Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

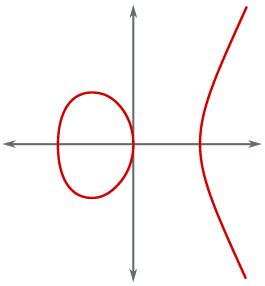
Elliptische Kurven

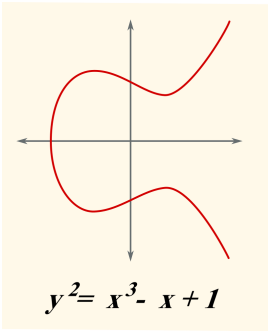
Vorlesung 1

Elliptische Kurven

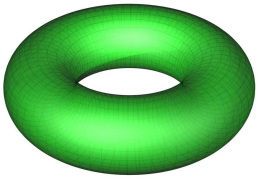
Dies ist eine Ellipse und auch eine Kurve. Es ist aber keine elliptische Kurve.

Dagegen zeigen die folgenden Bilder (reelle affine Ausschnitte) elliptische Kurven.





Ebenso zeigt das folgende Bild eine elliptsche Kurve. Gemeint ist die Oberfläche des Torus (Reifens), die ja dem Anschein nach eher eine Fläche und weniger eine Kurve ist.



Auch einzelne Punkte können eine geeignete Visualisierung einer elliptischen Kurve sein.

Nun sind Bilder nicht unmittelbar hilfreich, sondern eine Illustration eines mathematischen Sachverhaltes. Aber auch der eigentliche mathematische Sachverhalt, der sich hinter einer elliptischen Kurve verbirgt, ist vielfältig, was sich schon darin zeigt, dass es ziemlich viele verschiedene Definitionen für eine elliptische Kurve gibt.

Elliptische Kurven bilden ein herausragendes Objekt an der Schnittstelle von algebraischer Geometrie, komplexer Analysis, Zahlentheorie. Diese Reichhaltigkeit zeigt sich auch in den vielfältigen Möglichkeiten, eine elliptische Kurve zu definieren. Diese Definitionen nehmen Bezug auf recht unterschiedliche geometrische, algebraische, gruppentheoretische, topologische, arithmetische Eigenschaften, und das Studium der elliptischen Kurven ist durch ein intensives Wechselspiel zwischen diesen Konzepten gekennzeichnet. Einige Definitionsmöglichkeiten sind

(1) Eine kubische glatte projektive Kurve.
(2) Eine projektive Kurve mit einer Gruppenstruktur.
(3) Eine glatte projektive Kurve vom Geschlecht 1.

Dabei gibt es mehrere Möglichkeiten, das Geschlecht zu definieren: Als Dimension der globalen Differentialformen, als Dimension der ersten Kohomologie der Strukturgarbe, über topologische Eigenschaften.

Über den komplexen Zahlen ergeben sich weitere Definitionsmöglichkeiten.

(1) Eine eindimensionale kompakte komplexe Lie-Gruppe.
(2) Ein reell zweidimensionaler Torus mit einer komplexen Struktur.
(3) Die komplexen Zahlen $\mathbb{C}$ modulo einem Gitter $\Gamma \cong \mathbb{Z}^2 \subset \mathbb{C}$.
(4) Eine kompakte Riemannsche Fläche mit trivialem Tangentialbündel.
(5) Eine kompakte Riemannsche Fläche mit topologischem Geschlecht 1.
(6) Eine kompakte Riemannsche Fläche mit Fundamentalgruppe $\mathbb{Z}^2$.

Innerhalb der glatten projektiven Kurven nehmen die elliptischen Kurven eine mittlere Position ein. Die projektive Gerade ist als einfachste Kurve auf der einen Seite und die Kurven von einem Geschlecht ≥ 2 sind auf der anderen Seite. Diese Mittelstellung bestätigt sich, wenn man Eigenschaften des

