solcher Punkt wird repräsentiert durch *homogene Koordinaten* (a_0, a_1, \dots, a_n) , wobei nicht alle $a_i = 0$ sein dürfen, und wobei zwei solche Koordinatentupel genau dann den gleichen Punkt repräsentieren, wenn sie durch Multiplikation mit einem Skalar $\lambda \in K^\times$ ineinander übergehen.



Die Geraden durch einen Punkt

Wir werden den projektiven Raum zunehmend mit mehr Strukturen versehen.

Satz 27.2. Sei K ein Körper und sei \mathbb{P}_K^n ein projektiver Raum. Sei $i \in \{0, 1, \dots, n\}$ fixiert. Dann gibt es eine natürliche Abbildung

$$\varphi_i : \mathbb{A}_K^n \longrightarrow \mathbb{P}_K^n, (u_1, \dots, u_n) \longmapsto (u_1, \dots, u_i, 1, u_{i+1}, \dots, u_n).$$

Diese Abbildung ist injektiv und induziert eine Bijektion zu denjenigen Punkten des projektiven Raumes, bei denen die i -te homogene Koordinate nicht null ist. Die Umkehrabbildung wird gegeben durch

$$\begin{aligned} \mathbb{P}_K^n \supset D_+(X_i) &:= \{(x_0, x_1, \dots, x_n) : x_i \neq 0\} \longrightarrow \mathbb{A}_K^n, \\ (x_0, x_1, \dots, x_n) &\longmapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right). \end{aligned}$$

Der projektive Raum wird überdeckt von diesen $n + 1$ affinen Räumen. Das Komplement eines solchen affinen Raumes $\mathbb{A}_K^n \cong D_+(X_i) \subset \mathbb{P}_K^n$ ist ein $(n - 1)$ -dimensionaler projektiver Raum.

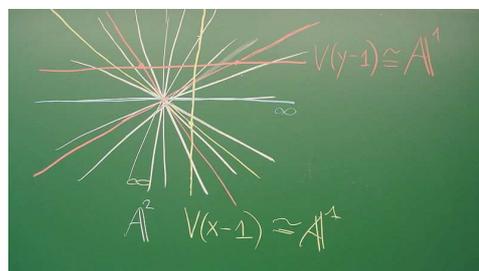
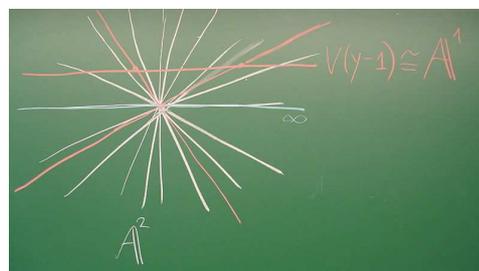
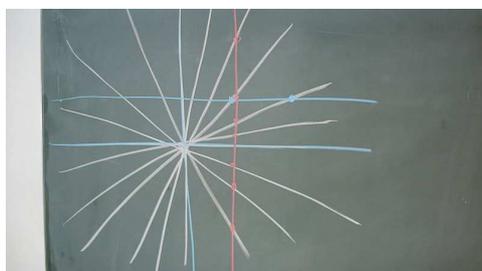
Beweis. Die Abbildung ist offensichtlich wohldefiniert, da die 1 sicher stellt, dass mindestens eine homogene Koordinate nicht null ist. Die Abbildung ist injektiv, da aus einer Gleichung der Form (für homogene Koordinaten)

$$(u_1, \dots, u_i, 1, u_{i+1}, \dots, u_n) = \lambda(v_1, \dots, v_i, 1, v_{i+1}, \dots, v_n)$$

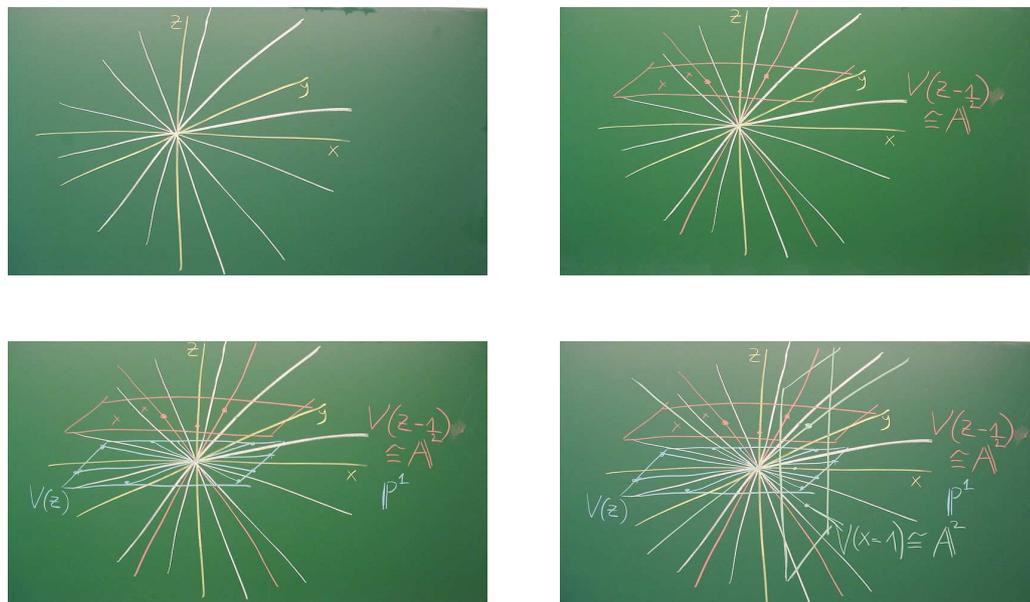
sofort $\lambda = 1$ folgt wegen der 1. Die Umkehrabbildung ist auf der angegebenen Teilmenge wohldefiniert, und ist invers zu der Abbildung. Die Überdeckungseigenschaft ist klar, da für jeden Punkt des projektiven Raumes mindestens eine homogene Koordinate nicht null ist. Das Komplement zu $D_+(X_i)$ ist

$$V_+(X_i) = \{(x_0, x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) : x_j \in K\}$$

mit keinerlei Einschränkung an die übrigen n Variablen und mit der Identifizierung von zwei solchen Tupeln, wenn sie durch Multiplikation mit einem Skalar ineinander übergehen. \square



Beispiel 27.3. (Die projektive Gerade) Die projektive Gerade \mathbb{P}_K^1 ist gegeben als die Menge der Geraden durch den Nullpunkt in der affinen Ebene \mathbb{A}_K^2 . Eine solche Gerade ist entweder die x -Achse oder aber eine Gerade, die die Gerade $V(y-1)$ (also die zur x -Achse parallele Gerade durch $(0, 1)$) in genau einem Punkt schneidet. Umgekehrt liefert jeder Punkt $P \in V(y-1) \cong \mathbb{A}_K^1$ eine eindeutig bestimmte Gerade durch den Nullpunkt. D.h. die projektive Gerade besteht aus einer affinen Gerade und einem weiteren Punkt, den man den „unendlich fernen“ Punkt nennt. Wichtig ist dabei aber, dass dieser unendlich ferne Punkt nicht wesensverschieden von den anderen Punkten ist. Wenn man eine beliebige Gerade G durch den Nullpunkt nimmt sowie eine dazu parallele Gerade $L \neq G$, so übernimmt L die Rolle der affinen Geraden, und G repräsentiert dann einen (von dieser affinen Geraden aus gesehen) unendlich fernen Punkt.



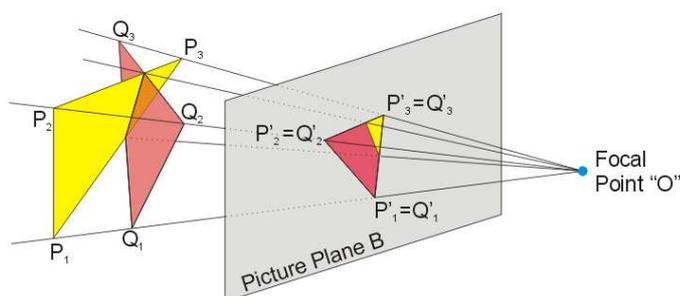
Beispiel 27.4. (Die projektive Ebene) Die Punkte in der projektiven Ebene \mathbb{P}_K^2 entsprechen den Geraden durch den Nullpunkt im affinen Raum \mathbb{A}_K^3 . Jeder Punkt der projektiven Ebene wird repräsentiert durch ein Tupel (x, y, z) , wobei nicht alle x, y, z gleichzeitig null sein dürfen und wobei zwei Koordinatentupel identifiziert werden, wenn sie durch Multiplikation mit einem Skalar $\lambda \neq 0$ ineinander überführt werden können. Die projektive Ebene wird überdeckt durch drei affine Ebenen, nämlich

$$D_+(X), D_+(Y) \text{ und } D_+(Z).$$

Dabei besteht $D_+(Z)$ aus allen Punkte wo die dritte Koordinate nicht null ist. Durch Multiplikation mit z^{-1} kann man diese Punkte identifizieren mit

$$(x/z, y/z, z/z) = (u, v, 1),$$

so dass wirklich eine affine Ebene vorliegt. Das Komplement der affinen Ebene $D_+(Z)$ ist die Menge $V_+(Z)$ der Punkte, wo die dritte Komponente null ist. Da man nach wie vor Punkte identifiziert, die durch Multiplikation mit einem Skalar ineinander überführbar sind, ist $V_+(Z)$ eine projektive Gerade. Ein Punkt $(x, y, 0)$ auf dieser Geraden und der Nullpunkt $(0, 0, 1)$ von $D_+(Z)$ definieren die Gerade durch den Nullpunkt mit dem Richtungsvektor (x, y) (und der homogenen Geradengleichung $yX - xY = 0$ bzw. $V_+(yX - xY)$.) Man kann sich also die projektive Ebene gut vorstellen als eine affine Ebene, in der jede Gerade durch den Nullpunkt noch einen zusätzlichen („unendlich fernen“) Punkt definiert.



27.2. Nullstellen von homogenen Polynomen.

Für ein beliebiges Polynom $F \in K[X_0, \dots, X_n]$ macht es keinen Sinn zu sagen, ob ein Punkt $P \in \mathbb{P}_K^n$ eine Nullstelle davon ist, da diese Eigenschaft nicht invariant unter der Multiplikation mit einem Skalar ist und daher vom Repräsentanten von P abhängt. Für homogene Polynome sieht das anders aus.

Lemma 27.5. *Sei K ein Körper und sei $F \in K[X_0, \dots, X_n]$ ein homogenes Polynom vom Grad d . Dann gilt für einen Punkt (x_0, \dots, x_n) und einen Skalar $\lambda, \lambda \neq 0$, die Beziehung*

$$F(\lambda x_0, \dots, \lambda x_n) = \lambda^d F(x_0, \dots, x_n).$$

Insbesondere verschwindet F an $P \in \mathbb{P}_K^n$ genau dann, wenn F an $\lambda P \in \mathbb{P}_K^n$ verschwindet.

Beweis. Dies kann man auf den Fall eines Monoms vom Grad d zurückführen. Für $X_0^{d_0} \dots X_n^{d_n}$ mit $\sum_{i=0}^n d_i = d$ und $\lambda \in K$ gilt

$$(\lambda X_0)^{d_0} \dots (\lambda X_n)^{d_n} = (\lambda^{d_0} X_0^{d_0}) \dots (\lambda^{d_n} X_n^{d_n}) = \lambda^d (X_0^{d_0} \dots X_n^{d_n}).$$

□

Man beachte, dass es durch diese Aussage zwar wohldefiniert ist, ob ein homogenes Polynom an einem projektiven Punkt verschwindet oder nicht, dass es aber keinen Sinn macht, einem homogenen Polynom einen Wert an jedem Punkt des projektiven Raumes zuzuordnen. Ein homogenes Polynom definiert keine Funktion auf dem projektiven Raum.

Definition 27.6. Sei K ein Körper. Zu einem homogenen Polynom F bezeichnet man die Menge

$$V_+(F) = \{P = (x_0, \dots, x_n) \in \mathbb{P}_K^n : F(x_0, \dots, x_n) = 0\}$$

als die *projektive Nullstellenmenge* zu F .

Definition 27.7. Sei K ein Körper und $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$ ein Ideal. Das Ideal heißt *homogen*, wenn für jedes $H \in \mathfrak{a}$ mit homogener Zerlegung $H = \sum_i H_i$ auch $H_i \in \mathfrak{a}$ ist für alle homogenen Bestandteile H_i .

Definition 27.8. Zu einem homogenen Ideal $\mathfrak{a} \subseteq K[X_0, \dots, X_n]$ nennt man

$$V_+(\mathfrak{a}) = \{P = (x_0, \dots, x_n) \in \mathbb{P}_K^n : F(P) = 0 \text{ für alle homogenen } F \in \mathfrak{a}\}$$

das *projektive Nullstellengebilde* oder die *projektive Varietät* zu \mathfrak{a} .

Definition 27.9. Der projektive Raum \mathbb{P}_K^n wird mit der *Zariski-Topologie* versehen, bei der die Mengen $V_+(\mathfrak{a}) \subseteq \mathbb{P}_K^n$ zu einem homogenen Ideal $\mathfrak{a} \subseteq K[X_0, X_1, \dots, X_n]$ als abgeschlossen erklärt werden.

Die offenen Mengen des projektiven Raumes sind demnach die Mengen der Form $D_+(\mathfrak{a})$ mit einem homogenen Ideal $\mathfrak{a} \subseteq K[X_0, \dots, X_n]$. Dabei sind die offenen Mengen $D_+(X_i)$ isomorph zu einem affinen Raum der Dimension n .

Bemerkung 27.10. Ein Punkt $P = (a_0, \dots, a_n) \in \mathbb{P}_K^n$ ist abgeschlossen, und zwar ist $P = V_+(\mathfrak{a})$ mit

$$\mathfrak{a} = (a_i X_j - a_j X_i : 0 \leq i, j \leq n).$$

Wenn $a_0 \neq 0$ ist, so kann man dies auch schreiben als $(X_j - \frac{a_j}{a_0} X_0 : j \neq 0)$. Die Erzeuger $a_i X_j - a_j X_i, i \neq 0$, sind dann überflüssig. Dies ist offenbar ein homogenes Ideal, und P liegt in $V_+(\mathfrak{a})$. Sei $a_0 \neq 0$ angenommen. Für einen weiteren Punkt $Q = (b_0, \dots, b_n) \in V_+(\mathfrak{a})$ folgt sofort $b_j - \frac{a_j}{a_0} b_0 = 0$ bzw.

$$(b_0, \dots, b_n) = \frac{b_0}{a_0} (a_0, \dots, a_n),$$

so dass es sich projektiv um den gleichen Punkt handelt.

\mathfrak{a} ist kein maximales Ideal, es ist aber maximal unter allen homogenen Idealen, die von (X_0, \dots, X_n) verschieden sind. Der Restklassenring $K[X_0, \dots, X_n]/\mathfrak{a}$ ist ein Polynomring in einer Variablen.

27.3. Der projektive Raum über \mathbb{R} und über \mathbb{C} .

Wir wollen uns ein Bild über die projektiven Räume für $\mathbb{K} = \mathbb{R}$ und $\mathbb{K} = \mathbb{C}$ machen. Die (reell) n -dimensionale Sphäre ist

$$S^n = \{x \in \mathbb{R}^{n+1} : \|x\| = 1\}.$$

Dabei ist $\|x\| = \sqrt{x_0^2 + \dots + x_n^2}$ die *euklidische Norm*.

Satz 27.11. Man kann den reell-projektiven Raum $\mathbb{P}_{\mathbb{R}}^n$ repräsentieren durch die n -dimensionale Sphäre $S^n \subset \mathbb{R}^{n+1}$ modulo der Äquivalenzrelation, die antipodale Punkte miteinander identifiziert.

Den komplex-projektiven Raum $\mathbb{P}_{\mathbb{C}}^n$ kann man repräsentieren durch die $(2n+1)$ -dimensionale Sphäre $S^{2n+1} \subset \mathbb{R}^{2n+2} \cong \mathbb{C}^{n+1}$ modulo der Äquivalenzrelation, die zwei Punkte $z, w \in S^{2n+1}$ miteinander identifiziert, wenn man $z = \lambda w$ mit einem $\lambda \in S^1$ schreiben kann.

Beweis. Wir behandeln die beiden Fälle parallel. Jeder Punkt der Sphäre S definiert eine (reelle oder komplexe) Gerade durch den Nullpunkt im umliegenden Raum \mathbb{R}^{n+1} oder \mathbb{C}^{n+1} und damit einen Punkt im projektiven Raum. Zwei Punkte $z, w \in S$ definieren genau dann die gleiche Gerade, wenn es einen Skalar $\lambda \in \mathbb{K}$ gibt mit $z = \lambda w$. Wegen der Multiplikativität der Norm ist dann auch $\|z\| = |\lambda| \cdot \|w\|$, woraus sich wegen $z, w \in S$ sofort $|\lambda| = 1$ ergibt. Dies bedeutet im reellen Fall $\lambda = \pm 1$ und im komplexen Fall, dass $\lambda \in S^1 \subset \mathbb{C}$ ist, also zum Einheitskreis gehört. \square

Wir haben insgesamt Abbildungen

$$S^n \subset \mathbb{R}^{n+1} - \{0\} \longrightarrow \mathbb{P}_{\mathbb{R}}^n$$

(im reellen Fall) bzw.

$$S^{2n+1} \subset \mathbb{R}^{2n+2} \cong \mathbb{C}^{n+1} \longrightarrow \mathbb{P}_{\mathbb{C}}^n$$

(im komplexen Fall). Nach dem vorstehenden Lemma sind die Gesamtabbildungen jeweils surjektiv. Man versieht die reell und die komplex-projektiven Räume mit der Quotiententopologie zur metrischen Topologie des reellen Vektorraumes unter dieser Abbildung, d.h. man erklärt eine Teilmenge $U \subseteq \mathbb{P}_{\mathbb{K}}^n$ für offen, wenn das Urbild in $\mathbb{K}^{n+1} - \{0\}$ offen ist. (dies ist äquivalent dazu, dass das Urbild auf der jeweiligen Sphäre offen ist). Mit dieser (*metrischen* oder *natürlichen*) Topologie auf dem projektiven Raum sind diese Abbildungen stetig. Dies hat folgende Konsequenz.

Lemma 27.12. *Für den reell-projektiven und den komplex-projektiven Raum sind die Teilmengen $D_+(X_i)$ offen in der natürlichen Topologie und homöomorph zu \mathbb{R}^n bzw. \mathbb{C}^n . Insbesondere sind die reell- und komplex-projektiven Räume topologische Mannigfaltigkeiten.*

Beweis. Das Urbild von $D_+(X_i)$ unter der kanonischen Abbildung ist $D(X)$, also das Komplement eines n -dimensionalen Untervektorraumes und damit offen in der natürlichen Topologie. Wir betrachten die stetigen Abbildungen

$$\mathbb{K}^n \cong V(X_i - 1) \subset D(X_i) \longrightarrow D_+(X_i).$$

Die Gesamtabbildung ist eine Bijektion und $D_+(X_i)$ trägt die Quotiententopologie unter der zweiten Abbildung. Wir müssen zeigen, dass die Bijektion eine Homöomorphie ist. Dazu genügt es, die Offenheit zu zeigen. Sei also $U \subseteq V(X_i - 1) \cong \mathbb{K}^n$ offen und U' das zugehörige Bild in $D_+(X_i)$. Die Offenheit von U' ist nach Definition der Quotiententopologie äquivalent dazu, dass das Urbild $U \subseteq D(X_i)$ von U' offen ist. Diese Menge U besteht aus allen Punkten in $D(X_i)$, die auf einer Geraden durch den Nullpunkt und durch einen Punkt aus U liegen. Sei Q ein solcher Punkt, und $Q = \lambda P$ mit $P \in U$ und $\lambda \in \mathbb{K}^\times$. Sei B eine offene Ballumgebung um P in $V(X_i - 1)$. Dann ist auch der dadurch definierte Kegel in $D(X_i)$ offen und liegt ganz in U . \square



Die projektive Gerade
über \mathbb{C} ist eine Sphäre.

Korollar 27.13. (*Kompaktheit der projektiven Räume*) Die reell-projektiven und die komplex-projektiven Räume sind kompakt und hausdorffsch in der natürlichen Topologie.

Beweis. Es gibt eine surjektive stetige Abbildung von einer Sphäre auf einen jeden projektiven Raum. Die Sphäre ist eine abgeschlossene und beschränkte Teilmenge eines reellen endlichdimensionalen Vektorraumes und daher kompakt. Da unter einer stetigen Abbildung das Bild einer kompakten Menge wieder kompakt ist, folgt, dass die projektiven Räume kompakt sind.

Für die Hausdorff-Eigenschaft seien $P, Q \in \mathbb{P}_{\mathbb{K}}^n$ zwei verschiedene Punkte. Man kann annehmen, dass sie beide auf einem der affinen überdeckenden Räume $D_+(X_i)$ liegen. Damit gibt es nach Satz 27.12 trennende Umgebungen. \square

28. VORLESUNG

28.1. Projektive Varietäten.

Definition 28.1. Eine *projektive Varietät* ist eine Zariski-abgeschlossene Teilmenge

$$V_+(\mathfrak{a}) \subseteq \mathbb{P}_K^n,$$

wobei \mathfrak{a} ein homogenes Ideal in $K[X_0, X_1, \dots, X_n]$ ist.

Eine projektive Varietät Y ist also die Nullstellenmenge im projektiven Raum einer (endlichen) Menge von homogenen Polynomen.