Tangentialbündels oder Krümmungseigenschaften betrachtet. In einem gewissen Sinn spiegelt sich diese mittlere Stellung auch im Schwierigkeitsgrad nieder. Es gibt viele Fragen, die für die projektive Gerade trivial sind, die man für elliptische Kurven mit einigem Aufwand versteht, und die man für andere Kurven nicht zu fragen wagt bzw. die dafür erst Jahrzehnte später beantwortet werden können. Da man aber eben für elliptische Kurven sich Fragen zu stellen wagt, vor denen man sonst zurückweicht (oder gar nicht weiß, wie die Frage zu formulieren wäre), ist das Studium der elliptischen Kurven wiederum beliebig schwierig. Dies gilt insbesondere für arithmetisch angehauchte Probleme. Es hat sich nämlich herausgestellt, dass man Probleme aus der Zahlentheorie in Fragen über elliptische Kurven übersetzen und damit lösen kann. Das prominenteste Beispiel ist die Lösung des großen Fermat über die Modularitätseigenschaft von elliptischen Kurven über $\mathbb{Q}$ durch Andrew Wiles. Eine weiteres Problem, das eng mit elliptischen Kurven verbunden ist, ist das Problem der kongruenten Zahlen. Dieser enge Zusammenhang mit der Zahlentheorie hat sich auch darin niedergeschlagen, dass die Vermutung von Birch und Swinnerton-Dyer über den Rang von elliptischen Kurven in die Liste der sogenannten (sieben) Milleniums-Probleme aufgenommen wurde.

Polynomringe

Wir nähern uns zunächst den elliptischen Kurven im Rahmen der algebraischen Geometrie an, also als Lösungsmenge zu gewissen polynomialen Gleichungen. Wir beschränken uns zunächst auf die affine Situation, obwohl eine elliptische Kurve eine projektive Kurve. Wir erinnern an Polynomringe.

Definition 1.1. Der *Polynomring* über einem kommutativen Ring R besteht aus allen *Polynomen*

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

mit $a_i \in R$, $i = 0, \ldots, n$ $n \in \mathbb{N}$, 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

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

etc. Ein Polynom in n Variablen hat die Gestalt

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

Es wird dabei summiert über eine endliche Familie von *Exponententupel* $(\nu_1, \ldots, \nu_n)$. 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.

Affine Nullstellengebilde

In der algebraischen Geometrie fixiert man einen *Grundkörper* K. Wichtige Körper sind für uns die rationalen Zahlen $\mathbb{Q}$, weitere Zahlkörper, die reellen Zahlen $\mathbb{R}$ (insbesondere sind die Bilder meistens so zu verstehen!) oder die komplexen Zahlen $\mathbb{C}$, ferner die endlichen Körper.

Definition 1.2. Es 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

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

D.h. es ist

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

Es handelt sich also um gewisse, durch ein Polynom festgelegte Teilmengen des K^2, den man in diesem Zusammenhang auch die affine Ebene nennt und mit $\mathbb{A}^2_K$ bezeichnet. Das Polynom selbst definiert durch Einsetzen eine Abbildung $F\colon\ K^2 \to K$ und die Kurve ist das Urbild über dem Nullpunkt.

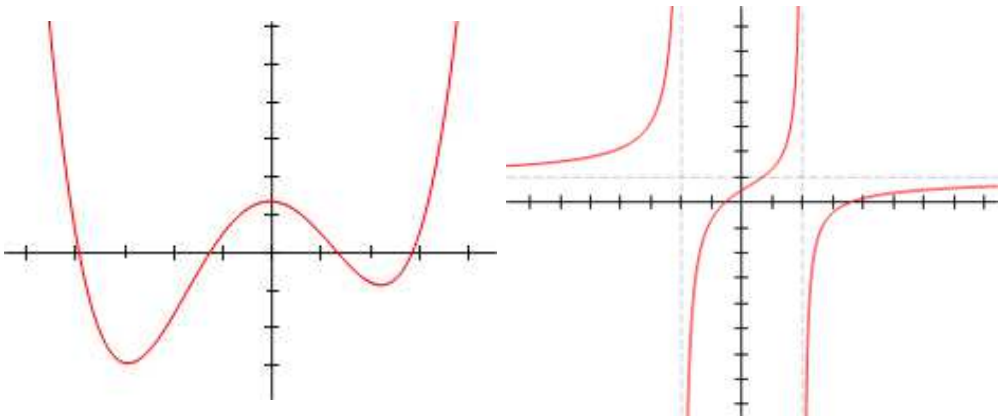
Betrachten wir einige vergleichsweise einfach gebaute Polynome F in zwei Variablen und versuchen das zugehörige Nullstellenmenge zu verstehen.

Wenn F die Form $Y - P(X)$ mit einem Polynom P in der einen Variablen X besitzt, so ist das zugehörige Nullstellengebilde einfach der Graph dieses Polynoms. Für einen Punkt $(x,y) \in K^2$ ist ja $F(x,y) = 0$ genau dann, wenn

$$y = P(x)$$

ist, und dies charakterisiert die Zugehörigkeit zum Graphen. Ein solcher Graph ist insofern ein einfaches Gebilde, dass es zu jedem Wert für X genau einen Wert für Y (nämlich den Funktionswert) gibt, und den man auch noch

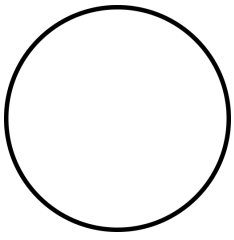
einfach ausrechnen kann, wenn man im gegebenen Körper rechnen kann. Der Graph ist in gewissem Sinne eine „gebogene“ Kopie der Grundlinie, der X-Achse.



Eine rationale Funktion in X ist von der Form $\frac{P(X)}{Q(X)}$ mit zwei Polynomen P, Q in einer Variablen X, wobei der Ausdruck nur dort einen Sinn ergibt, wo der Nenner nicht 0 ist, an den Nullstellen des Nennerpolynoms ist die rationale Funktion nicht definiert.Wenn der Nenner 0 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 Undefinierbarkeitsstellen keine optimale Beschreibung für die Kurve. Wenn man sie hingegen mit dem Nennerpolynom multipliziert, so erhält man die Bedingung

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

in der links und rechts wohldefinierte Polynome stehen. Der Graph ist dann die Nullstellenmenge des Polynoms $F = YQ(X) - P(X)$. In den bisherigen Beispielen kam die Variable Y nur in ihrer esten Potenz vor, wobei X beliebig kompliziert darin vorkam.



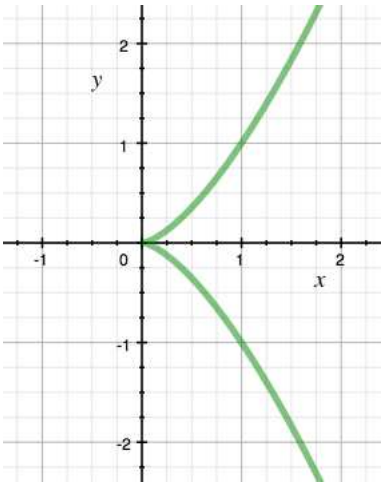
Betrachten wir einen *Kreis*, seine Gleichung ist $C = \{(x, y) \mid x^2 + y^2 = r^2\}$, wobei r den Radius des Kreises bezeichnet. Eine Kreisgleichung kann man als eine Gleichung der Form

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

auffassen, 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 $G(X)$ auch 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 $(x, \pm\sqrt{G(x)})$ (falls der Radikand nichtnegativ ist) einen Punkt. Im Komplexen sind nur die Fälle $G(x) = 0$ oder $G(x) \neq 0$ zu unterscheiden.



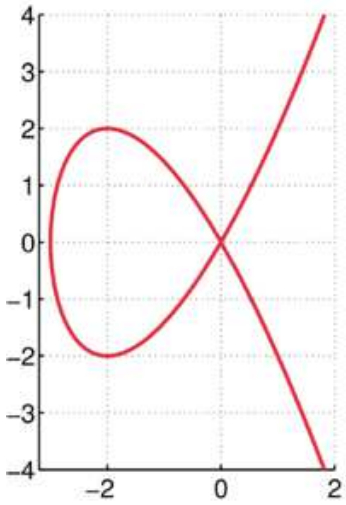
Mit dem Fall, dass $G(X)$ ein kubisches (reelles) Polynom ist (also den Grad drei besitzt), hat sich bereits Isaac Newton intensiv beschäftigt. Dieses Beispielmaterial ist schon sehr reichhaltig und insbesondere in Hinblick auf elliptische Kurven relevant.

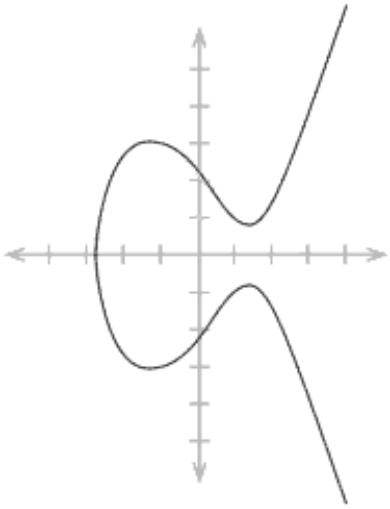
Betrachten wir den Fall $G(X) = X^3$, also das durch

$$\left\{(x, y) \mid y^2 = x^3\right\}$$

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).