Über die induzierte Topologie ist eine projektive Varietät wieder mit einer Zariski-Topologie versehen. Die offenen Mengen haben wieder die Form $D_+(\mathfrak{b})$ zu einem homogenen Ideal aus $K[X_0, X_1, \dots, X_n]$ bzw. aus dem Restklassenring $K[X_0, X_1, \dots, X_n]/\mathfrak{a}$, den man auch den *homogenen Koordinatenring* zu $V(\mathfrak{a})$ nennt. Insbesondere definiert jedes homogene Element $F \in K[X_0, X_1, \dots, X_n]$ eine offene Menge $D_+(F) \subseteq Y$.

Lemma 28.2. Sei $Y \subseteq \mathbb{P}_K^n$ eine projektive Varietät. Dann liefern die affinen Räume $D_+(X_i) \cong \mathbb{A}_K^n \subset \mathbb{P}_K^n$ affine Varietäten

$$D_+(X_i) \cap Y,$$

die Y überdecken. Insbesondere gibt es zu jedem Punkt $P \in Y$ und jeder offenen Umgebung $P \in U$ affine offene Umgebungen von P innerhalb von U .

Beweis. Es ist

$$D_+(X_i) = D_+(X_i) \cap Y \cong \mathbb{A}_K^n \cap Y,$$

wobei links die zugehörige offene Menge in Y steht und rechts die entsprechende offene Teilmenge des projektiven Raumes. Daher ist $D_+(X_i) \cap Y$ eine abgeschlossene (siehe Aufgabe 28.3) Teilmenge des affinen Raumes $D_+(X_i) \cong \mathbb{A}_K^n$ und als solche selbst eine affine Varietät. Da die $D_+(X_i)$, $i = 0, \dots, n$, den projektiven Raum überdecken, gilt dies auch für die Durchschnitte mit Y . \square

Diese Aussage hat die unmittelbare Konsequenz, dass sich „lokale Konzepte“, die wir für affine Varietäten entwickelt haben, sofort auf projektive Varietäten übertragen. Für Eigenschaften, die für oder in einem Punkt gelten sollen, kann man sich sofort auf eine offene affine Umgebung des Punktes zurückziehen. Dies gilt bspw. für Konzepte wie Glattheit, Normalität oder den Begriff der regulären Funktion.

28.2. Algebraische Funktionen und Morphismen.

Mit dem zuletzt bewiesenen Resultat können wir auf einer projektiven Varietät wieder definieren, was eine reguläre oder algebraische Funktion sein soll.

Definition 28.3. Sei K ein algebraisch abgeschlossener Körper, $Y \subseteq \mathbb{P}_K^n$ eine projektive Varietät, $U \subseteq Y$ eine offene Teilmenge und $P \in U$ ein Punkt. Dann heißt eine Funktion $f : U \rightarrow \mathbb{A}_K^1 = K$ *algebraisch* (oder *regulär* oder *polynomial*) im Punkt P , wenn es eine offene affine Umgebung $P \in V \subseteq U$ gibt, derart, dass auf V die eingeschränkte Funktion f algebraisch im Punkt P ist. f heißt *algebraisch* auf U , wenn f in jedem Punkt aus U algebraisch ist.

Zu einer offenen Menge U bildet die Menge der auf U definierten regulären Funktionen wieder eine kommutative K -Algebra, die wieder mit $\Gamma(U, \mathcal{O})$ bezeichnet wird. Von nun an verstehen wir unter einer projektiven Varietät ein projektives Nullstellengebilde zusammen mit der induzierten Zariski-Topologie und versehen mit der *Strukturgarbe* \mathcal{O} der regulären Funktionen. Diese Konzepte übertragen sich sofort auf offene Teilmengen, was zum Begriff der quasiprojektiven Varietät führt.

Definition 28.4. Eine offene Teilmenge einer projektiven Varietät zusammen mit der induzierten Zariski-Topologie und versehen mit der Strukturgarbe der regulären Funktionen nennt man eine *quasiprojektive Varietät*.

Insbesondere ist eine projektive Varietät aber auch eine affine Varietät quasiprojektiv. Letzteres folgt daraus, dass man eine affine Varietät $Y \subseteq \mathbb{A}_n^K$ fortsetzen kann zu einer projektiven Varietät $\tilde{Y} \subseteq \mathbb{P}_n^K$, in der Y eine offene Teilmenge ist. Auch die Definition von Morphismus lässt sich wortgleich auf die allgemeinere Situation übertragen.

Definition 28.5. Seien X und Y zwei quasiprojektive Varietäten und sei

$$\psi : Y \longrightarrow X$$

eine stetige Abbildung. Dann nennt man ψ einen *Morphismus* (von quasiprojektiven Varietäten), wenn für jede offene Teilmenge $U \subseteq X$ und jede algebraische Funktion $f \in \Gamma(U, \mathcal{O})$ gilt, dass die zusammengesetzte Funktion

$$f \circ \psi : \psi^{-1}(U) \longrightarrow U \xrightarrow{f} \mathbb{A}_K^1$$

zu $\Gamma(\psi^{-1}(U), \mathcal{O})$ gehört.

28.3. Homogenisierung und projektiver Abschluss.

Betrachten wir die Hyperbel $V(XY - 1) \subset \mathbb{A}_K^2 \subset \mathbb{P}_K^2$. Die Hyperbel ist abgeschlossen in der affinen Ebene, aber nicht in der projektiven Ebene. Dies sieht man, wenn man die affine Ebene als $V(Z - 1)$ in den dreidimensionalen Raum einbettet und die durch die Punkte auf der Hyperbel definierten Geraden durch den Nullpunkt betrachtet. Diese Geraden neigen sich zunehmend stärker, und scheinen gegen die x -Achse und gegen die y -Achse zu konvergieren. Dies ist in der Tat, was auch die algebraische Berechnung ergibt.

Definition 28.6. Zu einem Ideal $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$ heißt das Ideal in $K[X_1, \dots, X_n, Z]$, das von allen Homogenisierungen von Elementen aus \mathfrak{a} erzeugt wird, die *Homogenisierung* \mathfrak{a}^h des Ideals \mathfrak{a} .

Man beachte, dass es hier im Allgemeinen nicht ausreicht, nur die Homogenisierungen aus einem Ideal-Erzeugendensystem aus \mathfrak{a} zu betrachten.

Definition 28.7. Zu einer affinen Varietät $V(\mathfrak{a}) \subset \mathbb{A}_K^n \subset \mathbb{P}_K^n$ heißt der Zariski-Abschluss von $V(\mathfrak{a})$ in \mathbb{P}_K^n der *projektive Abschluss* von $V(\mathfrak{a})$.

Satz 28.8. (*Projektiver Abschluss*) Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affine Varietät. Dann wird der projektive Abschluss durch $V_+(\mathfrak{b})$ beschrieben, wobei \mathfrak{b} die Homogenisierung von \mathfrak{a} in $K[X_1, \dots, X_n, Z]$ bezeichnet.

Beweis. Ein Punkt $P = (x_1, \dots, x_n)$ in \mathbb{A}_K^n definiert den Punkt $\tilde{P} = (x_1, \dots, x_n, 1)$ in \mathbb{P}_K^n . Für ein Polynom $F \in K[X_1, \dots, X_n]$ und P gilt $F(P) = \tilde{F}(\tilde{P})$ für die Homogenisierung \tilde{F} . Daher gilt insbesondere $\tilde{F}(\tilde{P}) = 0$

für alle Punkte $P \in V(\mathfrak{a})$ und alle homogenen Polynome aus dem homogenisierten Ideal \mathfrak{b} . Es ist also $V(\mathfrak{a}) \subseteq V_+(\mathfrak{b})$. Damit liegt insgesamt das kommutative Diagramm

$$\begin{array}{ccc} V(\mathfrak{a}) & \longrightarrow & V_+(\mathfrak{b}) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^n & \longrightarrow & \mathbb{P}_K^n \end{array}$$

vor (wobei alle Abbildungen injektiv sind). Der projektive Abschluss von $V(\mathfrak{a})$ wird von einer Menge $V_+(\mathfrak{c})$ mit einem homogenen Ideal \mathfrak{c} und mit $V(\mathfrak{a}) \subseteq V_+(\mathfrak{c})$ und $V_+(\mathfrak{c}) \subseteq V_+(\mathfrak{b})$ beschrieben.

Wir haben die Inklusion $V_+(\mathfrak{b}) \subseteq V_+(\mathfrak{c})$ zu zeigen, was aus $\mathfrak{c} \subseteq \text{rad}(\mathfrak{b})$ folgt. Da beides homogene Ideale sind, kann man sich auf $F \in \mathfrak{c}$ homogen beschränken. Wir schreiben $F = X_0^r G$, so dass G kein Vielfaches von X_0 ist. Da F auf $V(\mathfrak{a})$ verschwindet und da X_0 beschränkt auf $V(\mathfrak{a})$ konstant gleich eins ist, folgt, dass G auf $V(\mathfrak{a})$ verschwindet. Wir können also annehmen, dass F kein Vielfaches von X_0 ist. Dann ist die Dehomogenisierung $\bar{F} = F(X_1, \dots, X_n, 1)$ die Nullfunktion auf $V(\mathfrak{a})$ und besitzt den gleichen Grad wie F . Nach dem Hilbertschen Nullstellensatz gehört eine Potenz \bar{F}^r von \bar{F} zu \mathfrak{a} . Dann gehört aber auch F^r , das sich aus \bar{F}^r durch Homogenisieren ergibt, zur Homogenisierung von \mathfrak{a} , also zu \mathfrak{b} . \square

28.4. Projektive ebene Kurven.

Definition 28.9. Eine *projektive ebene Kurve* ist die Nullstellenmenge $C = V_+(F) \subset \mathbb{P}_K^2$ zu einem homogenen nicht-konstanten Polynom $F \in K[X, Y, Z]$.

Zu einer ebenen affinen Kurve $V(F) \subset \mathbb{A}_K^2$ liegt insgesamt die Situation

$$V = V(F) \subset \mathbb{A}_K^2 \subset \mathbb{P}_K^2$$

vor. Den (topologischen) Abschluss von V in \mathbb{P}_K^2 nennt man den *projektiven Abschluss* der Kurve.

Lemma 28.10. *Zu einer ebenen affinen Kurve $V = V(G) \subseteq \mathbb{A}_K^2 \subseteq \mathbb{P}_K^2$, $G \in K[X, Y]$, wird der Zariski-Abschluss von V in \mathbb{P}_K^2 durch $C = V_+(H)$ beschrieben, wobei H die Homogenisierung von G in $K[X, Y, Z]$ bezeichnet.*

Beweis. Dies folgt direkt aus Satz 28.8, da die Homogenisierung eines Hauptideals das durch die Homogenisierung erzeugte Hauptideal ist. \square

Bemerkung 28.11. Sei $G \in K[X, Y]$ mit der Homogenisierung $F \in K[X, Y, Z]$. Man gewinnt G aus F zurück, indem man Z durch 1 ersetzt. G beschreibt dann den Durchschnitt $D_+(Z) \cap V_+(F)$. Die beiden anderen affinen Ausschnitte, also

$$D_+(X) \cap V_+(F) \text{ und } D_+(Y) \cap V_+(F),$$

sind gleichberechtigt und liefern insbesondere affine Umgebungen für die Punkte von $C = V_+(F)$, die nicht in $D_+(Z)$ liegen.

Um bspw. die Glattheit in einem Punkt $P \in C$ nachzuweisen wählt man sich eine offene affine Umgebung (am besten eine der $D_+(L) \cap C, L = X, Y, Z$) und überprüft dort mit dem Ableitungskriterium und der affinen Gleichung die Glattheit in diesem Punkt. Dabei hängt das Ergebnis für den Punkt nicht davon ab, mit welcher affinen Umgebung man arbeitet (es kann aber manchmal die eine Umgebung rechnerisch geschickter sein als eine andere).

Von der affinen Kurve $V(G)$ aus gesehen sind die Punkte im Unendlichen die Punkte aus $V_+(F) \cap V_+(Z)$. Das ist der Schnitt der projektiven Kurve mit einer projektiven Geraden. Dies ist eine endliche Menge, es sei denn die projektive Gerade ist eine Komponente der Kurve, was aber nicht sein kann, wenn man mit einer affinen Kurve startet (da Z kein Teiler der Homogenisierung ist). Zur Berechnung der unendlich fernen Punkte betrachtet man die homogene Zerlegung

$$G = G_d + \dots + G_m \text{ mit } m \leq d$$

und die Homogenisierung

$$F = G_d + G_{d-1}Z + \dots + G_m Z^{d-m}.$$

Zur Berechnung des Durchschnittes mit $V_+(Z)$ muss man $Z = 0$ setzen, so dass man die Nullstellen des homogenen Polynoms $G_d(X, Y)$ (in zwei Variablen) berechnen muss. Der Grad d gibt also sofort eine Schranke, wie viele unendlich fernen Punkte es maximal auf der Kurve geben kann.

Beispiel 28.12. Wir betrachten den Standardkegel $V(X^2 + Y^2 - Z^2) \subset \mathbb{A}_K^3$. Da dies durch eine homogene Gleichung gegeben ist, kann man diesen Kegel auch sofort als eine ebene projektive Kurve (vom Grad zwei) auffassen. Die Schnitte des Kegels mit einer beliebigen Ebene $E \subset \mathbb{A}_K^3$ nennt man Kegelschnitte. Diese bekommen nun eine neue Interpretation. Eine Ebene E , auf der nicht der Nullpunkt liegt kann man in natürlicher Weise identifizieren mit einer offenen affinen Ebene $D_+(L) \subseteq \mathbb{P}_K^2$ (wobei L eine homogene Linearform ist). Die Schnitte mit dem Kegel sind dann verschiedene affine Ausschnitte aus der ebenen projektiven Kurve $V_+(X^2 + Y^2 - Z^2)$. Insbesondere sind also Kreis, Hyperbel und Parabel solche affinen Ausschnitte.

Die Schnitte mit einer Ebenen durch den Nullpunkt sind hingegen projektiv verstanden die endlichen Teilmengen $V_+(X^2 + Y^2 - Z^2) \cap V(L)$.

Definition 28.13. Sei K ein Körper und $d \geq 1$. Dann heißt die projektive Kurve

$$V(X^d + Y^d + Z^d) \subset \mathbb{P}_K^2$$

die *Fermat-Kurve* vom Grad d .

Für $d = 1$ handelt es sich einfach um eine projektive Gerade.

Lemma 28.14. *Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p \geq 0$ und sei $C = V_+(X^d + Y^d + Z^d) \subset \mathbb{P}_K^2$ die Fermat-Kurve vom Grad d . Die Charakteristik sei kein Teiler von d . Dann ist C eine glatte Kurve.*

Beweis. Da Glattheit eine lokale Eigenschaft ist, können wir mit einem beliebigen affinen Ausschnitt argumentieren. Da die Situation symmetrisch ist, können wir uns auf das affine Teilstück

$$V(X^d + Y^d + 1) \subset \mathbb{A}_K^2$$

beschränken. Die partiellen Ableitungen sind dX^{d-1} und dY^{d-1} . Aufgrund der Voraussetzung über die Charakteristik ist $d \neq 0$, so dass beide Ableitungen nur bei $x = y = 0$ verschwinden. Dieser Punkt gehört aber nicht zur Kurve. \square

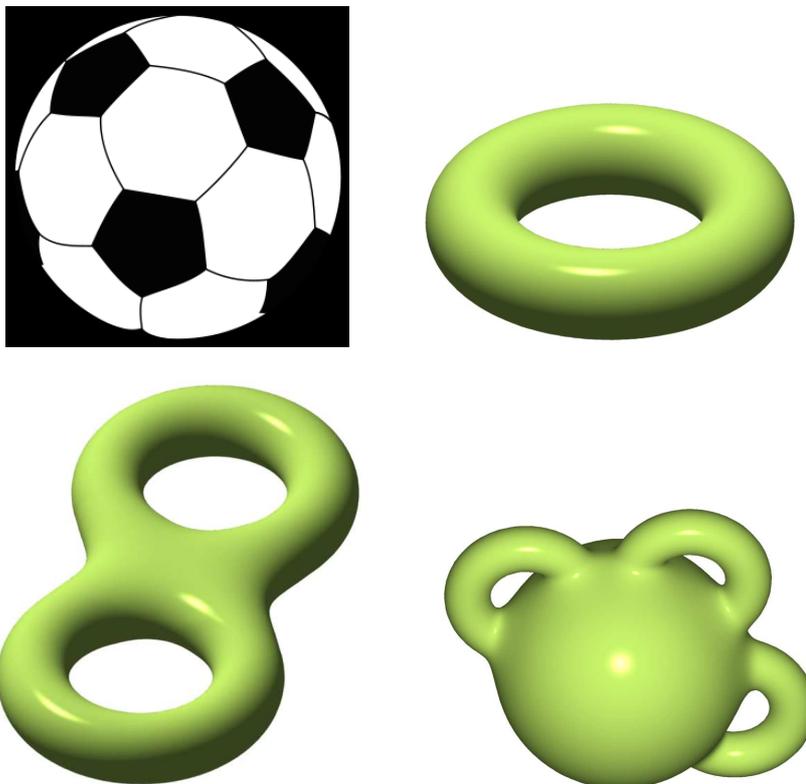
Bemerkung 28.15. Wählt man die komplexen Zahlen \mathbb{C} als Grundkörper, so kann man eine glatte projektive Kurve auch als eine reell zweidimensionale kompakte orientierte Mannigfaltigkeit auffassen. Diese lassen sich topologisch einfach klassifizieren, und zwar ist eine solche Mannigfaltigkeit homöomorph zu einer Kugeloberfläche, an die g Henkel angeklebt werden. Diese Zahl nennt man das *Geschlecht* der reellen Fläche und damit auch der Kurve. Die komplex-projektive Gerade ist eine zweidimensionale Sphäre und hat keinen Henkel, ihr Geschlecht ist also null. Eine Fläche vom Geschlecht eins ist ein Torus (Autoreifen), der homöomorph zu $S^1 \times S^1$ ist. Projektive Kurven, die als topologische Mannigfaltigkeit das Geschlecht eins besitzen, nennt man *elliptische Kurven*.

Es gibt auch algebraische Definitionen für das Geschlecht, so dass diese Invariante für glatte projektive Kurven über jedem algebraisch abgeschlossenen Körper definiert ist. Und zwar ist das Geschlecht gleich der K -Dimension der *ersten Kohomologiegruppe der Strukturgarbe* und auch gleich der K -Dimension der *globalen Differentialformen* auf der Kurve. Zu jedem g gibt es projektive Kurven mit Geschlecht g . Insbesondere kann man jede orientierbare reell zweidimensionale kompakte Fläche als komplex-projektive Kurve realisieren. Man spricht dann auch von *Riemannschen Flächen*.

Für eine glatte ebene Kurve $C = V_+(F) \subset \mathbb{P}_K^2$ vom Grad $d = \deg(F)$ gibt es eine einfache Formel für das Geschlecht: es ist nämlich

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

Damit haben glatte projektive Kurven vom Grad eins und zwei (Geraden und Quadriken) das Geschlecht null, es handelt sich in der Tat um projektive Geraden. Für $d = 3$ erhält man das Geschlecht 1, also elliptische Kurven. Für $d = 4$ erhält man schon $g = 3$. Dies zeigt auch, dass sich nicht jedes Geschlecht als Geschlecht einer ebenen glatten Kurve realisieren lässt. Es ist bspw. gar nicht so einfach, explizit Gleichungen für eine Kurve vom Geschlecht 2 anzugeben.



29. VORLESUNG

29.1. Projektion weg von einem Punkt.

Definition 29.1. Die Abbildung

$$\mathbb{P}_K^n - \{(1, 0, \dots, 0)\} \longrightarrow \mathbb{P}_K^{n-1}, (x_0, x_1, \dots, x_n) \longmapsto (x_1, \dots, x_n),$$

heißt *die Projektion weg vom Punkt* $(1, 0, \dots, 0)$.

Diese Abbildung ist ein wohldefinierter Morphismus, der außerhalb des *Zentrums* $(1, 0, \dots, 0)$ der Projektion definiert ist. Jedem anderen Punkt wird derjenige Punkt des \mathbb{P}_K^{n-1} zugeordnet, der der Geraden durch den Punkt und dem Zentrum entspricht. Daher ist die Abbildung surjektiv und jede Faser ist eine projektive Gerade ohne den Zentrumspunkt, also eine affine Gerade (es liegt ein sogenanntes *Geradenbündel* über dem \mathbb{P}_K^{n-1} vor). Es handelt sich um die Fortsetzung der Kegelabbildung $\mathbb{A}_K^n \rightarrow \mathbb{P}_K^{n-1}$ auf den projektiven Raum. Die entsprechende Abbildung kann man zu jedem Zentrumspunkt definieren, siehe Aufgabe 29.3.

29.2. Abbildungen nach \mathbb{P}_K^1 .

Der folgende Satz liefert eine neue Version der Noetherschen Normalisierung (siehe Satz 5.4).

Satz 29.2. Sei K ein algebraisch abgeschlossener Körper und sei $C \subset \mathbb{P}_K^2$ eine ebene projektive Kurve vom Grad d . Dann gibt es einen surjektiven Morphismus

$$C \longrightarrow \mathbb{P}_K^1$$

derart, dass alle Fasern aus maximal d Punkten bestehen.

Beweis. Es sei $P \in \mathbb{P}_K^2$ ein Punkt, der nicht auf der Kurve liegt. Einen solchen Punkt gibt es, da der Körper insbesondere unendlich ist. Wir betrachten die Projektion weg von P , die insgesamt einen Morphismus

$$C \hookrightarrow \mathbb{P}_K^2 - \{P\} \longrightarrow \mathbb{P}_K^1$$

induziert. Die Faser dieses Morphismus über einem Punkt $Q \in \mathbb{P}_K^1$ (der eine Richtung in $P \in \mathbb{P}_K^2$ repräsentiert) besteht genau aus den Punkten der Kurve, die auf der durch Q definierten Geraden

$$G = V_+(aX + bY + cZ) \cong \mathbb{P}_K^1 \subset \mathbb{P}_K^2$$

liegen. Daher wird die Faser über Q auf G beschrieben, indem man in der Kurvengleichung $C = V_+(F)$ mittels der Geradengleichung eine Variable eliminiert. Das Ergebnis ist ein homogenes Polynom \tilde{F} in zwei Variablen vom Grad d , das nicht null ist, denn sonst wäre P ein Punkt der Kurve. Da wir über einem algebraisch abgeschlossenen Körper sind besitzt dieses Polynom \tilde{F} mindestens eine und höchstens d Nullstellen, die alle von P verschieden sind. Dies ergibt die Surjektivität und die Abschätzung für die Faser. \square

Satz 29.3. Es sei K ein Körper und $C \subset \mathbb{P}_K^2$ eine glatte irreduzible ebene projektive Kurve. Es sei $D = C \cap D_+(Z) \cong K\text{-Spek}(R)$ ein affines Teilstück davon. Es sei $q = f/g \in Q(R)$ eine rationale Funktion (mit $f, g \in R$, $g \neq 0$). Dann gibt es einen eindeutigen Morphismus $\varphi : C \rightarrow \mathbb{P}_K^1$ derart, dass das Diagramm

$$\begin{array}{ccc} D(g) & \xrightarrow{f/g} & \mathbb{A}_K^1 \cong D_+(t) \\ \downarrow & & \downarrow \\ C & \xrightarrow{\varphi} & \mathbb{P}_K^1 \end{array}$$

kommutiert. Dabei werden die echten Polstellen (mit $g(P) = 0$ und $f(P) \neq 0$) von f/g in D auf den unendlich fernen Punkt $\infty \in \mathbb{P}_K^1$ abgebildet.

Beweis. Wir definieren zunächst auf D eine Fortsetzung $\varphi : D \rightarrow \mathbb{P}_K^1$ der rationalen Funktion f/g . Sei hierzu $P \in D$ ein Punkt der Kurve. Bei $P \in D(g)$ ist nichts zu tun, sei also $g(P) = 0$. Da die Kurve glatt ist, ist der lokale Ring B der Kurve im Punkt P ein diskreter Bewertungsring. Daher hat der Quotient f/g dort eine Beschreibung als

$$\frac{f}{g} = u\pi^n$$

mit $u \in B^\times$ und $n \in \mathbb{Z}$ (π sei eine Ortsuniformisierende). Es gibt eine offene Umgebung $P \in D(h) \subseteq D$ derart, dass π und u über $D(h)$ definiert sind und u dort eine Einheit ist. Bei $n \geq 0$ ist $f/g \in R_h$ und die undefinierte Stelle

ist also sogar als Abbildung nach \mathbb{A}_K^1 „hebbar“. Bei $n \leq 0$ ist der umgekehrte Bruch $g/f = u^{-1}\pi^{-n}$ auf $D(h)$ definiert als eine Abbildung nach \mathbb{A}_K^1 . Mittels der „verdrehten Einbettung“ $\mathbb{A}_K^1 \cong D_+(s) \hookrightarrow \mathbb{P}_K^1$ erhält man eine Abbildung nach \mathbb{P}_K^1 .

Wir müssen zeigen, dass diese zwei Morphismen in die projektive Gerade dort, wo beide definiert sind, übereinstimmen. Das sind die Punkte P mit $n = 0$. Die Verträglichkeit folgt daraus, dass in einer offenen Umgebung $P \in U$ eine Abbildung $f/g : U \rightarrow (\mathbb{A}_K^1)^\times = \mathbb{A}_K^1 - \{0\}$ vorliegt, und dass das Diagramm

$$\begin{array}{ccc} (\mathbb{A}_K^1)^\times & \xrightarrow{i^{-1}} & \mathbb{A}_K^1 \cong D_+(s) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^1 \cong D_+(t) & \longrightarrow & \mathbb{P}_K^1 \end{array}$$

kommutiert. Dies ergibt einen wohldefinierten Morphismus auf dem affinen Stück D .

Für einen beliebigen Punkt der projektiven Kurve C und eine affine Umgebung $P \in D' \subset C$ liegt die gleiche Situation vor, da $D_+(g) \cap D' \neq \emptyset$ ist, und somit auf einer offenen nichtleeren Menge die rationale Funktion (mit anderen Zählern und Nennern) definiert ist. Damit lässt sich das vorhergehende Argument genauso anwenden.

Die Eindeutigkeit folgt daraus, dass auf jeder affinen offenen Menge $P \in U$ der Durchschnitt $U \cap D_+(g)$ nicht leer ist. Ein Morphismus auf einer integren Varietät in die affine Gerade \mathbb{A}_K^1 ist durch die rationale Funktion eindeutig festgelegt. \square

Beispiel 29.4. Die Inversenbildung

$$\mathbb{A}_K^1 \supset D(z) \longrightarrow \mathbb{A}_K^1, z \longmapsto z^{-1},$$

lässt sich zu einem bijektiven Morphismus

$$\mathbb{P}_K^1 \longrightarrow \mathbb{P}_K^1, (x, y) \longmapsto (y, x)$$

fortsetzen. Dies folgt direkt aus Satz 29.3. Dabei geht ein Punkt $z \neq 0$ auf $1/z$ und der Nullpunkt geht auf den unendlich fernen Punkt ∞ .

29.3. Parametrisierte projektive ebene Kurven.

Sei eine rational parametrisierte Kurve $s \mapsto (\frac{\varphi_1(s)}{\psi(s)}, \frac{\varphi_2(s)}{\psi(s)})$ gegeben. Wir haben in Satz 6.11 gesehen, dass das Bild eine algebraische Gleichung erfüllt. Dabei haben wir im dortigen Beweis schon die homogenisierte Parametrisierung verwendet, die jetzt als projektive Fortsetzung wieder auftaucht.

Satz 29.5. *Es sei*

$$\mathbb{A}_K^1 \supseteq D(\psi) \longrightarrow \mathbb{A}_K^2, s \longmapsto \left(\frac{\varphi_1(s)}{\psi(s)}, \frac{\varphi_2(s)}{\psi(s)} \right),$$

eine rationale Parametrisierung in gekürzter (d.h. die $\varphi_1, \varphi_2, \psi$ haben keinen gemeinsamen Teiler) Darstellung. Es sei d der maximale Grad der beteiligten

Polynome und es seien $\tilde{\varphi}_1, \tilde{\varphi}_2, \tilde{\psi}$ die Homogenisierungen (in (s, t)) davon. Es seien H_i die Produkte dieser Homogenisierungen mit einer Potenz von s derart, dass H_1, H_2, H_3 alle den Grad d besitzen. Dann definieren die H_1, H_2, H_3 einen Morphismus

$$H : \mathbb{P}_K^1 \longrightarrow \mathbb{P}_K^2, (s, t) \longmapsto (H_1(s, t), H_2(s, t), H_3(s, t)),$$

derart, dass das Diagramm

$$\begin{array}{ccc} \mathbb{A}_K^1 \supseteq D(\psi) & \longrightarrow & \mathbb{A}_K^2 \cong D_+(Z) \\ \downarrow & & \downarrow \\ \mathbb{P}_K^1 & \xrightarrow{H} & \mathbb{P}_K^2 \end{array}$$

kommutativ ist. Dabei liegt das Bild unter H auf dem projektiven Abschluss der affinen Bildkurve.

Beweis. Die Abbildung H ist aufgrund von Aufgabe 29.2 wohldefiniert, und zwar auf ganz \mathbb{P}_K^1 , da $\varphi_1, \varphi_2, \psi$ insgesamt teilerfremd sind. Zur Kommutativität muss man lediglich beachten, dass $s \in D(\psi) \subseteq \mathbb{A}_K^1$ einerseits über $(s, 1)$ auf

$$(H_1(s, 1), H_2(s, 1), H_3(s, 1)) = (\varphi_1(s), \varphi_2(s), \psi(s))$$

abgebildet wird und andererseits auf

$$\left(\frac{\varphi_1(s)}{\psi(s)}, \frac{\varphi_2(s)}{\psi(s)}, 1 \right) = (\varphi_1(s), \varphi_2(s), \psi(s)).$$

Für den Zusatz sei C der affine Abschluss des Bildes und $\bar{C} \subset \mathbb{P}_K^2$ der projektive Abschluss davon. Wir betrachten das offene Komplement $U = \mathbb{P}_K^2 - \bar{C}$. Da die Abbildung stetig ist, ist das Urbild $H^{-1}(U)$ offen in \mathbb{P}_K^1 , und es kann nur Punkte aus $\mathbb{P}_K^1 - D(\psi)$ enthalten. Eine endliche und offene Teilmenge der projektiven Geraden muss aber leer sein. \square

Satz 29.6. Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X]$ ein Polynom in einer Variablen vom Grad $d \geq 1$. Dann wird der projektive Abschluss C des Graphen $V(Y - F(X))$ durch $V(YZ^{d-1} - \tilde{F}(X, Z))$ beschrieben, wobei $\tilde{F}(X, Z)$ die Homogenisierung von F bezeichnet. Dabei gibt es in C bei $d = 1$ (mit $F = aX + b$) noch den glatten Punkt $(1, -a, 0)$ und bei $d \geq 2$ noch den Punkt $(0, 1, 0)$, der bei $d \geq 3$ singulär ist. Bei $d \geq 2$ besitzt der Punkt im Unendlichen die Multiplizität $d - 1$.

Beweis. Die Gleichung für den projektiven Abschluss folgt direkt aus Satz 28.10. Der Schnitt mit der projektiven Geraden im Unendlichen erhält man, wenn man in der Gleichung $Z = 0$ setzt. Bei $d = 1$ liegt insgesamt die Geradengleichung $V_+(Y + aX + bZ)$ vor, und der Schnitt mit $V_+(Z)$ legt den einzigen Punkt $(1, -a, 0)$ fest. Bei $d \geq 2$ liegt die Kurvengleichung

$$V_+(YZ^{d-1} - s_d X^d - s_{d-1} X^{d-1} Z - \dots - s_0 Z^d)$$

mit $s_d \neq 0$ vor. Setzt man $Z = 0$ bleibt $V_+(-s_d X^d)$ übrig, woraus $X = 0$ folgt. Dies entspricht dem einzigen unendlich fernen Punkt $(0, 1, 0)$.

Für die Multiplizität betrachtet man die affine Gleichung der Kurve auf $D_+(Y)$. D.h. man setzt $Y = 1$ und erhält die affine Gleichung

$$V_+(Z^{d-1} - s_d X^d - s_{d-1} X^{d-1} Z - \dots - s_0 Z^d),$$

und der Punkt ist in diesen Koordinaten der Nullpunkt. Daher ist die Multiplizität $d - 1$ mit der einzigen durch $Z = 0$ gegebenen Tangente. Bei $d \geq 3$ ist die Multiplizität ≥ 2 und daher liegt ein singulärer Punkt vor. \square

Dieser Satz ist so zu verstehen, dass bei $d \geq 2$ die y -Achse (dafür steht der Punkt $(0, 1, 0)$) „asymptotisch“ zum Graph gehört (und auch die einzige Asymptote des Graphen ist). Die unendlich ferne Gerade $V_+(Z)$ ist die (einzige) Tangente an diesem Punkt. Die Normalisierung von C ist der \mathbb{P}_K^1 , und zwar ist die Normalisierungsabbildung nach Satz 29.5 gegeben durch

$$\mathbb{P}_K^1 \longrightarrow C \subset \mathbb{P}_K^2, (x, t) \longmapsto (xt^{d-1}, \tilde{F}(x, t), t^d).$$

Dabei geht der unendlich ferne Punkt $(1, 0)$ auf $(0, s_d, 0) = (0, 1, 0)$.

Satz 29.7. *Sei K ein algebraisch abgeschlossener Körper und seien $G, H \in K[X]$ Polynome in einer Variablen vom Grad $d, e \geq 1$ ohne gemeinsame Nullstelle. Sei $H \neq 0$ und sei $F(X) = G(X)/H(X)$ die zugehörige rationale Funktion. Seien $\tilde{H}(X, Z)$ und $\tilde{G}(X, Z)$ die zugehörigen Homogenisierungen. Dann wird der projektive Abschluss C des Graphen von $F(X)$ bei $d > e$ durch*

$$V_+(\tilde{H}(X, Z)Y Z^{d-e-1} - \tilde{G}(X, Z))$$

und bei $d \leq e$ durch

$$V_+(\tilde{H}(X, Z)Y - \tilde{G}(X, Z)Z^{e-d+1})$$

beschrieben.

Beweis. Die affine Beschreibung der Kurve ist $V(YH - G)$. Nach Satz 28.10 wird der projektive Abschluss durch die Homogenisierung von $YH - G$ beschrieben. Für diese ist der maximale Grad von YH und G ausschlaggebend, der Summand mit kleinerem Grad muss durch eine geeignete Potenz von Z „aufgefüllt“ werden. Dies ergibt die angegebenen Gleichungen. \square

29.4. Monomiale projektive Kurven.

Zu einer ebenen monomialen Kurve $s \mapsto (s^e, s^d) = (x, y)$ mit teilerfremden Exponenten $e > d$ gehört nach Satz 29.5 die monomiale projektive Kurve

$$(s, t) \longmapsto (s^e, s^d t^{e-d}, t^e).$$

Auf der offenen Menge $D_+(t)$ ist dies die ursprüngliche Abbildung und auf $D_+(s)$ ist dies die affine Abbildung

$$t \longmapsto (t^{e-d}, t^e).$$

Satz 29.8. Seien $e > d$ teilerfremd. Für die zugehörige durch

$$(s, t) \longmapsto (s^e, s^d t^{e-d}, t^e)$$

gegebene ebene projektive monomiale Kurve C vom Grad e gelten folgende Aussagen.

- (1) Die Kurve wird beschrieben durch die homogene Gleichung $Y^e = X^d Z^{e-d}$ vom Grad e .
- (2) Die Kurve ist glatt für alle Punkte $\neq (0, 0, 1)$ und $\neq (1, 0, 0)$.
- (3) Die Kurve hat im Punkt $(0, 0, 1)$ die Multiplizität d und im Punkt $(1, 0, 0)$ die Multiplizität $e - d$.
- (4) Bei $e \geq 3$ ist die Kurve nicht glatt.

Beweis. (1) Die affine Gleichung ist $Y^e - X^d$, und nach Satz 28.10 wird der projektive Abschluss durch die Homogenisierung, also durch $V(Y^e - X^d Z^{e-d})$ beschrieben.

- (2) Auf der affinen Kurve $V(X^d - Y^e) \subset \mathbb{A}_K^2 \subset \mathbb{P}_K^2$ ist nach Satz 20.12 nur der Nullpunkt, der dem projektiven Punkt $(0, 0, 1)$ entspricht, (eventuell) nicht glatt. Die Punkte auf der Kurve außerhalb von $D_+(Z)$ erhält man, indem man in der Gleichung $Z = 0$ setzt. Dies erzwingt $Y = 0$, so dass es lediglich noch den Punkt $(1, 0, 0)$ gibt.
- (3) Die Multiplizität in einem Punkt ist eine lokale Eigenschaft. Der Punkt $(0, 0, 1)$ entspricht dem Nullpunkt auf der affinen monomialen Kurve $V(X^d - Y^e)$, deren Multiplizität im Nullpunkt nach Korollar 23.9 gleich dem kleineren Exponenten, also gleich d ist. Der Punkt $(1, 0, 0)$ liegt auf $D_+(X)$ und dort ist $V(Y^e - Z^{e-d})$ die affine Gleichung. Die Multiplizität ist wieder der kleinere Exponent, also gleich $e - d$.
- (4) folgt aus (3).

□

30. VORLESUNG

30.1. Der Satz von Bezout.

Wir werden in dieser Vorlesung den Satz von Bezout für die projektive Ebene beweisen, das ist die Aussage, dass für zwei projektive Kurven in der projektiven Ebene ohne gemeinsame Komponente vom Grad m und n die Summe über alle Schnittmultiplizitäten gleich mn ist. Unsere Darstellung folgt weitgehend dem Aufbau in Fulton.

Zu einem Polynomring P und einer natürlichen Zahl ℓ bezeichnet P_ℓ im Folgenden die sogenannte ℓ -te Stufe, die aus allen homogenen Polynomen vom Grad ℓ besteht. Diese Bezeichnungsweise übernehmen wir auch für homogene Restklassenringe des Polynomrings. Diese Stufen werden über dem

Grundkörper K von allen Monomen vom Grad ℓ erzeugt. Insbesondere handelt es sich um endlichdimensionale K -Vektorräume.

Lemma 30.1. *Sei K ein Körper und seien $F, G \in K[X, Y, Z] = P$ zwei homogene Polynome vom Grad m und n ohne gemeinsamen nichtkonstanten Teiler. Dann ist*

$$\dim_K(P/(F, G))_\ell = mn \text{ für } \ell \text{ hinreichend groß.}$$

Beweis. Wir betrachten die exakte Sequenz

$$0 \longrightarrow P \xrightarrow{(G, -F)} P \times P \xrightarrow{(F, G)} P \longrightarrow P/(F, G) \longrightarrow 0.$$

Dabei steht vorne die Abbildung $H \mapsto (GH, -FH)$, dann folgt die Abbildung $(A, B) \mapsto (AF + BG)$ und schließlich die Restklassenbildung. All diese Abbildungen sind P -Modul Homomorphismen. Die Injektivität vorne ist klar, da P ein Integritätsbereich ist. Die Exaktheit an den beiden hinteren Stellen ist klar, bleibt noch die Exaktheit an der zweiten Stelle zu zeigen. Dort ist klar, dass die Verknüpfung die Nullabbildung ist. Sei also $AF + BG = 0$ in P . Da P faktoriell ist und da F und G teilerfremd sind folgt aber, dass A ein Vielfaches von G sein muss. Dann kann man durch G teilen und erhält, dass B ein Vielfaches von F sein muss (mit dem gleichen Faktor). Also kommt (A, B) von links.

Da F und G homogen sind mit fixierten Graden, kann man diese Sequenz einschränken auf homogene Stufen, und zwar ergibt sich dabei die kurze exakte Sequenz

$$0 \longrightarrow P_{\ell-m-n} \xrightarrow{(G, -F)} P_{\ell-m} \times P_{\ell-n} \xrightarrow{(F, G)} P_\ell \longrightarrow (P/(F, G))_\ell \longrightarrow 0$$

(dabei sind die Stufen für negativen Index null). Die Exaktheit bleibt erhalten, da bei einem homogenen Homomorphismus die Stufen unabhängig voneinander sind. Alle beteiligten Stufen sind nun endlichdimensionale Vektorräume. Für $\ell \geq m + n$ sind alle Indizes nichtnegativ und daher gilt $\dim(P_\ell) = \frac{(\ell+1)(\ell+2)}{2}$. Wegen der Additivität der Dimension bei exakten Sequenzen ergibt sich

$$\begin{aligned} & \dim((P/(F, G))_\ell) \\ &= \frac{(\ell+1)(\ell+2)}{2} - \frac{(\ell-m+1)(\ell-m+2)}{2} - \frac{(\ell-n+1)(\ell-n+2)}{2} \\ & \quad + \frac{(\ell-m-n+1)(\ell-m-n+2)}{2} \\ &= \frac{2 - (-m+1)(-m+2) - (-n+1)(-n+2) + (-m-n+1)(-m-n+2)}{2} \\ &= \frac{2mn}{2} \\ &= mn. \end{aligned}$$

□

Lemma 30.2. *Sei K ein algebraisch abgeschlossener Körper und seien $F, G \in K[X, Y, Z]$ homogene Polynome ohne gemeinsame (projektive) Nullstelle auf $V_+(Z) \subset \mathbb{P}_K^2$. Es sei $R = K[X, Y, Z]/(F, G)$ der zugehörige Restklassenring. Dann ist die Abbildung*

$$R \longrightarrow R, H \longmapsto ZH,$$

injektiv.

Beweis. Sei $H \in K[X, Y, Z]$ und vorausgesetzt, dass H unter der angegebenen Abbildung auf null geht. Das bedeutet, dass eine Gleichung

$$ZH = LF + MG$$

mit $L, M \in K[X, Y, Z]$ vorliegt. Wir ersetzen in dieser Gleichung die Variable Z durch 0 und erhalten die Gleichung

$$0 = L(X, Y, 0)F(X, Y, 0) + M(X, Y, 0)G(X, Y, 0)$$

in $K[X, Y]$. Nach der Voraussetzung, dass es keine gemeinsame projektive Nullstelle auf $V_+(Z)$ gibt, sind $F(X, Y, 0)$ und $G(X, Y, 0)$ (als homogene Polynome) teilerfremd. Das bedeutet, dass es ein Polynom $Q \in K[X, Y]$ mit

$$L(X, Y, 0) = QG(X, Y, 0) \text{ und } M(X, Y, 0) = -QF(X, Y, 0).$$

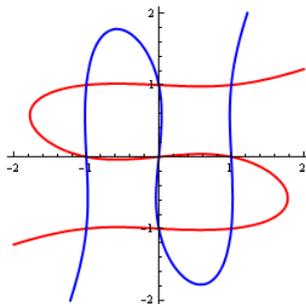
Dies wiederum heißt zurückübersetzt nach $K[X, Y, Z]$, dass dort

$$L = QG(X, Y, 0) + Z\tilde{L} \text{ und } M = -QF(X, Y, 0) + Z\tilde{M}$$

gilt. Mit $F = F(X, Y, 0) + Z\tilde{F}$ und $G = G(X, Y, 0) + Z\tilde{G}$ ergibt sich aus der Ausgangsgleichung

$$\begin{aligned} ZH &= LF + MG \\ &= (QG(X, Y, 0) + Z\tilde{L})F + (-QF(X, Y, 0) + Z\tilde{M})G \\ &= Q(G - Z\tilde{G})F - Q(F - Z\tilde{F})G + Z\tilde{L}F + Z\tilde{M}G \\ &= -QZ\tilde{G}F + QZ\tilde{F}G + Z\tilde{L}F + Z\tilde{M}G \\ &= Z(-Q\tilde{G}F + Q\tilde{F}G + \tilde{L}F + \tilde{M}G). \end{aligned}$$

Aus dieser Gleichung können wir Z herauskürzen und erhalten eine Darstellung für H als Linearkombination aus F und G . Damit ist die Restklasse von H in R ebenfalls 0. □



Satz 30.3. (Satz von Bezout) Sei K ein algebraisch abgeschlossener Körper und seien $F, G \in K[X, Y, Z]$ zwei homogene Polynome vom Grad m und n ohne gemeinsame Komponente mit zugehörigen Kurven $C = V_+(F), D = V_+(G) \subset \mathbb{P}_K^2$. Dann gilt

$$\sum_P \text{mult}_P(C, D) = mn.$$

Beweis. Der Durchschnitt $C \cap D$ besteht nur aus endlich vielen Punkten. Wir können daher annehmen, dass alle Schnittpunkte in $\mathbb{A}_K^2 = D_+(Z) \subset \mathbb{P}_K^2$ liegen. Es seien \tilde{F} und \tilde{G} die inhomogenen Polynome aus $K[X, Y]$, die die affinen Kurven $C \cap \mathbb{A}_K^2$ und $D \cap \mathbb{A}_K^2$ beschreiben. Damit ist

$$\begin{aligned} \sum_{P \in \mathbb{P}_K^2} \text{mult}_P(F, G) &= \sum_{P \in \mathbb{A}_K^2} \text{mult}_P(\tilde{F}, \tilde{G}) \\ &= \sum_{P \in \mathbb{A}_K^2} \dim_K (K[X, Y]_{\mathfrak{m}_P} / (\tilde{F}, \tilde{G})) \\ &= \dim_K (K[X, Y] / (\tilde{F}, \tilde{G})). \end{aligned}$$

Dabei beruht die letzte Gleichung auf Satz 26.11. Wie wollen die Dimension dieses inhomogenen Restklassenrings mit der Dimension einer Stufe des homogenen Restklassenrings $(K[X, Y, Z]/(F, G))_\ell$ in Verbindung bringen. Von letzterer wissen wir aufgrund von Lemma 30.1, dass sie für ℓ hinreichend groß gleich mn ist.

Wir wählen eine Basis V_1, \dots, V_{mn} von $(K[X, Y, Z]/(F, G))_\ell$ (ℓ hinreichend groß und fixiert) und behaupten, dass die Dehomogenisierungen $v_i = V_i(X, Y, 1)$ eine Basis von $K[X, Y]/(\tilde{F}, \tilde{G})$ bilden. Dazu sei $q \in K[X, Y]$ beliebig vorgegeben mit Homogenisierung $Q \in K[X, Y, Z]$ vom Grad d . Sei e so gewählt, dass $d + e \geq \ell$ ist. Aufgrund von Lemma 30.2 sind die Abbildungen

$$(K[X, Y, Z]/(F, G))_\ell \longrightarrow (K[X, Y, Z]/(F, G))_{\ell+\lambda}, \quad Q \longmapsto Z^\lambda Q,$$

injektiv und daher auch bijektiv, da die Dimensionen übereinstimmen. Es gibt dann also eine Darstellung $Z^e Q = \sum_{i=1}^{mn} a_i Z^{d+e-\ell} V_i$. Durch Dehomogenisieren ergibt sich daraus sofort eine Darstellung für q .

Für die lineare Unabhängigkeit sei $\sum_{i=1}^{mn} a_i v_i$ angenommen, so dass in $K[X, Y]$ eine Gleichung $\sum_{i=1}^{mn} a_i v_i = \tilde{A}\tilde{F} + \tilde{B}\tilde{G}$ vorliegt. Dabei setzen wir \tilde{A}, \tilde{B} als Dehomogenisierung von zwei homogenen Polynomen $A, B \in K[X, Y, Z]$ an, so

dass zwei Ausdrücke vorliegen – nämlich $\sum_{i=1}^{mn} a_i V_i$ und $AF + BG$ –, deren Dehomogenisierungen übereinstimmen. Die ursprünglichen homogenen Polynome kann man aber aus der Dehomogenisierung rekonstruieren, in dem man homogenisiert und mit einer Potenz von Z multipliziert. Aus der Gleichung erhält man also durch Homogenisierung (wobei der höchste Grad ausschlaggebend ist) eine Gleichung der Form

$$\sum_{i=1}^{mn} a_i Z^r V_i = Z^s AF + Z^t BG,$$

in der alle Summanden den gleichen Grad besitzen. Dabei kommt links nur eine Potenz von Z vor, da die V_i homogen vom gleichen Grad sind. Diese Gleichung bedeutet $\sum_{i=1}^{mn} a_i Z^r V_i$ in $K[X, Y, Z]/(F, G)$, woraus sich $a_i = 0$ ergibt. \square

Korollar 30.4. *Sei K ein algebraisch abgeschlossener Körper und seien $C, D \subset \mathbb{P}_K^2$ zwei ebene projektive Kurven. Dann ist der Durchschnitt $C \cap D$ nicht leer.*

Beweis. Die Aussage stimmt, wenn C und D eine gemeinsame Komponente besitzen. Andernfalls folgt sie aus Satz 30.3. \square

Korollar 30.5. *Sei K ein algebraisch abgeschlossener Körper und seien $F, G \in K[X, Y, Z]$ zwei homogene Polynome vom Grad m und n ohne gemeinsame Komponente mit zugehörigen Kurven $C = V_+(F), D = V_+(G) \subset \mathbb{P}_K^2$. Dann gibt es maximal mn Schnittpunkte von C und D .*

Beweis. Dies folgt direkt aus Satz 30.3, da jeder Schnittpunkt zumindest mit Schnittmultiplizität 1 in die Summe eingeht. \square

Beispiel 30.6. Wir betrachten die Neilsche Parabel $C = (ZY^2 - X^3)$ und den Kreis mit Mittelpunkt $(1, 0, 1)$, also $D = V((X - Z)^2 + Y^2 - Z^2)$. Nach dem Satz von Bezout erwarten wir eine Gesamtschnittzahl von 6. Wir berechnen die Schnittpunkte. Für $Z = 0$ folgt aus der ersten Gleichung $X = 0$ und dann aus der zweiten $Y = 0$, so dass es keinen Schnittpunkt auf der projektiven Geraden $V_+(Z)$ gibt. Wir betrachten daher die affinen Gleichungen $Y^2 - X^3 =$ und $(X - 1)^2 + Y^2 - 1 =$. Wir berechnen die Schnittpunkte, indem wir $Y^2 = 1 - (X - 1)^2$ in die erste Gleichung einsetzen. Dies ergibt

$$1 - (X - 1)^2 - X^3 = -X^3 - X^2 + 2X = X(-X^2 - X + 2) = -X(X - 1)(X + 2).$$

Dies führt zu den Schnittpunkten

$$(0, 0), (1, 1), (1, -1), (-2, 2\sqrt{2}i), (-2, -2\sqrt{2}i).$$

Die beiden letzten Punkte zeigen auch, dass der Satz nur über einem algebraisch abgeschlossenen Körper gilt. Es gibt also nur fünf Schnittpunkte. Da die Neilsche Parabel im Nullpunkt eine Singularität besitzt und dieser ein

Schnittpunkt ist, so muss dort die Schnittmultiplizität größer als 1 sein. Um dies zu bestätigen betrachten wir

$$\begin{aligned}
 & K[X, Y]_{(X, Y)} / (Y^2 - X^3, Y^2 - 1 + (X - 1)^2) \\
 &= K[X, Y]_{(X, Y)} / (Y^2 - X^3, X(X - 1)(X + 2)) \\
 &= K[X, Y]_{(X, Y)} / (Y^2 - X^3, X) \\
 &= K[X, Y]_{(X, Y)} / (Y^2, X) \\
 &= K[Y] / (Y^2).
 \end{aligned}$$

Dabei haben wir die Einsetzungsrechnung von oben wiederholt und dann ausgenutzt, dass $X - 1$ und $X + 2$ Einheiten im lokalen Ring $K[X, Y]_{(X, Y)}$ sind. Die Dimension ist also 2 und damit muss die Schnittmultiplizität an allen anderen Schnittpunkten 1 sein, was man auch direkt bestätigen kann.

ANHANG 1: BILDLICENSEN

Die Bilder dieses Textes stammen aus Commons (also <http://commons.wikimedia.org>), und stehen unter unterschiedlichen Lizenzen, die zwar alle die Verwendung hier erlauben, aber unterschiedliche Bedingungen an die Verwendung und Weitergabe stellen. Es folgt eine Auflistung der verwendeten Bilder dieses Textes (nach der Seitenzahl geordnet, von links nach rechts, von oben nach unten) zusammen mit ihren Quellen, Urhebern (Autoren) und Lizenzen. Dabei ist *Quelle* so zu verstehen, dass sich, wenn man

<http://commons.wikimedia.org/wiki/File:>

unmittelbar davor setzt, die entsprechende Datei auf Commons ergibt. *Autor* benennt den Urheber des Werkes, falls dieser bekannt ist. *Benutzer* meint den Hochlader der Datei; wenn keine weitere Information über den Autor vorliegt, so gilt der Benutzer als Urheber. Die Angabe des Benutzernamen ist so zu verstehen, dass sich, wenn man

<http://commons.wikimedia.org/wiki/User:>

unmittelbar davor setzt, die Benutzerseite ergibt. Wenn das Bild ursprünglich in einem anderen Wikimedia-Projekt hochgeladen wurde, so wird die Domäne (bspw. *de.wikipedia.org*) explizit angegeben.

Die *Lizenz* ist die auf der Dateiseite auf Commons angegebene Lizenz. Dabei bedeuten

- GFDL: Gnu Free Documentation License (siehe den angehängten Text, falls diese Lizenz vorkommt)
- CC-BY-SA-2.5 (3.0): Creative Commons Attribution ShareAlike 2.5 (oder 3.0)
- PD: gemeinfrei (public domain)

ABBILDUNGSVERZEICHNIS

Quelle = Linear function.svg , Autor = Benutzer Luks auf Commons, Lizenz = PD	7
Quelle = Polynomialdeg4.png, Autor = Benutzer Derbeth auf Commons, Lizenz = CC-BY-SA-2.5	7
Quelle = RationalDegree2byXedi.gif , Autor = Sam Derbyshire (= Benutzer Ylebru auf en-wikipedia.org), Lizenz = GFDL	7
Quelle = Circle.svg , Autor = Benutzer Zorgt auf Commons, Lizenz = CC-BY-SA-3.0	7

Quelle = Ellipse.svg , Autor = Benutzer Zorgit auf Commons, Lizenz = CC-BY-SA-3.0	7
Quelle = Cusp.png , Autor = Benutzer Satipatthana auf Commons, Lizenz = PD	7
Quelle = Elliptic curve simple.png , Autor = Sean Kelly (= Benutzer Giro720 auf en-wikipedia.org), Lizenz = GFDL	7
Quelle = Tschirnhausen cubic.png , Autor = Oleg Alexandrov (= Benutzer Oleg Alexandrov auf Commons), Lizenz = PD	7
Quelle = Eudoxus.png , Autor = Donald Hosek (= Benutzer Oleg Alexandrov auf Commons), Lizenz = PD	7
Quelle = Conchoid of Pascal.png , Autor = Benutzer Luke33 auf Commons, Lizenz = PD	8
Quelle = Bifolium.png , Autor = Oleg Alexandrov (= Benutzer Oleg Alexandrov auf Commons), Lizenz = PD	8
Quelle = Limacon.png , Autor = Benutzer Berto auf Commons, Lizenz = PD	8
Quelle = Rose curve (four leaves).svg , Autor = Benutzer Gunther auf Commons, Lizenz = PD	8
Quelle = Lemniscate of Bernoulli.svg , Autor = Benutzer Zorgit auf Commons, Lizenz = CC-BY-SA-3.0	8
Quelle = Cicloide.svg , Autor = Benutzer Elborgo auf Commons, Lizenz = CC-BY-SA-2.5	8
Quelle = Logarithmic spiral.png , Autor = Benutzer Anarkman auf en.wikipedia.org, Lizenz = GFDL	8
Quelle = Sin.svg , Autor = Keytotime (= Benutzer Ysae auf Commons), Lizenz = PD	8
Quelle = Quadratic Koch.png , Autor = Alexis Monnerot-Dumaine (= Benutzer Prokofiev auf Commons), Lizenz = CC-BY-SA-2.5	8
Quelle = Rectangular hyperbola.svg , Autor = Benutzer Qef auf Commons, Lizenz = PD	10
Quelle = GodfreyKneller-IsaacNewton-1689.jpg , Autor = Godfrey Kneller, Lizenz = PD	11
Quelle = ECexamples01.png , Autor = Benutzer Dake auf Commons, Lizenz = GFDL	12

	175
Quelle = Carl Friedrich Gauss.jpg , Autor = Benutzer Bcrowell auf Commons, Lizenz = PD	14
Quelle = Conic sections 2n.png, Autor = Benutzer NK auf Commons, Lizenz = GFDL	16
Quelle = Conjuntos algebraicos 2.svg , Autor = Benutzer Drini auf Commons, Lizenz = GFDL	21
Quelle = Linline.jpg, Autor = Benutzer Astur1 auf Commons, Lizenz = PD	21
Quelle = IntersectingPlanes.png, Autor = Benutzer Stib auf en.wikipedia.org, Lizenz = GFDL	22
Quelle = Secretsharing-3-point.png, Autor = Benutzer Stib auf en.wikipedia.org, Lizenz = GFDL	22
Quelle = Delaunay points.png, Autor = Benutzer Nü Es auf Commons, Lizenz = GFDL	25
Quelle = Gerade svg.svg, Autor = Benutzer Lokilech auf Commons, Lizenz = GFDL	25
Quelle = Hydrant Insel Krk Kroatien.jpg, Autor = Benutzer Usien auf Commons, Lizenz = GFDL	27
Quelle = Cylinder principal directions.svg, Autor = Luca Antonelli (= Benutzer Luke Antony auf Commons), Lizenz = GFDL	28
Quelle = Two cubic curves.png, Autor = Benutzer Hack auf Commons, Lizenz = PD	29
Quelle = Kuzel obecny.svg, Autor = Benutzer Pajs auf cs.wikipedia.org, Lizenz = PD	30
Quelle = Krivka parametricky.png, Autor = Benutzer Beny auf cs.wikipedia.org, Lizenz = PD	35
Quelle = Cubic with double point.svg, Autor = Benutzer Gunther auf de.wikipedia.org, Lizenz = PD	37
Quelle = Dioklova kisoida.png, Autor = Benutzer Pajs auf cs.wikipedia.org, Lizenz = PD	41
Quelle = DoubleCone.png, Autor = Lars H. Rohwedder (= Benutzer RokerHRO auf Commons), Lizenz = PD	41
Quelle = Conic sections.svg, Autor = Benutzer Anuskafm auf Commons, Lizenz = GFDL	41

Quelle = Hauptachsentransformation1.png, Autor = Benutzer Rdb auf Commons, Lizenz = PD	45
Quelle = Hauptachsentransformation2.png, Autor = Benutzer Rdb auf Commons, Lizenz = PD	45
Quelle = Hauptachsentransformation3.png, Autor = Benutzer Rdb auf Commons, Lizenz = PD	45
Quelle = Johannes Kepler 1610.jpg, Autor = Unbekannt (1610), Lizenz = PD	48
Quelle = Elliptic orbit.gif, Autor = Benutzer Brandir auf Commons, Lizenz = GFDL+CC-BY-SA 2.5	49
Quelle = Parabolic orbit.gif, Autor = Benutzer Brandir auf Commons, Lizenz = GFDL+CC-BY-SA 2.5	49
Quelle = Hyperbolic orbit.gif, Autor = Benutzer Brandir auf Commons, Lizenz = GFDL+CC-BY-SA 2.5	49
Quelle = Lemniscate Building.gif, Autor = Benutzer Zorgit auf Commons, Lizenz = CC-BY-SA 3.0	49
Quelle = Parallele lijnen.png , Autor = Benutzer Ellywa auf nl.wikipedia.org, Lizenz = GFDL	52
Quelle = Ellipse tri.png, Autor = Benutzer ? (hebräischer Name) auf he.wikipedia.org, Lizenz = GFDL	53
Quelle = Steam engine in action.gif, Autor = Benutzer Panther auf Commons, Lizenz = CC-BY-SA 2.5	54
Quelle = Intersection of cylinders.jpg , Autor = Jan Schoenke, Lizenz = CC-BY-SA 2.5	56
Quelle = Alg Kurven OS2008 Lsg8.10 v2.png, Autor = Christian Boberg, Lizenz = CC-BY-SA 2.5	57
Quelle = Noether.jpg, Autor = Unbekannt (vor 1910), Lizenz = PD	59
Quelle = David Hilbert 1886.jpg , Autor = Unbekannt (1886), Lizenz = PD	60
Quelle = Disjoint ellipses.png, Autor = Benutzer pmidden auf Commons, Lizenz = PD	71
Quelle = Alexander Grothendieck.jpg, Autor = Konrad Jacobs, Lizenz = CC-BY-SA 2.0	73
Quelle = Linline.jpg , Autor = Astur1, Lizenz = PD	74

	177
Quelle = Lineair-cartesiaans.png , Autor = MADe, Lizenz = GFDL	74
Quelle = Polynomialdeg5.png , Autor = Benutzer Derbeth auf Commons, Lizenz = CC-BY-SA-2.5	74
Quelle = Hyperbola one over x.svg , Autor = Benutzer Ktims auf Commons, Lizenz = GFDL	81
Quelle = Connected and disconnected spaces2.svg, Autor = Benutzer Dbc334 auf Commons, Lizenz = PD	82
Quelle = Monkey Saddle Surface (Shaded).png, Autor = Benutzer Inductiveload auf Commons, Lizenz = PD	88
Quelle = Concentric (PSF).png, Autor = Pearson Scott Foresman, Lizenz = PD	92
Quelle = Kaffeefilter.jpg , Autor = Elke Wetzig (= Benutzer Elya auf Commons), Lizenz = GFDL	95
Quelle = Cone intersects line.png, Autor = Benutzer Pmidden auf Commons, Lizenz = PD	100
Quelle = FiberBundle 2.png, Autor = Benutzer 1 3 2 人 auf ja.wikipedia.org, Lizenz = GFDL	101
Quelle = Cusp.png , Autor = Benutzer Satipatthana auf Commons, Lizenz = PD	107
Quelle = Twisted cubic curve.png , Autor = Claudio Rocchini, Lizenz = CC-BY-SA-3.0	113
Quelle = Whitney umbrella.png , Autor = Claudio Rocchini, Lizenz = CC-BY-SA-2.5	119
Quelle = Tangent.png , Autor = Axel Boldt, Lizenz = GFDL	127
Quelle = 3 equations -5.JPG , Autor = Cronholm144, Lizenz = PD	128
Quelle = Intersect3.png , Autor = Michael Larsen, Lizenz = GFDL	129
Quelle = Frans Hals - Portret van René Descartes.jpg , Autor = Frans Hals (= Benutzer Dedden auf Commons), Lizenz = PD	130
Quelle = Folium of decartes.png , Autor = KENPEI, Lizenz = GFDL	130
Quelle = Intersect3.png , Autor = Michael Larsen (= Benutzer Maksim auf Commons), Lizenz = GFDL	147
Quelle = Loewenzahn 20.jpg , Autor = Waugsberg, Lizenz = CC-BY-SA-2.5	150

Quelle = Projektiveline1bb.jpg, Autor = Darapti, Lizenz = CC-BY-SA-3.0	151
Quelle = Projektiveline2bb.jpg, Autor = Darapti, Lizenz = CC-BY-SA-3.0	151
Quelle = Projektiveline3bb.jpg, Autor = Darapti, Lizenz = CC-BY-SA-3.0	151
Quelle = Projektiveplane1bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0	152
Quelle = Projektiveplane2bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0	152
Quelle = Projektiveplane3bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0	152
Quelle = Projektiveplane4bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0	152
Quelle = Perspective Projection Principle.jpg , Autor = Benutzer Fantagu auf Commons, Lizenz = GFDL	153
Quelle = Blue-sphere.png, Autor = Benutzer Kieff auf Commons, Lizenz = PD	156
Quelle = Soccerball.svg , Autor = Benutzer Ranveig auf Commons, Lizenz = PD	162
Quelle = Torus illustration.png , Autor = Oleg Alexandrov, Lizenz = PD	162
Quelle = Double torus illustration.png , Autor = Oleg Alexandrov, Lizenz = PD	162
Quelle = Sphere with three handles.png , Autor = Oleg Alexandrov, Lizenz = PB	162
Quelle = Two cubic curves.png , Autor = Hack, Lizenz = PD	170

ANHANG 2: GFDL-LIZENZ

GNU Free Documentation License Version 1.2,

November 2002 Copyright (C) 2000,2001,2002Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others. This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software. We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law. A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language. A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal,

commercial, philosophical, ethical or political position regarding them. The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none. The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words. A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straight forwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text for matters or for automatic translation to a variety of formats suitable for input to text for matters. A copy made in anotherwise Transparent file format whose mark up, or absence of mark up, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque". Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only. The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text. A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition. The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in

this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this

License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3. You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects. If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages. If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public. It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to who ever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document. E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be replaced in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of thesection, and preserve in the section all the substance and tone of each the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such as section may not be included in the Modified Version.

N. Do not retile any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles. You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard. You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one. The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers. The combined work need only contain one copy of this License, and multiple identical Invariant Sections maybe replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher

of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work. In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects. You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document. If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version

will prevail. If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>. Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOURNAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation. If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.