Auch der Fall $G(X) = X^3 + 3X^2$ besitzt einen eigenen Namen, man spricht von der *Tschirnhausen Kubik*. Die gezeigte Singularität nennt man einen *Kreuzungspunkt* oder einen *Doppelpunkt*. In den beiden Beispielen mit Singularität besitzt das Polynom $G(X)$ eine zumindest doppelte Nullstelle (im Fall der Kuspe sogar eine dreifache).

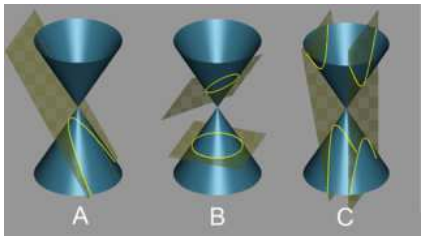




Es sei nun $G(X)$ ein Polynom vom Grad 3 ohne mehrfache Nullstelle. Das Nullstellengebilde zu $Y^2 = G(X)$ besitzt dann keine Singularität, siehe Lemma 2.6. Es handelt sich um einen affinen Ausschnitt einer elliptischen Kurve.

Auch wenn wir uns wie in diesem Kurs hauptsächlich für ebene Kurven interessieren, ist es für viele Begrifflichkeiten sinnvoll, beliebige durch Polynome gegebene Nullstellengebilde zu betrachten, nicht nur die Nullstellenmenge zu einem Polynom in zwei Variablen. Schon die Nullstellenmenge eines Polynoms in einer Variablen reflektiert wichtige Eigenschaften des Körpers, man kann sich für den Durchschnitt von zwei algebraischen Kurven in der Ebene interessieren, eine Kurve kann als Raumkurve gegeben sein und man interessiert sich für die Projektionen auf eine Ebene, Kegelschnitte sind gegeben als

Durchschnitte von einem Kegel mit verschiedenen Ebenen im Raum, über einer projektiven Kurve liegt der zweidimensionale affine Kegel, etc. Dies führt zu den folgenden Begriffen.



Kegelschnitte

DEFINITION 1.3. Es sei K ein Körper und sei $F_j \in K[X_1, \ldots, X_n]$, $j \in J$, eine Familie von Polynomen in n Variablen. Dann nennt man

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

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

DEFINITION 1.4. Es sei K ein Körper und sei $K[X_1, \ldots, X_n]$ 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 $F_j \in K[X_1, \ldots, X_n]$ ist, wenn also $V = V(F_j, j \in J)$ gilt.

Algebraisches oder polynomiales Nullstellengebilde und (affin)-algebraische Menge bzw. (affine) *Varietät* sind im Wesentlichen austauschbare Begriffe, wobei bei Varietät oft irreduzibel gefordert wird. In diesen Definitionen sind sogar unendliche Polynomfamilien erlaubt, aus dem Hilbertschen Basissatz folgt aber, dass es stets auch eine endliche Polynomfamilie gibt, mit der die Varietät beschrieben werden kann. Der beliebige Durchschnitt und eine endliche Vereinigung von affin-algebraischen Mengen ist wieder affin-algebraisch,

Eine erste einfache Eigenschaft einer algebraischen Kurve betrifft das Schnittverhalten mit Geraden. Die Argumentation ist typisch für das Wechselspiel zwischen geometrischen und algebraischen Gesichtspunkten in der algebraischen Geometrie.

LEMMA 1.5. *Es 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 sowohl $F(P) = 0$ als auch

die Geradengleichung erfüllen. 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 nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) nur endlich viele Nullstellen. □

Körperwechsel

Betrachten wir die durch das Polynom

$$F = X^2 + Y^2 + 1$$

gegebene Nullstellengebilde im $\mathbb{R}^2$. Dieses ist offenbar leer, da ja für $(x, y) \in \mathbb{R}^2$ wegen der Nichtnegativität der Quadrate direkt $F(x, y) \geq 1 > 0$ gilt. Wenn man hingegen das gleiche Polynom über $\mathbb{C}$ auffasst und nach Lösungen in $\mathbb{C}^2$ sucht, so ergibt sich eine Vielzahl an Nullstellen. Oder betrachten wir das Polynom

$$G = X^2Y + XY^2 + 1$$

über dem Körper $\mathbb{Z}/(2)$ mit zwei Elementen. Für jedes Punktepaar $(x, y) \in \mathbb{Z}/(2) \times \mathbb{Z}/(2)$ besitzt dieses Polynom den Wert 1 und besitzt keine Nullstelle. Wenn man aber zu dem Körper mit vier Elementen übergeht, also die endliche Körpererweiterung

$$\mathbb{Z}/(2) \subseteq \mathbb{F}_4 = \mathbb{Z}/(2)[T]/(T^2 + T + 1)$$

durchführt, so findet man dort beispielsweise die Lösung $(1, t)$, wobei t die Restklasse von T bezeichnet.

In der algebraischen Geometrie stellt man die Polynome bzw. die zugehörigen Gleichungen in den Mittelpunkt. Dazu braucht man zunächst einen Grundkörper K, über dem die Polynome definiert sind. Die zugehörige Nullstellenmenge betrachtet man aber nicht nur in K^2, sondern allgemeiner in L^2, wobei $K \subseteq L$ eine (nicht notwendigerweise endliche) Körpererweiterung bezeichnet. Wesentliche Eigenschaften der Polynome werden erst dann sichtbar, wenn man das Lösungsverhalten zu verschiedenen Körpererweiterungen untersucht. Dabei spielt der algebraische Abschluss des Körpers eine besondere Rolle (siehe unten). Es ist aber auch wichtig, sich zu fragen, welche Lösungen es über einem gegebenen Körper gibt. Der reelle Kreis $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ ist ein geometrisch sehr einfaches Objekt. Dagegen ist der rationale Kreis $\{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\}$, das durch die gleiche Gleichung definiert wird, ein zahlentheoretisch recht subtiles Objekt, das eng mit pythagoreischen Tripeln zusammenhängt.

Wenn $V = V(\mathfrak{a}) \subseteq \mathbb{A}^n_K$ die affin-algebraische Menge zum Ideal $\mathfrak{a}$ ist, so bezeichnen wir die entsprechende Menge über L zu einer Körpererweiterung

$K \subseteq L$ mit V_L, also

$$V_L = \{P \in \mathbb{A}_L^n \mid F(P) = 0 \text{ für alle } F \in \mathfrak{a}\},$$

wobei das Ideal $\mathfrak{a}$ (als Erweiterungsideal) bzw. ein Erzeugendensystem davon in $L[X_1, \ldots, X_n]$ aufzufassen ist. Für diese Bezeichnung ist es entscheidend, dass man bei $V(\mathfrak{a})$ nicht nur die (rein mengentheoretische) Nullstellenmenge, sondern auch das definierende Ideal als Teil der Information betrachtet. Ein Extremfall ist, wenn zwei verschiedene Ideale $\mathfrak{a}$ und $\mathfrak{b}$ beide eine leere Nullstellenmenge haben, da sind im Allgemeinen $V(\mathfrak{a})_L$ und $V(\mathfrak{b})_L$ auch als Punktmenge verschieden. Die Notation $\mathbb{A}_K^n, \mathbb{A}_L^n$ orientiert sich auch an dieser Bezeichnungsphilosophie. Einen Punkt $P \in V_L$ nennt man auch einen *L-Punkt* oder einen *L-rationalen Punkt* von V.

Zu einem Ideal $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ nennt man den Restklassenring $K[X_1, \ldots, X_n]/\mathfrak{a}$ auch den *Koordinatenring* der affinen Varietät $V = V(\mathfrak{a})$. Der Koordinantering von V_L ist dann $L[X_1, \ldots, X_n]/\mathfrak{a}L[X_1, \ldots, X_n]$. Da die Elemente des Ideals auf $V(\mathfrak{a})$ zur Nullfunktion werden, beinhaltet der Koordinatenring die auf V definierten polynomialen Funktionen. Speziell ist der Ring $K[X, Y]/(F)$ der Koordinatenring auf der algebraischen Kurve $V(F)$.

Das eben erwähnte Problem, dass die Existenz von Nullstellen zu Polynomen vom Körper abhängt, ist bereits in einer Variablen präsent, und bildet den Ausgangspunkt für folgende Definition.

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

Carl Friedrich Gauss (1777-1855)

Der sogenannte *Fundamentalsatz der Algebra* wurde erstmals von Gauss bewiesen.

SATZ 1.7. *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.

□

DEFINITION 1.8. Es sei K ein Körper. Eine Körpererweiterung $K \subseteq L$ heißt *algebraischer Abschluss* von K, wenn die Erweiterung algebraisch und L algebraisch abgeschlossen ist.

Die komplexen Zahlen $\mathbb{C}$ sind der algebraische Abschluss von $\mathbb{R}$. Jeder Körper besitzt einen (bis auf Isomorphie) eindeutig bestimmten algebraischen Abschluss.

Wir werden die Begriffe (glatt, zusammenhängend, irreduzibel) zumeist so aufbauen, dass sie für alle Körpererweiterungen gelten.

Abbildungsverzeichnis

Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von http://commons.wikimedia.org) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren