Diplomarbeit

Matthias Schiechtl

25. März 2008

Kardinalität und Konfiguration nulldimensionaler algebraischer Varietäten

Diplomarbeit
in der Studienrichtung Technische Mathematik

zur Erlangung des akademischen Grades
Diplom-Ingenieur

eingereicht an der **Fakultät für Mathematik, Informatik und Physik der Universität Innsbruck**

von
Matthias Schiechtl

Betreuer der Diplomarbeit: Prof.Dr.Herwig Hauser

Innsbruck, am

Inhaltsverzeichnis

0.1 Kurventheorie 3
0.1.1 Schnitt von Kurve mit Gerade 3
0.1.2 Schnitt zweier Kurven und Satz von Bézout 7
0.1.3 Anwendungen des Satzes von Bézout 12
0.1.4 Der Satz von Cayley-Bacharach 17
0.2 Reelle Nullstellen von Polynomen 21
0.2.1 Obere Schranken 21
0.2.2 Zählverfahren 24
0.3 Sperner-Lemma 33
0.4 Schubert-Kalkül 36

Einleitung

Wieviele Geraden gibt es im dreidimensionalen Raum, die durch vier gegebene Geraden gehen? Dabei sollen die vier Geraden keine solche Lage einnehmen, sodass die Anzahl der gesuchten Geraden unendlich wird. Mit Fragen dieser Art befasst sich das *Schubert-Kalkül* im fünften Kapitel dieser Diplomarbeit. Das Faszinierende an jenem Kalkül der abzählenden Geometrie ist, dass die Anzahl von geometrischen Objekten mit gewissen Bedingungen rein algebraisch ermittelt werden kann.
In dieser Diplomarbeit werden prinzipiell wichtige Sätze und deren Anwendungen in Bezug auf Anzahl und Lage von algebraischen Varietäten erörtert. Dabei sind algebraische Varietäten geometrische Objekte, die durch polynomiale Gleichungen beschrieben werden können. Im ersten Kapitel wird der *Satz von Bézout* als entscheidendes Instrument zur Bestimmung der Anzahl von Schnittpunkten zweier ebener Kurven bzw. Anzahl der Lösungen zweier Polynome über einem algebraisch abgeschlossenen Körper hergeleitet. Wir werden einige Anwendungen davon kennenlernen. Mit Hilfe des Satzes von Bézout kann man beispielsweise zeigen, dass die Anzahl von singulären Punkten einer ebenen Kurve endlich ist und einer irreduziblen ebenen Kurve vom Grad m durch $\frac{(m-1)(m-2)}{2}$ beschränkt ist. Am Ende des ersten Kapitels wird der *Satz von Cayley-Bacharach* vorgestellt. Dieser besagt speziell, dass wenn sich zwei Kubiken in neun verschiedenen Punkten schneiden und eine weitere Kubik durch acht dieser neun Schnittpunkte geht, diese ebenso durch den neunten Schnittpunkt gehen muss. Genau jener Spezialfall des Satzes von Cayley-Bacharach liefert neben dem Satz von Bézout einen Alternativbeweis des Satzes von Pascal, eines Satzes über die Lage von Schnittpunkten bezüglich ein in eine irreduzible Quadrik eingeschriebenes Hexagon. Außerdem dient er im zweiten Kapitel dazu, die Assoziativität der Gruppenverknüpfung bezüglich den elliptischen Kurven als Gruppe elegant zu beweisen. Wir werden erkennen, dass sich elliptische Kurven durch elliptische Funktionen parametrisieren lassen, deren Eigenschaften und Struktur ein wesentlicher Bestandteil des zweiten Kapitels sind.
Unter welchen Bedingungen an die Koeffizienten $a, b, c \in \mathbb{R}$ besitzt das Polynom $x^3 + ax^2 + bx + c$ eine bzw. drei reelle Nullstellen? Aufschluss darüber gibt das dritte Kapitel, das zwei Zählverfahren zur Bestimmung der Anzahl von reellen Nullstellen eines Polynoms in einer Variablen über einem reell abgeschlossenen Körper behandelt.
Der *Satz von Bernstei*n gibt an, wieviel Nullstellen n Polynome in n Variablen über $\mathbb{C}^n$ besitzen, sofern die Koeffizienten des Gleichungssystems genügend allgemein sind. Im vierten Kapitel wird ein Gleichungssystem in den Filterkoeffizienten von *Wavelets* durch einen Koordinatenwechsel in ein neues System umgeschrieben.

Anschließend werden wir mit Hilfe des Satzes von Bernstein sehen, dass eine obere Schranke für die Anzahl von Lösungen dieses Gleichungssystems existiert.
Betrachten wir nun ein Dreieck, das beliebig in kleinere Dreiecke trianguliert werde. Wir färben die Eckpunkte mit drei verschiedenen Farben, die Punkte auf der i,j-Seite des Dreiecks jeweils nur mit den Farben i oder j und alle inneren Punkte beliebig. Dann ist nach dem *Sperner-Lemma* die Anzahl der dreifarbigen Dreiecke stets ungerade. Drei Beweise davon sind im sechsten Kapitel angeführt. Der Fixpunktsatz von Brouwer besagt, dass jede stetige Abbildung der n-dimensionalen Vollkugel in die n-dimensionale Vollkugel einen Fixpunkt hat. Wir werden sehen, dass sich mit Hilfe des Sperner-Lemmas dieser Satz elementar beweisen lässt. Zuletzt wird noch ein kurzer Einblick gegeben, wie ebene reelle algebraische Kurven ähnlich wie im dritten Beweis des Sperner-Lemmas mittels geschlossener Pfade durch triangulierte Dreiecke konstruiert werden können.
Abschließend möchte ich meinem Betreuer Herwig Hauser für seine große Unterstützung bei der Abfassung meiner Diplomarbeit danken.
Innsbruck, März 2008
Matthias Schiechtl

Kapitel 1

Kurventheorie

1.1 Schnitt von Kurve mit Gerade

Seien $f \in \mathbb{C}[x_1, x_2]$ ein Polynom vom Grad n, geschrieben $\deg(f) = n$, und $C = V(f) := \{(x_1, x_2) \in \mathbb{C}^2 | f(x_1, x_2) = 0\}$ die dazugehörige affin-algebraische Kurve. Man nennt das Polynom $F := x_0^n \cdot f(\frac{x_1}{x_0}, \frac{x_2}{x_0}) \in \mathbb{C}[x_0, x_1, x_2]$ die Homogenisierung von f und $\overline{C} := V(F) \subset \mathbb{P}_2(\mathbb{C})$ den projektiven Abschluss von C. Weiters ist eine ebene komplexe und projektiv-algebraische Kurve die Nullstellenmenge $V(F)$ eines nichtkonstanten homogenen Polynoms $F \in \mathbb{C}[x_0, x_1, x_2]$ in der projektiven Ebene $\mathbb{P}_2(\mathbb{C})$. Jede ebene Kurve lässt sich somit durch die Gleichung $F(x_0, x_1, x_2) = 0$ für ein bis auf einen konstanten Faktor eindeutig bestimmtes homogenes Polynom F beschreiben. Diese Definition dient der Vervollständigung von Kurven, also der Hinzunahme von unendlich fernen Punkten. Unter topologischer Betrachtungsweise sind die Kurven als abgeschlossene Teilmengen der projektiven Ebene $\mathbb{P}_2(\mathbb{C})$ kompakt. Wir betrachten im Folgenden stets ebene komplexe und projektiv-algebraische Kurven C_i und nennen sie *ebene* Kurven.

Definition. Eine ebene Kurve $C = V(F)$ heißt *reduzibel*, wenn sie die Vereinigung von zwei verschiedenen ebenen Kurven ist. Andernfalls heißt sie irreduzibel. Ferner entspricht der Grad von C, geschrieben $\deg(C)$, dem Grad des definierenden Polynoms F.

Neben dieser mengentheoretischen Betrachtungsweise lassen sich ebene Kurven auch vom algebraischen Standpunkt analysieren. Allgemein können wir eine reduzible Kurve C formal als Linearkombination ihrer irreduziblen Komponenten C_i schreiben:

$$C = n_1 C_1 + \ldots + n_r C_r.$$

Dabei sind die Faktoren $n_i \geq 0$ die Vielfachheiten der Komponenten. Diese formale Linearkombination trägt die Bezeichnung „effektiver Divisor“. Ist $C_i = V(F_i)$, so lautet die Gleichung für C

$$F_1^{n_1} \cdot \ldots \cdot F_r^{n_r} = 0.$$

Wir bezeichnen das Polynom $F_1 \cdot \ldots \cdot F_r$ als das *reduzierte Polynom* der Kurve C. Dieses ist quadratfrei, d.h. jeder Faktor tritt genau einmal auf und die Faktoren

sind paarweise verschieden.

Sei nun $C = V(F)$ eine ebene Kurve vom Grad m und L die Gerade mit der Gleichung $x_2 = 0$, die keine Komponente von C sei. Da x_2 das Polynom F nicht teilt, ist $F(x_0, x_1, 0)$ ein nicht-verschwindendes homogenes Polynom vom gleichen Grad m und besitzt somit nach dem Fundamentalsatz der Algebra (siehe Satz **??**) genau m mit Vielfachheit gezählte Nullstellen. Also schneiden sich C und L in höchstens m verschiedenen Schnittpunkten.

Beispiel 1.1. Seien $C = V(x_0x_2^2 - x_1^3)$ der projektive Abschluss der Neil'schen Parabel und die Gerade L sei parametrisiert durch $(t_0, t_1) \mapsto (t_0, \lambda_0 t_1, \lambda_1 t_1)$ für $\lambda_1, \lambda_2 \in \mathbb{C}$ und sei $p = (1, 0, 0) \in L$. Als Schnitt von C mit L ergibt sich die Gleichung

$$F(t_0, \lambda_0 t_1, \lambda_1 t_1) = t_1^2(\lambda_1^2 t_0 - \lambda_0^3 t_1).$$

Der erste Faktor t_1^2 beschreibt den Schnittpunkt p, der zweite Faktor einen weiteren Schnittpunkt $q = (\lambda_0^3, \lambda_0\lambda_1^2, \lambda_1^3)$. Es ergeben sich somit zwei Schnittpunkte von $C \cap L$, die zusammenfallen, falls die Gerade L waagrecht verläuft, d.h. $\lambda_0 = 1$ und $\lambda_1 = 0$.

Definition. Seien $f = a_0x^m + ... + a_m$ und $g = b_0x^n + ... + b_n$ mit $a_0 \neq 0 \neq b_0$ Polynome in einer Variablen über $\mathbb{C}$. Dann heißt

$$\mathrm{Res}_{f,g} := \det \begin{pmatrix} a_0 & \cdots & a_m & & \\ & \ddots & & \ddots & \\ & & a_0 & \cdots & a_m \\ b_0 & \cdots & b_n & & \\ & \ddots & & \ddots & \\ & & b_0 & \cdots & b_n \end{pmatrix}$$

die *Resultante* von f und g und $\mathrm{Res}_{f,f'}$ die *Diskriminante* von f.

Die Resultante ist ein homogenes Polynom in den Koeffizienten der Polynome f und g vom Grad $\deg(f) \cdot \deg(g)$. Außerdem besitzen zwei Kurven genau dann eine gemeinsame Komponente, wenn die Resultante der beiden definierenden Polynome verschwindet. Für den Beweis sei auf [1], p.176 verwiesen.

Der nachfolgende Satz liefert eine obere Schranke für die Anzahl von Geraden, die nicht in einer ebenen Kurve C enthalten sind und diese in weniger als $\deg(C)$ verschiedenen Punkten schneiden.

Satz 1. *Sei C eine ebene Kurve vom Grad m und sei p ein Punkt im Komplement von C. Dann schneidet eine Gerade L durch p die Kurve C in genau m verschiedenen Punkten mit Ausnahme von höchstens $m(m-1)$ Geraden, welche C in weniger als m verschiedenen Punkten schneiden.*

Beweis: Es lässt sich ein geeignetes Koordinatensystem wählen, sodass $p = (0, 0, 1)$. Sei $V(F)$ die Gleichung von C und g die projektive Gerade mit der Gleichung $x_2 = 0$. Wir bezeichnen die Gerade durch λ und p mit L_λ. Dann erhalten wir eine Bijektion zwischen der Familie aller Geraden durch p und deren Schnittpunkte auf

g. Denn jede Gerade L_λ hat einen eindeutigen Schnittpunkt $\lambda = (\lambda_0, \lambda_1, 0)$ mit g. Offensichtlich gilt

$$L_\lambda \setminus \{p\} = \{(\lambda_0, \lambda_1, t) \in \mathbb{P}_2(\mathbb{C}) |\ t \in \mathbb{C}\}.$$

Damit sind die Schnitte von L_λ mit C durch die Gleichung $F(\lambda_0, \lambda_1, t) = 0$ in t gegeben. Weil L_λ keine Komponente von C ist, verschwindet das Polynom $F(\lambda_0, \lambda_1, t)$ nicht identisch. Wegen $p \notin C$ hat es zudem Grad m. L_λ schneidet C genau dann in weniger als m verschiedenen Punkten, wenn $F(\lambda_0, \lambda_1, t)$ eine mehrfache Nullstelle besitzt, d.h., wenn die Diskriminante $\mathrm{Res}_{\mathrm{F}(\lambda_0,\lambda_1,\mathrm{t}),\frac{\partial \mathrm{F}}{\partial \mathrm{t}}(\lambda_0,\lambda_1,\mathrm{t})}$ verschwindet. Letztere ist ein homogenes Polynom in λ_0, λ_1 vom Grad $m(m-1)$, welches höchstens $m(m-1)$ Nullstellen besitzt. □

Als Beispiele zur Verifizierung hierfür seien die drei Kegelschnitte Ellipse, Hyperbel und Parabel erwähnt.

Definition. Sei $C \subset \mathbb{C}^2$ eine affine algebraische Kurve und $f \in \mathbb{C}[x_1, x_2]$ das quadratfreie Polynom von C. Dann heißt C *glatt* oder *regulär* in einem Punkt $p \in C$, wenn der Gradient von f in p nicht verschwindet, d.h.,

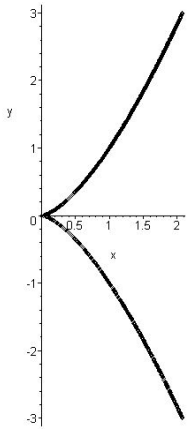
$$\mathrm{grad}_p f = \left(\tfrac{\partial f}{\partial x_1}(p), \tfrac{\partial f}{\partial x_2}(p)\right) \neq (0, 0).$$

Andernfalls heißt C singulär in p. Ferner wird ihre Singularitätenmenge mit $\mathrm{Sing}(C)$ bezeichnet.

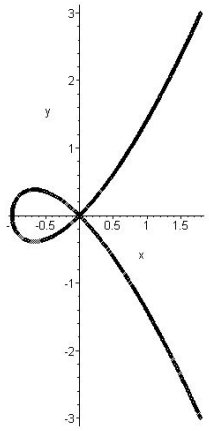
Wäre in der Voraussetzung f nicht quadratfrei, d.h. $f = g^k$ für $k \geq 2$, so wäre

$$\mathrm{grad}_p f = \left(k g^{k-1}(p) \tfrac{\partial g}{\partial x_1}(p), k g^{k-1}(p) \tfrac{\partial f}{\partial x_2}(p)\right).$$

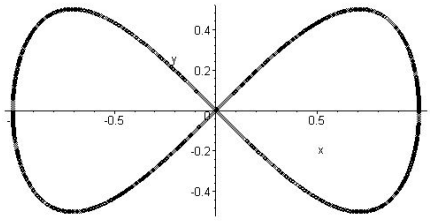
Aber aus $p \in V(f)$ folgt dann, dass $g^{k-1}(p) = 0$ und somit $\mathrm{grad}_p = (0, 0)$, d.h., C wäre in allen Punkten singulär, das einen Widerspruch zu Satz **??** (siehe unten) impliziert.
Die obige Definition lässt sich anhand des Satz über implizite Funktionen im zweidimensionalen Fall erklären. Dieser besagt nämlich, dass für offene Teilmengen $U, V \subset \mathbb{R}$ eine stetig differenzierbare Funktion $f : U \times V \to \mathbb{R}$ in einem Punkt $(u, v) \in U \times V$ mit $f(u, v) = 0$ genau dann in einer Umgebung $U_0 \subset U$ von x_1 bzw. $V_0 \subset V$ von x_2 auflösbar nach x_1 bzw. x_2 ist, wenn $\frac{\partial f(x_1,x_2)}{\partial x_1} \neq 0$ bzw. $\frac{\partial f(x_1,x_2)}{\partial x_2} \neq 0$.
Beispiele für Singularitäten sind in der affinen Ebene der Nullpunkt der Neil'schen Parabel $V(x_1^3 - x_2^2)$, des Newton'schen Knotens $V(x_1^3 + x_1^2 - x_2^2)$, der Lemniskate $V(x_1^2(1 - x_1^2) - x_2^2)$ und des Kardioids $V((x_1^2 + x_2^2 + 4x_2)^2 - 16(x_1^2 + x_2^2))$.



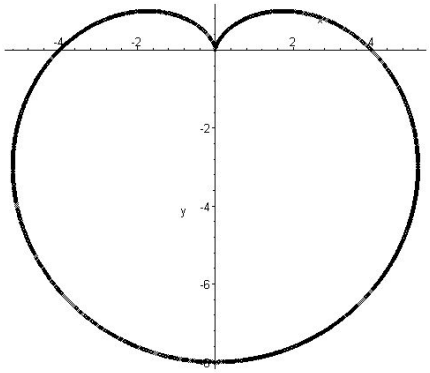
Neil'sche Parabel



Newton'scher Knoten

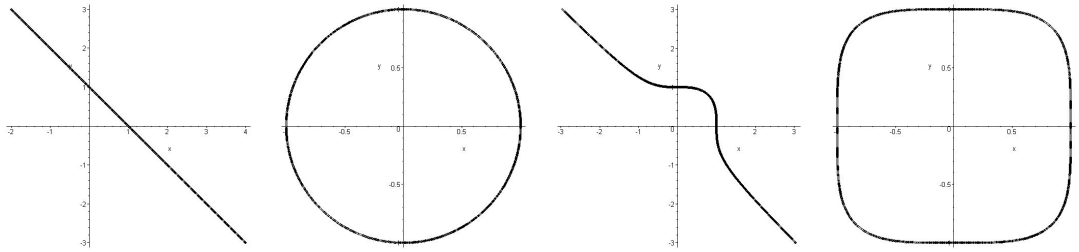


Lemniskate



Kardioid

Die Fermat-Kurven $V(x_0^n - x_1^n - x_2^n) \subset \mathbb{P}_2(\mathbb{C})$ sind für $n \geq 1$ dagegen glatt.



Fermat-Kurven für $n = 1, 2, 3, 4$.

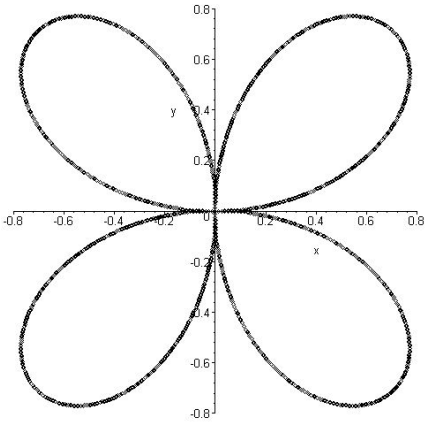
Für eine glatte algebraische Kurve lässt sich die Tangente T_pC an einen Punkt $p \in C$ beschreiben durch $T_pC = \{(x_1, x_2) \in \mathbb{C}^2 : \frac{\partial f}{\partial x_1}(p)x_1 + \frac{\partial f}{\partial x_2}(p)x_2 = c\}$. Dabei ist $c \in \mathbb{C}$ so zu wählen, dass $p \in T_pC$.

Definition. Die *Vielfachheit* $\mu_p(C)$ einer algebraischen Kurve $C = V(f)$ in $p = (a, b) \in C$ ist der Untergrad der Taylorreihe von f in p

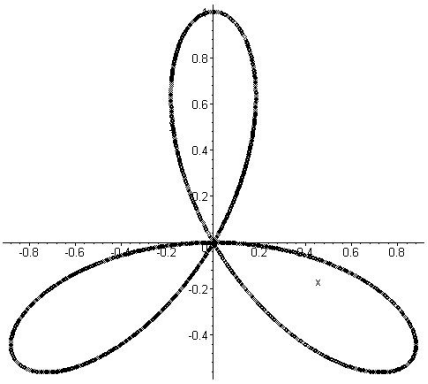
$$f(x_1, x_2) = \sum_{k=0}^{\infty} \frac{1}{k!} \underbrace{\sum_{i=0}^{k} \binom{k}{i} \frac{\partial^k f}{\partial_{x_1}^i \partial_{x_2}^{k-i}}(a, b)(x_1 - a)^i (x_2 - b)^{k-i}}_{\text{homogen vom Grad k}} =: \sum_{k=0}^{\infty} f_k.$$

Wir schreiben $\text{ord}_p(f) := \min \{k \in \mathbb{N} |\ f_k \neq 0\}$.

Sei $f_{\tilde{k}}$ der Term in der Taylorentwicklung von f in p homogen vom Grad $\tilde{k} = \text{ord(f)}$. Die Tangenten der dazugehörigen algebraischen Kurve $C = V(f)$ lassen sich durch die Gleichung $f_{\tilde{k}} = 0$ ermitteln. Die Vielfachheit einer Tangente ist durch die Vielfachheit des jeweiligen die Tangente definierenden Polynoms als Komponente von $f_{\tilde{k}}$ bestimmt. Es gibt somit genau $\mu_p(C)$ mit Vielfachheit gezählte Tangenten in einem Punkt $p \in C$. Die Neil'sche Parabel $V(x_2^3 - x_1^2)$ besitzt etwa im Nullpunkt die x_1-Achse als zweifache Tangente, das vierblättrige Kleeblatt $V((x_1^2+x_2^2)^3-4x_1^2x_2^2)$ die x_1- und x_2-Achse jeweils als zweifache Tangente, während das dreiblättrige Kleeblatt $V((x_1^2 + x_2^2)^2 + 3x_1^2x_2 - x_2^3)$ im Nullpunkt drei einfache Tangenten besitzt, nämlich $V(x_2)$, $V(x_1 - x_2)$ und $V(x_1 + x_2)$.



Vierblättriges Kleeblatt

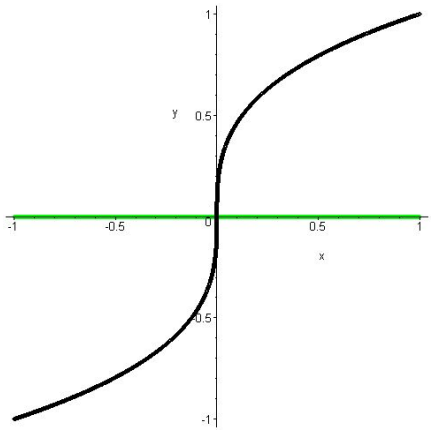


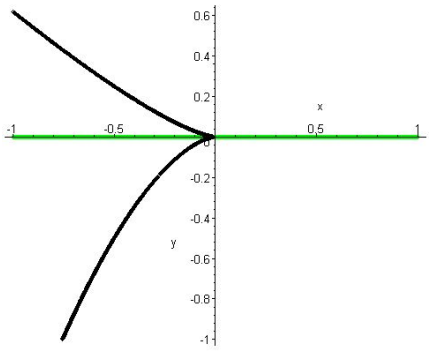
Dreiblättriges Kleeblatt

Die *Schnittmultiplizität* einer Kurve $C = V(f)$ und einer Geraden L in einem Punkt $p \in C \cap L$, geschrieben $\mu_p(C, L)$ lässt sich durch die Dimension des Vektorraumes der formalen Potenzreihen modulo einem Ideal ausdrücken. Sei dazu o.B.d.A. $p = (0, 0)$ und $L = V(x_2)$. Dann gilt per Definition

$\mu_p(C, L) = \text{ord}_{x_1} f(x_1, 0) = \dim_{\mathbb{C}} \mathbb{C}[[x_1, x_2]] / \langle f, x_2 \rangle = \dim_{\mathbb{C}} \mathbb{C}[[x_1, x_2]] / \langle f(x_1, 0), x_2 \rangle$
$= \dim_{\mathbb{C}} \mathbb{C}[[x_1]] / \langle f(x_1, 0) \rangle$.

So ergibt sich beispielweise für $C = V(x_1 - x_2^3)$, $L = V(x_2)$ und $p = (0, 0)$ die Schnittmultiplizität $\mu_p(C, L) = 1$, für $C = V(x_1^2x_2 + x_2^2 + x_1^3)$ dagegen die Schnittmultiplizität $\mu_p(C, L) = 3$, was die beiden nachfolgenden Abbildungen visualisieren.





Nun liegt die Frage nahe, wie wir die Tangenten an eine ebene Kurve durch einen vorgegebenen Punkt in der projektiven Ebene finden.
Sei dazu $C = V(F) \subset \mathbb{P}_2(\mathbb{C})$ eine ebene Kurve mit F als reduziertes Polynom vom Grad $m \geq 2$, $q = (q_0, q_1, q_2) \in \mathbb{P}_2(\mathbb{C})$ und $D_qF := q_0\frac{\partial F}{\partial x_0} + q_1\frac{\partial F}{\partial x_1} + q_2\frac{\partial F}{\partial x_2}$. Der Punkt q liegt genau dann auf der Tangente an einen glatten Punkt $p \in C$, wenn $D_qF(p) = 0$.

Definition. Falls $\deg_{\mathbb{C}}(D_qF) \geq 1$, so heißt $P_qF := V(D_qF)$ die *Polare* von C bezüglich q als Pol.

Die Polare von C bezüglich q ist eine Kurve vom Grad $\leq m - 1$. Schneidet man sie mit C, so erhält man die Berührpunkte von den Tangenten an C durch q. Wir wissen nach Satz 1, dass höchstens $m(m-1)$ Tangenten an C durch q existieren. Dies lässt sich auch mit dem Satz von Bézout (siehe Satz **??** unten) begründen, weil $\deg(D_qF) = m - 1$ gilt.

Es gilt $D_qF = 0$ genau dann, wenn C aus m Geraden durch q besteht. Sei hierfür o.B.d.A. $q = (1, 0, 0)$. Dann ist die Gleichung $D_qF = \frac{\partial F}{\partial x_0} = 0$ äquivalent dazu, dass $F(1, x_1, x_2) = f(x_1, x_2)$ homogen vom Grad m ist. Damit besteht C aus m Geraden durch q.

Ferner liegt jeder singuläre Punkt p von $C = V(F)$ für einen beliebigen Punkt $q \in \mathbb{P}_2(\mathbb{C})$ auf der Polaren von C bezüglich q, weil alle partiellen Ableitungen von F in p verschwinden. Wir fassen die Ergebnisse in folgendem Satz zusammen:

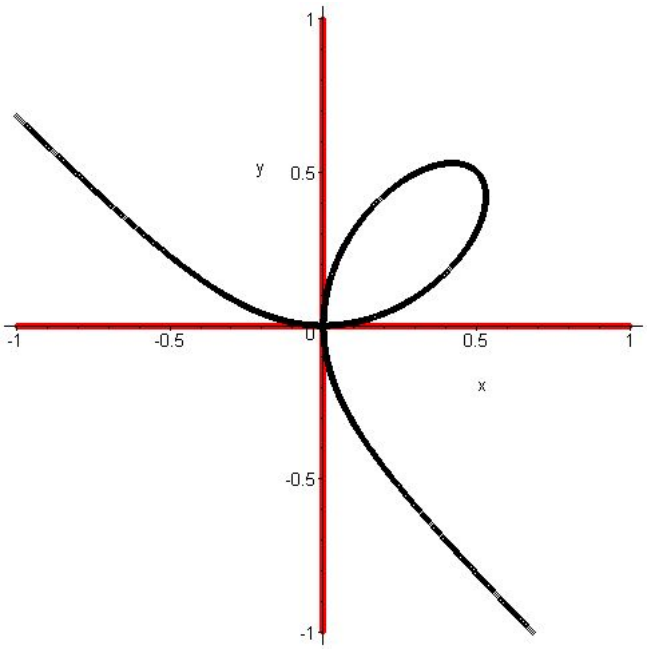
Satz 2. *Sei $C = V(F)$ eine algebraische Kurve vom Grad $m \geq 2$ ohne Gerade als Komponente und $q \in \mathbb{P}_2(\mathbb{C}) \setminus C$. Dann ist die Polare P_qC eine ebene Kurve vom Grad $\leq m - 1$, die mit C keine Komponente gemeinsam hat. Die Schnittmenge $C \cap P_qC$ besteht aus den Berührpunkten von höchstens $m(m-1)$ Tangenten an C durch q und den Singularitäten von C.*

Beispiele. (1) Sei $F = x_1x_2$. Für $q = (1, 0, 0)$ ist die Polare nicht erklärt. Für $q = (\lambda, 1, 0)$ und $\lambda \in \mathbb{C}$ ist $D_qF = x_2$. Die Polare ist somit eine Komponente der Kurve. Dies sind die pathologischen Fälle.

(2) Für eine glatte Quadrik C ist P_qC eine Gerade.

(3) Gegeben sei das Blatt von Descartes C mit dem Minimalpolynom $F = x_1^3 + x_2^3 - 3x_0x_1x_2$. Wir erhalten $\frac{1}{3}D_qF = -q_0x_1x_2 + q_1(x_1^2 - x_0x_2) + q_2(x_2^2 - x_0x_1)$. Die Polare

bezüglich $q = (1, 0, 0)$ ist das Achsenkreuz $x_1x_2 = 0$. Ist $(q_1, q_2) \neq (0, 0)$, so ist P_qC eine glatte Quadrik mit der Tangente $q_2x_1 + q_1x_2 = 0$ im Punkt $p = (1, 0, 0)$ von C.



Blatt von Descartes und seine Polare bezüglich $(0, 0)$

1.2 Schnitt zweier Kurven und Satz von Bézout

Zunächst gilt es, eine obere Schranke für die Anzahl von Schnittpunkten zweier Kurven $C_1 = V(F_1)$ und $C_2 = V(F_2)$ mit $\deg(C_1) = m$ und $\deg(C_2) = n$ in der projektiven Ebene $\mathbb{P}_2(\mathbb{C})$ zu finden. Dabei nehmen wir an, dass C_1 und C_2 keine gemeinsame Komponente besitzen.

Wir wählen nun einen Punkt q im Komplement von C_1 und C_2 und betrachten die Zentralprojektion

$$\Pi : \mathbb{P}_2(\mathbb{C}) \setminus \{q\} \to L$$

mit Zentrum q auf eine nicht durch q gehende Gerade L. Dabei sind die Projektionsgeraden das Geradenbündel durch q. Wir erhalten die Bildpunkte der Zentralprojektion Π, indem wir die Projektionsgeraden mit L schneiden. Zu jedem $c \in L$ bezeichnen wir die entsprechende Projektionsgerade mit L_c. Da eine Gerade die Kurve C_1 vom Grad m nach Satz 1 in höchstens m Punkten schneidet, liegen auf jedem L_c endlich viele Punkte aus $C_1 \cap C_2 \subset C_1$. Um zu beweisen, dass sich C_1 und C_2 nur in endlich vielen Punkten schneiden, genügt es daher zu zeigen, dass nur für endlich viele $c \in L$ die Schnittpunkte von C_1 und C_2 auf L_c liegen.

Wir setzen dazu o.B.d.A. $q = (0, 0, 1)$ und $L := V(x_2)$. Somit ist die Zentralprojektion gegeben durch $\Pi(x_0, x_1, x_2) = (x_0, x_1)$. Wir schreiben die beiden definierenden Polynome von C_1 und C_2 folgendermaßen:

$$F_1 = a_0x_2^m + a_1x_2^{m-1} + \ldots + a_m \text{ und}$$

$$F_2 = b_0 x_2^n + b_1 x_2^{n-1} + \ldots + b_n,$$

wobei $a_i, b_j \in \mathbb{C}[x_0, x_1]$ homogene Polynome vom Grad i bzw. j sind. Insbesondere gilt wegen $q \notin C_1, C_2$, dass $a_0 \neq 0$ und $b_0 \neq 0$. Weil F_1 und F_2 keinen nicht-konstanten gemeinsamen Faktor besitzen, ist die Resultante bezüglich x_2 mit der formalen Bezeichnung $\mathrm{Res}_{F_1,F_2}(x_0, x_1)$ ein nicht-verschwindendes homogenes Polynom vom Grad $m \cdot n$. Für $p = (c_0, c_1, c_2) \in C_1 \cap C_2$ ist c_2 eine Lösung der beiden Gleichungen

$$a_0(c_0, c_1)x_2^m + \ldots + a_m(c_0, c_1) = 0 \text{ und}$$
$$b_0(c_0, c_1)x_2^n + \ldots + b_n(c_0, c_1) = 0,$$

und daher $\mathrm{Res}_{F_1,F_2}(c_0, c_1) = 0$. Damit sind die Nullstellen von Res_{F_1,F_2} genau diejenigen $c \in L$, für welche die Geraden L_c Schnittpunkte von C_1 und C_2 enthalten.

Satz 3. *Zwei Kurven C_1 und C_2 vom Grad m und n ohne gemeinsame Komponente in der komplexen projektiven Ebene besitzen höchstens $m \cdot n$ Schnittpunkte.*

Beweis: Angenommen, C_1 und C_2 schneiden sich in mindestens $mn + 1$ Punkten $p_1, \ldots, p_{mn+1}$. Seien L und q gleich wie oben gewählt und liege q zusätzlich o.B.d.A. auf keiner Geraden durch p_i und p_j für $i \neq j$. Damit erhalten wir durch die Zentralprojektion Π mindestens $mn + 1$ verschiedene Punkte $c_1, \ldots, c_{mn+1}$ auf L, die aber zugleich Nullstellen von Res_{F_1,F_2} sind. Weil jedoch Res_{F_1,F_2} als ein homogenes Polynom vom Grad mn höchstens mn verschiedene Nullstellen besitzt, erhalten wir einen Widerspruch zur Annahme. □

Definition. Für $p = (c_0, c_1, c_2)$ ist die *Schnittvielfachheit* $\mu_p(C_1, C_2)$ zweier ebener Kurven $C_1 = V(F_1)$ und $C_2 = V(F_2)$ definiert durch die Vielfachheit der Nullstelle (c_0, c_1) von Res_{F_1,F_2}. Präzise ausgedrückt bedeutet dies

$$\mu_p(C_1, C_2) = \mathrm{ord}_{(c_0,c_1)}(\mathrm{Res}_{F_1,F_2}).$$

Auf diese Weise haben wir die Schnittvielfachheit von ebenen Kurven auf die Vielfachheit von Nullstellen eines Polynoms reduziert. Weil Res_{F_1,F_2} als ein homogenes Polynom vom Grad $m \cdot n$ genau $m \cdot n$ mit Vielfachheit gezählte Nullstellen besitzt, beträgt die Summe der Schnittvielfachheiten in den Schnittpunkten von C_1 und C_2 genau $m \cdot n$. Damit ist der Satz von Bézout bewiesen.

Satz 4 (Bézout)**.** *Seien C_1 und C_2 Kurven in der projektiven Ebene $\mathbb{P}_2(\mathbb{C})$ vom Grad m und n ohne gemeinsame Komponente. Dann gilt:*

$$\sum_{p \in C_1 \cap C_2} \mu_p(C_1, C_2) = m \cdot n.$$

Der Satz von Bézout hat einen lokalen und einen globalen Aspekt. Die Schnittmultiplizität ist durch das lokale Verhalten der Kurven in der Nähe des Schnittpunktes festgelegt.

Analog wie beim Schnitt einer Kurve mit einer Geraden lässt sich die Schnittmultiplizität zweier Kurven als Dimension von Vektorräumen interpretieren. Für zwei ebene Kurven $C_1 = V(F_1)$ und $C_2 = V(F_2)$ und einem Punkt $p \in C_1 \cap C_2$ entspricht sie nämlich der Dimension des Vektorraums der formalen Potenzreihen modulo dem Ideal, das von den beiden definierenden Polynomen erzeugt wird. Es gilt somit

$$\mu_p(C_1, C_2) = \dim_{\mathbb{C}} \mathbb{C}[[x_1, x_2]] / \langle F_1, F_2 \rangle.$$

Beispiel 1.2. Die beiden Kurven $C_1 = V(x_2^3 - x_0 x_1^2)$ und $C_2 = V(x_2^3 + x_0 x_1^2)$ schneiden sich nach dem Satz von Bézout in neun mit Vielfachheit gezählten Schnittpunkten. Aus den Gleichungen ergibt sich, dass diese in $C_1 \cap C_2 \cap V(x_0 x_1^2)$ liegen. Somit sind $p = (1, 0, 0)$ und $q = (0, 1, 0)$ die Schnittpunkte von C_1 und C_2. Die Schnittvielfachheit in p lässt sich einerseits über die Resultante ermitteln: $\mathrm{Res}_{F_1,F_2} = 8x_0^3 x_1^6$ und somit ist $\mu_p(C_1, C_2) = 6$.

Andererseits ist $W := \mathbb{C}[[x_1, x_2]] / \langle x_2^3 - x_1^2, x_2^3 + x_1^2 \rangle = \langle 1, x_1, x_2, x_1 x_2, x_2^2, x_1 x_2^2 \rangle$ und daher wieder $\dim_{\mathbb{C}} W = 6$.
In q schneiden sich die beiden Kurven mit Vielfachheit drei. Das entspricht nämlich der Vielfachheit der Nullstelle $(0, 1)$ von $\mathrm{Res}_{F_1,F_2} = 8x_0^3 x_1^6$.

Bevor nun konkrete Anwendungen des Satzes von Bézout erörtert werden, werden die Wendepunkte einer Kurve definiert. Anschließend wird untersucht, wie man diese findet.

Betrachten wir dazu für $m > 2$ und m ungerade die affine Gleichung

$$x_2(x_1) = (x_1 - \epsilon_1) \cdot \ldots \cdot (x_1 - \epsilon_m),$$

wobei ϵ_i die m paarweise verschiedenen Nullstellen von der Funktion $x_2(x_1)$ sind. Nach dem Satz von Rolle (siehe Satz **??** unten) hat $x_2(x_1)$ genau $m-1$ verschiedene Extrema und genau $m-2$ verschiedene Wendepunkte. Lässt man jetzt die ϵ_i für alle i gegen Null gehen, so liegt es nahe, den Ursprung als $(m-2)$-fachen Wendepunkt der Kurve $V(x_2 - x_1^m)$ zu bezeichnen. Dies motiviert Folgendes:
Wir nennen einen regulären Punkt p einer Kurve C in der komplexen projektiven Ebene einen *Wendepunkt* von C, wenn die Tangente T_p zu C in p keine Komponente von C ist und C bei p mit Vielfachheit größer gleich drei trifft. Dies wird in der folgenden Definition präzisiert.

Definition. p heißt ein r-facher Wendepunkt von C, wenn $T_p \not\subset C$ und $\mu_p(C, T_p) = r + 2$ gilt.

Sei im Folgenden $F \in \mathbb{C}[x_0, x_1, x_2]$ ein homogenes Polynom vom Grad $n \geq 2$.

Definition. Wir nennen $H_F := \left(\frac{\partial^2 F}{\partial x_i \partial x_j}\right)_{0 \leq i,j \leq 2}$ die *Hesse-Matrix* von F. Falls F ein reduziertes Polynom einer Kurve $C = V(F) \subset \mathbb{P}_2(\mathbb{C})$ ist und $\deg(\det(H_F)) \geq 1$, so heißt $H(C) := V(\det(H_F))$ die *Hesse-Kurve* von C.

Um gewisse Eigenschaften der Hesse-Kurve herleiten zu können, formen wir ihr definierendes Polynom um. Wir definieren $F_i := \frac{\partial F}{\partial x_i}$ und $F_{ij} := \frac{\partial^2 F}{\partial x_j \partial x_i}$. Wegen der Homogenität von F gilt die sogenannte Euler'sche Formel

$$x_0 F_0 + x_1 F_1 + x_2 F_2 = n \cdot F.$$

Wir dürfen aufgrund der Multilinearität der Determinante Zeilen und Spalten der Hesse-Matrix jeweils mit einem Faktor multiplizieren und zueinander addieren. Multiplizieren wir die nullte Zeile mit x_0 und zählen für $j = 1, 2$ die x_j-fache j-te Zeile dazu, so erhalten wir mit der Euler'schen Formel

$$\det(H_F) = \det \begin{pmatrix} F_{00} & F_{10} & F_{20} \\ F_{01} & F_{11} & F_{21} \\ F_{02} & F_{12} & F_{22} \end{pmatrix} = \tfrac{n-1}{x_0} \cdot \det \begin{pmatrix} F_0 & F_1 & F_2 \\ F_{01} & F_{11} & F_{21} \\ F_{02} & F_{12} & F_{22} \end{pmatrix}.$$

Verfährt man analog mit den Spalten, so ergibt sich

$$\det(H_F) = \tfrac{n-1}{x_0^2} \cdot \det \begin{pmatrix} nF & F_1 & F_2 \\ (n-1)F_1 & F_{11} & F_{21} \\ (n-1)F_2 & F_{12} & F_{22} \end{pmatrix}. \ (*)$$

Daraus folgt unmittelbar, dass $\deg(\det(H_F)) = 3(n-2)$, falls $\det(H_F) \neq 0$. Ebenso kann man daraus schließen, dass $\mathrm{Sing}(C) \subset H(C)$. Sei dazu $p = (p_0, p_1, p_2) \in C$ singulär und $p_0 \neq 0$. Wegen $F(p) = F_1(p) = F_2(p) = 0$ folgt $\det(H_F(p)) = 0$. Der nächste Satz besagt, dass ein glatter Punkt auf einer Kurve, die keine Gerade enthält, genau dann ein Wendepunkt der Kurve ist, wenn er auf der dazugehörigen Hesse-Kurve liegt.

Satz 5. *Sei $C = V(F) \subset \mathbb{P}_2(\mathbb{C})$ eine Kurve, die keine Gerade enthält. Dann ist ein glatter Punkt $p \in C$ genau dann ein Wendepunkt von C, wenn $p \in H(C)$.*

Beweis: Sei o.B.d.A. $p = (1, 0, 0) \in C$ glatt mit der Tangente $T_p = V(x_2)$. Ist $2 \leq k := \mu_p(C, T_p) < \infty$, so lässt sich $f(x_1, x_2) = F(1, x_1, x_2)$ in der Form

$$f(x_1, x_2) = x_1^k g(x_1) + x_2 h(x_1, x_2)$$

darstellen mit $g(0) \neq 0$ und $h(0, 0) \neq 0$. Dies folgt unmittelbar aus der Taylorentwicklung von f in $(0, 0)$. Somit können wir g und h folgendermaßen schreiben:

$$x_1^k g = a_2 x_1^2 + a_3 x_1^3 + \ldots,$$

$$h = b_0 + b_1 x_1 + b_2 x_2 + \ldots \text{ mit } b_0 \neq 0 \text{ und } a_i, b_j \in \mathbb{C}.$$

Infolgedessen ist genau dann $a_2 = 0$, wenn p ein Wendepunkt ist. Mit Hilfe der Formel $(*)$ erhalten wir

$$\det(H_F(p)) = (n-1)^2 \cdot \det \begin{pmatrix} 0 & 0 & b_0 \\ 0 & 2a_2 & b_1 \\ b_0 & b_1 & 2b_2 \end{pmatrix} = -2(n-1)^2 b_0^2 a_2,$$

woraus die Behauptung folgt. □

Mit den bisherigen Ergebnissen lässt sich außerdem feststellen, wann die Hesse-Kurve eine Gerade enthält. Ist nämlich eine Gerade L eine Komponente einer Kurve C , so ist L auch in $H(C)$ enthalten. Sei dazu $C = V(F)$, $L = V(x_0)$ und $F = x_0 G$. Dann ist mit der Notation von oben $F_i = x_0 G_i$ und $F_{ij} = x_0 G_{ij}$ für $i, j = 1, 2$ und wegen $(*)$ gilt $x_0^2 \cdot \det(H_F) = x_0^3 \cdot \det(H_G)$, also $\det(H_F) = x_0 \cdot \det(H_G)$.

Der nächste Satz dient der Anwendbarkeit des Satzes von Bézout:

Satz 6. *Sei $C = V(F) \subset \mathbb{P}_2(\mathbb{C})$ eine Kurve, die keine Gerade enthält. Dann haben C und $H(C)$ keine gemeinsame Komponente. Ist insbesondere $p \in C$ ein einfacher Wendepunkt, so ist $\mu_p(C, H(C)) = 1$.*

Beweis: Sei wiederum $p = (1,0,0) \in C$ glatt mit der Tangente $T_p = V(x_2)$ und $2 \leq k := \mu_p(C, T_p) < \infty$. Um die erste Behauptung zu zeigen, muss man die Terme niedrigster Ordnung der Taylorentwicklung von $\det(H_F)$ in p ausfindig machen. Es ergibt sich aus $(*)$

$$\det(H_F) = x_1^{k-2} \cdot G(x_0, x_1) + x_2 \cdot H(x_0, x_1, x_2), \text{ wobei } G(1,0) \neq 0.$$

Zu diesem Ergebnis kommt man mittels einer umfangreichen Rechnung, weshalb ein Computeralgebrasystem wie Maple hier dringend zu empfehlen ist. Aus Platzgründen wurde an dieser Stelle auf die explizite Darstellung der Polynome G und H verzichtet. Wegen $\mu_p(H(C), T_p) < k$ können C und $H(C)$ somit in keinem glatten Punkt eine gemeinsame Komponente haben.
Ist speziell p ein einfacher Wendepunkt, so ergibt sich für $k = 3$, dass $H(C)$ glatt in p und die Tangente an $H(C)$ in p verschieden von T_p ist, d.h., $\mu_p(C, H(C)) = 1$. $\square$

Weil demnach eine Kurve und ihre Hesse-Kurve keine gemeinsame Komponente besitzen, können wir den Satz von Bézout anwenden und kommen so zu folgendem Resultat:

Folgerung. *Eine algebraische Kurve $C \subset \mathbb{P}_2(\mathbb{C})$ vom Grad $n \geq 2$, die keine Gerade enthält, besitzt höchstens $3n(n-2)$ Wendepunkte.*

Die Höchstzahl von Wendepunkten wird nur dann erreicht, wenn C keine Singularität hat und alle Wendepunkte einfach sind. Eine nicht-singuläre Quadrik hat beispielsweise keine Wendepunkte, während eine nicht-singuläre Kubik neun mit Vielfachheit gezählte Wendepunkte besitzt. Weil aber die Schnittvielfachheit einer Wendetangente mit einer Kubik im Wendepunkt nach dem Satz von Bézout höchstens drei beträgt, während sie nach Definition des Wendepunktes mindestens drei beträgt, muss sie genau drei sein. Somit besitzt eine nicht-singuläre Kubik genau neun verschiedene, einfache Wendepunkte.

Betrachten wir beispielsweise die glatte Fermat-Kubik $C = V(x_0^3 + x_1^3 + x_2^3)$. Wegen

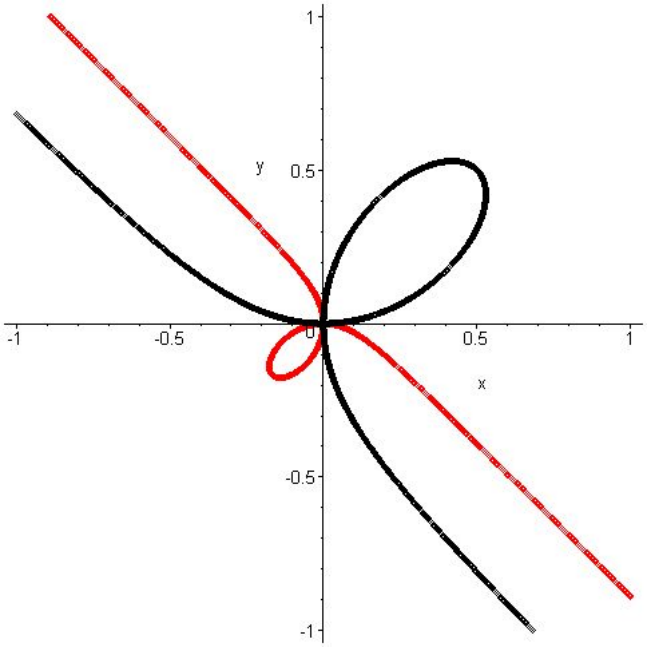
$$\det(H_F) = 216 x_0 x_1 x_2$$

zerfällt die Hesse-Kurve $H(C)$ in drei Geraden. Auf $V(x_0)$ liegen drei Wendepunkte, nämlich $(0,1,-1)$, $(0, -\frac{1}{2} + \frac{1}{2}i\sqrt{3}, -1)$ und $(0, -\frac{1}{2} - \frac{1}{2}i\sqrt{3}, -1)$. Auf $V(x_1)$ und $V(x_2)$ erhalten wir ebenfalls jeweils drei verschiedene Wendepunkte, also insgesamt neun.

Als zweites Beispiel sei das Blatt von Descartes $C = V(x_1^3 + x_2^3 - x_0 x_1 x_2)$ gegeben. Es ist singulär in $p = (1,0,0)$. Wir erhalten

$$G := \det(H_F) = -2(3x_1^3 + 3x_2^3 + x_0 x_1 x_2).$$

Somit ist die Hesse-Kurve $H(C)$ ein gespiegeltes Blatt von Descartes. Ihr Schnitt mit C besteht aus p sowie den drei unendlich fernen Wendepunkten $(0,1,-1)$, $(0, -\frac{1}{2} + \frac{1}{2}i\sqrt{3}, -1)$ und $(0, -\frac{1}{2} - \frac{1}{2}i\sqrt{3}, -1)$. Mittels Berechnung der Resultante $\mathrm{Res}_{F,G}$ erhalten wir $\mu_p(C, H(C)) = 6$. Also besitzt das Blatt von Descartes drei einfache Wendepunkte und einen Wendepunkt der Vielfachheit sechs.



Blatt von Descartes und seine Hesse-Kurve

1.3 Anwendungen des Satzes von Bézout

Für detaillierte Ausführungen dieser Thematik sei an dieser Stelle [1], Kapitel 2, 6.2 empfohlen. Der nachfolgende Satz gibt ein Kriterium an, wann eine ebene Kurve rational parametrisierbar ist. Für den Beweis wird der Satz von Bézout benötigt.

Satz 7. *Eine Kurve $C \subset \mathbb{P}_2(\mathbb{C})$ ohne Gerade als Komponente und mit einem Punkt p so, dass $\operatorname{ord}_p(C) = \deg(C) - 1$, gestattet eine rationale Parametrisierung, d.h., es existiert eine surjektive Abbildung*

$$\varphi : \mathbb{P}_1(\mathbb{C}) \to C, t = (t_0, t_1) \mapsto \big(\varphi_0(t), \varphi_1(t), \varphi_2(t)\big),$$

wobei $\varphi_i \in \mathbb{C}[t_0, t_1]$ homogen vom Grad $\deg(C)$ sind.

Beweis: Sei $C = V(F)$ und $n = \deg(F)$. Wir setzen $p = (1, 0, 0) \in \mathbb{P}_2(\mathbb{C})$. Dann ist $f(x_1, x_2) = F(1, x_1, x_2) = f_{n-1} + f_n$. Zum Parameter (t_0, t_1) betrachten wir die Gerade durch p mit dieser Steigung, also

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda \begin{pmatrix} t_0 \\ t_1 \end{pmatrix} \text{ mit } \lambda \in \mathbb{C}.$$

Der Schnitt dieser Geraden mit C ergibt

$$0 = f_{n-1}(\lambda t_0, \lambda t_1) + f_n(\lambda t_0, \lambda t_1) = \lambda^{n-1}\big(f_{n-1}(t_0, t_1) + \lambda f_n(t_0, t_1)\big).$$

Weil nach Voraussetzung C keine Gerade enthält, gibt es nach dem Satz von Bézout neben dem Schnittpunkt p der Vielfachheit $n - 1$ für $\lambda = 0$ genau einen weiteren Schnittpunkt für

$$\lambda = -\frac{f_{n-1}(t_0, t_1)}{f_n(t_0, t_1)}.$$

Insbesondere haben f_n und f_{n-1} keine gemeinsame Nullstelle, weil nach Voraussetzung die Kurve C keine Gerade als Komponente besitzt. Daher ist die gesuchte Parametrisierung gegeben durch

$$\varphi(t_0,t_1) = \big(1, -t_0\tfrac{f_{n-1}(t_0,t_1)}{f_n(t_0,t_1)}, -t_1\tfrac{f_{n-1}(t_0,t_1)}{f_n(t_0,t_1)}\big) = \big(f_n(t_0,t_1), -t_0 f_{n-1}(t_0,t_1), -t_1 f_{n-1}(t_0,t_1)\big).$$

Sie ist surjektiv, weil man zu jedem Punkt q der Kurve C eine Gerade durch p mit der Steigung (t_0,t_1) findet, sodass die Gerade die Kurve C in q schneidet. □

Beispiel 1.3. Das dreiblättrige Kleeblatt $V((x_1^2+x_2^2)^2+3x_1^2x_2-x_2^3)$ vom Grad vier hat im Ursprung die Ordnung drei und ist folglich rational parametrisierbar mittels der surjektiven Abbildung

$$\varphi : (t_0,t_1) \to \big((t_0^2+t_1^2)^2, -3t_0^3t_1+t_0t_1^3, -3t_0^2t_1^2+t_1^4\big).$$

Definition. Ein *lineares System* ist ein System linearer Gleichungen in homogenen Polynomen.

Anstatt die Anzahl der Schnittpunkte zweier Kurven zu bestimmen, können wir uns auch fragen, welche Kurven durch endlich viele gegebene Punkte in der projektiven Ebene gehen. Auf diese Weise erhalten wir ein lineares System von Kurven, sodass die gegebenen Punkte in der Schnittmenge aller Kurven des Systems liegen. Vor weiteren Anwendungen des Satzes von Bézout wird nun genauer auf solche Kurvensysteme eingegangen.

Die Menge aller homogenen Polynome $\sum_{i_0+\ldots+i_k=m} a_{i_0}\ldots a_{i_k}x_0^{i_0}\ldots x_k^{i_k}$ vom Grad m in den Unbestimmten $x_0,\ldots,x_k$ bildet einen komplexen Vektorraum der Dimension $\binom{m+k}{k}$. Werden nun zwei homogene Polynome als äquivalent angesehen, wenn sie sich nur durch einen konstanten Faktor unterscheiden, so bilden diese Äquivalenzklassen, also alle Kurven vom Grad m in der projektiven Ebene, einen komplexen, projektiven Vektorraum der Dimension $\binom{m+2}{2}-1 = \frac{m(m+3)}{2}$.
Man nennt projektive Untervektorräume von Kurven von einem gewissen Grad m lineare Teilsysteme. Ein solches lineares Teilsystem jenes projektiven Vektorraums der Dimension d lässt sich beschreiben, indem man sich eine Basis $F_0,\ldots,F_d$ des $(d+1)$-dimensionalen Vektorraums der homogenen Polynome vom Grad m vorgibt. Das lineare Teilsystem besteht dann aus allen Kurven mit Gleichungen

$$\lambda_0F_0+\ldots+\lambda_dF_d = 0 \text{ und } \lambda_i \in \mathbb{C}$$

Im Fall $d=1$ spricht man von einem linearen Kurvenbündel.

Lineare Kurvensysteme lassen sich außerdem mittels einer endlichen Punktmenge mit Vielfachheiten in der projektiven Ebene definieren. Wir betrachten dazu die Menge aller Kurven vom Grad m, die durch die Gleichungen

$$F(x_0,x_1,x_2) = \sum_{i+j+k=m} a_{ijk}x_0^ix_1^jx_2^k = 0$$

gegeben sind. Die Bedingung an eine Kurve, durch einen Punkt $p=(p_0,p_1,p_2)$ in der projektiven Ebene zu gehen, impliziert die Gleichung $\sum_{i+j+k=m} a_{ijk}p_0^ip_1^jp_2^k = 0$.

Diese Gleichung ist linear in den Unbekannten a_{ijk} mit $p_0^i p_1^j p_2^k$ als Koeffizienten. Damit bilden diejenigen Kurven vom Grad m, welche diese lineare Bedingung erfüllen, einen projektiven Untervektorraum der Kodimension eins des Vektorraums aller Kurven vom Grad m.

Allgemein bedeutet für eine Kurve C vom Grad m die Bedingung, mindestens Vielfachheit s in einem Punkt p zu besitzen, $\frac{s(s+1)}{2}$ linear unabhängige Bedingungen. Ein homogenes Polynom in drei Variablen hat nämlich genau $\frac{s(s+1)}{2}$ partielle Ableitungen der Ordnung $s-1$. Es bleibt noch zu zeigen, dass diese $\frac{s(s+1)}{2}$ Bedingungen linear unabhängig sind.
Seien dazu o.B.d.A. $p = (1,0,0)$ und $C = V(F)$ mit

$$F = \sum_{i+j+k=m} a_{ijk} x_0^i x_1^j x_2^k.$$

Dann folgt aus

$$\frac{\partial^{s-1} F}{\partial x_0^{s-1-j-k} \partial x_1^j \partial x_2^k}(1,0,0) = 0,$$

dass $a_{ijk} = 0$ für $j + k \leq s - 1$ gilt. Da die a_{ijk} als Variablen paarweise linear unabhängig sind, ergeben sich $\frac{s(s+1)}{2}$ linear unabhängige Bedingungen. Wir fassen die bisherigen Ergebnisse in folgendem Satz zusammen.

Satz 8. *Seien die Punkte $p_1, \ldots, p_r$ gegeben. Dann bilden die Kurven vom Grad m, welche mindestens Vielfachheit s_i bei p_i besitzen, ein lineares System der Dimension d, wobei*

$$d \geq \frac{m(m+3)}{2} - \sum_{i=1}^{r} \frac{s_i(s_i+1)}{2}.$$

Betrachten wir beispielsweise den Fall $m = 2$, d.h., Quadriken. Diese bilden ein lineares System der Dimension $\frac{2(2+3)}{2} = 5$. Somit geht mindestens eine Quadrik durch fünf verschiedene Punkte. Die nächste Definition dient dazu, bestimmen zu können, wann Punkte in einer genügend allgemeinen Lage sind, sodass durch sie genau eine Kurve von einem gewissen Grad geht.

Definition. r verschiedene Punkte $p_1, \ldots, p_r \in \mathbb{P}_2(\mathbb{C})$ sind in allgemeiner Lage in Relation zu Kurven vom Grad m, genannt *generisch*, wenn das dazugehörige lineare System durch $p_1, \ldots, p_r$ die kleinstmögliche Dimension d besitzt, d.h., $d = \frac{m(m+3)}{2} - r$.

Beispiel 1.4. Gesucht ist eine Gerade durch drei Punkte p_1, p_2, p_3 in der projektiven Ebene. Sind p_1, p_2, p_3 generisch, so ergibt sich für das dazugehörige lineare System die Dimension $d = -1$, d.h., es existiert keine Gerade durch diese Punkte. Sind p_1, p_2, p_3 dagegen kollinear, muss man folgende Fallunterscheidung treffen. Ist $p_i \neq p_j$ für ein i, j mit $i \neq j$, so erhalten wir ein nulldimensionales lineares System, also eine Gerade. Falls die Punkte alle zusammenfallen, d.h., $p_i = p_j \ \forall i, j$, so besitzt das dazugehörige lineare System die Dimension $d = 1$, was einem Geradenbündel entspricht.

Das Wort „generisch“ mit der Bedeutung „genügend allgemein“ wird in vielen Zusammenhängen verwendet. Es ist jedoch situationsbedingt. Drei Punkte in der projektiven Ebene sind beispielsweise generisch, wenn sie nicht kollinear sind. Will man einen Würfel in eine Ebene projizieren, genügt es für eine generische Projektion zu verlangen, dass die Projektionsstrahlen zu keiner Seitenfläche des Würfels normal stehen.
Um die obige Definition zu rechtfertigen, bleibt es zu zeigen, dass generische Punkte in der projektiven Ebene $\mathbb{P}_2(\mathbb{C})$ wirklich genügend allgemein sind, d.h., dass fast alle r-Tupel von Punkten generisch sind. Wir betrachten dazu das r-Tupel $(p_1, \ldots, p_r)$ als einen Punkt im m-fachen kartesischen Produkt $\mathbb{P}_2(\mathbb{C}) \times \ldots \times \mathbb{P}_2(\mathbb{C})$. Die Bedingung, dass $(p_1, \ldots, p_r)$ generisch ist, ist eine Bedingung an den Rang eines Systems linearer Gleichungen. Sie bedeutet folglich, dass gewisse Determinanten nicht verschwinden. Die Determinanten sind Polynome in den homogenen Koordinaten der Punkte $p_1, \ldots, p_r$. Die Menge von generischen r-Tupeln ist somit das Komplement einer abgeschlossenen Menge M, nämlich der Nullstellenmenge von Determinanten. Umfasst M speziell ganz $\mathbb{P}_2(\mathbb{C}) \times \ldots \times \mathbb{P}_2(\mathbb{C})$, so existiert kein generischer Punkt. Ansonsten ist M eine echte algebraische Teilmenge und folglich bilden die generischen r-Tupel in $\mathbb{P}_2(\mathbb{C}) \times \ldots \times \mathbb{P}_2(\mathbb{C})$ eine nichtleere Zariski-offene Teilmenge, die im Sinn der euklidischen Topologie offen und dicht ist. Damit ist die obige Definition gerechtfertigt.

Satz 9. *Es existiert genau eine Kurve vom Grad m durch $\frac{m(m+3)}{2}$ generische Punkte in $\mathbb{P}_2(\mathbb{C})$.*

Beweis: Wir zeigen dies mittels Induktion über m. Für $m = 1$ existiert genau eine Gerade durch zwei verschiedene Punkte. Um den Induktionsschritt von $m-1$ nach m durchzuführen, betrachten wir die Gleichung

$$\frac{m(m+3)}{2} = \frac{(m-1)(m-1+3)}{2} + m + 1.$$

Zuerst wählen wir $m+1$ verschiedene, auf einer Geraden L liegende Punkte $p_1, \ldots, p_{m+1}$ und $\frac{(m-1)(m-1+3)}{2}$ weitere nicht auf L liegende Punkte $p_{m+2}, \ldots, p_{\frac{m(m+3)}{2}}$. Letztere können wir nach Induktionsannahme generisch in Bezug auf Kurven vom Grad $m-1$ wählen. Nach dem Satz von Bézout muss L eine Komponente jeder Kurve C vom Grad m durch $p_1, \ldots, p_{m+1}$ sein und daher $C = L \cup C'$, wobei C' eine Kurve vom Grad $m-1$ ist. Weil die Kurve C' durch die übrigen $\frac{m(m+3)}{2} - m - 1$ Punkte gehen muss, ist sie nach deren Wahl eindeutig bestimmt. □

Durch fünf generische Punkte geht damit genau eine Quadrik, durch neun generische Punkte genau eine Kubik.

Im Folgenden wird ein Satz über spezielle Lagen von Schnittpunkten zweier Kurven als Anwendung des Satzes von Bézout bewiesen. Anschließend wird der Satz von Pascal als ein Spezialfall davon erläutert.

Satz 10. *Seien C, C' Kurven vom Grad n, die sich in genau n^2 verschiedenen Punkten schneiden. Falls genau $m \cdot n$ dieser Punkte auf einer irreduziblen Kurve C'' vom Grad m liegen, so liegen die übrigen $n \cdot (n-m)$ Schnittpunkte auf einer Kurve C''' vom Grad $n-m$.*

Dieser Satz setzt eine spezielle Lage von Punkten voraus. Nach Satz **??** geht nämlich eine Kurve vom Grad $n-m$ nicht durch $n \cdot (n-m)$ generische Punkte, weil für $n > m \geq 2$ die Ungleichung

$$\frac{(n-m)(n-m+3)}{2} < \frac{2n(n-m)}{2}$$

gilt. Drei nicht-kollineare Punkte in der projektiven Ebene liegen beispielsweise nicht auf einer Geraden.

Beweis: Seien $C = V(F)$, $C' = V(G)$ und $\mathcal{L}$ das lineare Kurvenbündel vom Grad n mit der Gleichung

$$\lambda F + \mu G = 0.$$

Alle Kurven in $\mathcal{L}$ gehen durch die n^2 Schnittpunkte von C und C'. Wir wählen einen Punkt $q \in C''$ aus den nm verschiedenen Punkten in $C \cap C''$. Weil $\mathcal{L}$ eindimensional ist, existiert eine Kurve $\hat{C} \in \mathcal{L}$, die durch q geht. Dann schneiden sich aber $\hat{C}$ und C'' in mindestens $nm+1$ Punkten. Somit haben sie nach dem Satz von Bézout eine gemeinsame Komponente. Diese kann nur C'' sein, weil C'' nach Voraussetzung irreduzibel ist. Daher können wir $\hat{C}$ schreiben als

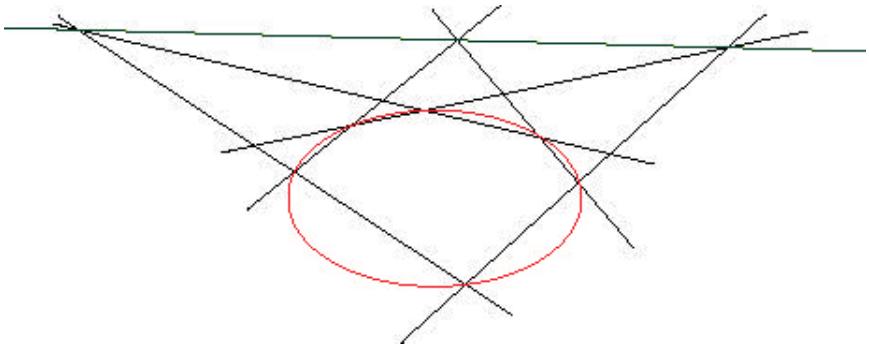
$$\hat{C} = C'' \cup C''',$$

wobei C''' eine Kurve vom Grad $n-m$ ist. Die restlichen, außerhalb von C'' liegenden $n(n-m)$ Schnittpunkte von C und C' liegen auf $\hat{C}$ und daher auf C'''. □

Der folgende Satz von Pascal bezieht sich auf ein Hexagon, welches in eine irreduzible Quadrik eingeschrieben wird. Ein Hexagon besteht aus sechs verschiedenen Punkten $p_1, \ldots, p_6$ und sechs Linien $L_1, \ldots, L_6$ in der projektiven Ebene, wobei L_i die Gerade durch p_i und p_{i+1} ist und $p_7 := p_1$.

Satz 11 (Pascal)**.** *Für ein in eine irreduzible Quadrik Q eingeschriebenes Hexagon liegen die Schnittpunkte der drei Paare von gegenüberliegenden Seiten auf einer Geraden.*

Beweis: Wir definieren $C := L_1 \cup L_3 \cup L_5$, $C' := L_2 \cup L_4 \cup L_6$ und $C'' := Q$. Nach dem Satz von Bézout und Konstruktion schneiden sich C und C' in neun verschiedenen Punkten. Es liegen $2 \cdot 3 = 6$ jener Schnittpunkte auf C''. Nach letztem Satz **??** liegen also die übrigen drei Schnittpunkte auf einer Kurve vom Grad eins, also auf einer Geraden. □



Die Situation des Satzes von Pascal an dem Beispiel der Ellipse

Der Satz von Pascal wird im letzten Unterkapitel über einen alternativen Zugang, nämlich den Satz von Cayley-Bacharach, bewiesen.

Als eine weitere Anwendung des Satzes von Bézout werden wir eine obere Schranke für die Anzahl von singulären Punkten einer Kurve herleiten. Die grundlegende Idee dabei ist es, eine Kurve durch die singulären Punkte einer gegebenen Kurve zu legen und anschließend den Satz von Bézout auf die Anzahl ihrer Schnittpunkte anzuwenden.

Satz 12. *Die Singularitätenmenge* $\mathrm{Sing}(C)$ *einer algebraischen Kurve* $C \subset \mathbb{C}^2$ *ist endlich.*

Beweis: Sei $C = V(f)$ mit dem reduzierten Polynom f und enthalte C o.B.d.A. keine achsenparallelen Geraden. Für $C_i := V(\frac{\partial f}{\partial x_i})$ und $i = 1, 2$ ist dann $\mathrm{Sing}(C) = C \cap C_1 \cap C_2$. Eine Gerade ist in jedem Punkt glatt. Demzufolge können wir $\deg(C) = \deg(f) \geq 2$ voraussetzen. Damit ist für ein i auch $\deg(\frac{\partial f}{\partial x_i}) \geq 1$. Sei nun o.B.d.A. $i = 1$. Dann ist C_1 eine algebraische Kurve und $\mathrm{Sing}(C) \subset C \cap C_1$. Nach dem Satz von Bézout genügt es also zu zeigen, dass C und C_1 keine gemeinsame Komponente besitzen.
Angenommen, f und $\frac{\partial f}{\partial x_1}$ haben einen gemeinsamen Primfaktor g. Dann ist $f = g \cdot h$ und $\frac{\partial f}{\partial x_1} = g \cdot h_1 = h \cdot \frac{\partial g}{\partial x_1} + g \cdot \frac{\partial h}{\partial x_1}$. Daher ist g auch Teiler von $h \cdot \frac{\partial g}{\partial x_1}$. Falls $\frac{\partial g}{\partial x_1} \neq 0$, so ist g Teiler von h, also g^2 Teiler von f, was im Widerspruch zu f reduziertes Polynom ist. Ist $\frac{\partial g}{\partial x_1} = 0$, so ist $g = x_2 - a$. Somit würde C eine achsenparallele Gerade enthalten, was ein Widerspruch zur Annahme ist. □

Ist $\deg(C) = n$, so besitzt C nach dem Satz von Bézout höchstens $n(n-1)$ singuläre Punkte. Diese Abschätzung wird im Folgenden für irreduzible Kurven verbessert.

Satz 13. *Eine irreduzible algebraische Kurve* $C \subset \mathbb{P}_2(\mathbb{C})$ *vom Grad* n *hat maximal* $\gamma(n) := \frac{1}{2}(n-1)(n-2)$ *Singularitäten, d.h.*

$$\sum_{p \in C} \mu_p(C) \cdot (\mu_p(C) - 1) \leq (n-1) \cdot (n-2).$$

Beweis: Sei o.B.d.A. $n \geq 3$. Angenommen, C hätte $\gamma(n) + 1$ singuläre Punkte.
Wir wählen $n - 3$ weitere Punkte auf C und erhalten somit insgesamt

$$\gamma(n) + 1 + n - 3 = \frac{1}{2}(n-2)(n+1)$$

Punkte. Daher existiert eine Kurve C' vom Grad $m \leq n - 2$, die durch alle Punkte geht. Es gilt also

$$\sum_{p \in C \cap C'} \mu_p(C, C') \geq 2(\gamma(n) + 1) + n - 3 = n(n-2) + 1.$$

Nach Voraussetzung ist C irreduzibel, kann also wegen $\deg(C') < n$ keine Komponente von C' sein. Mit Hilfe des Satzes von Bézout ergibt sich

$$\sum_{p \in C \cap C'} \mu_p(C, C') = n \cdot m \leq n \cdot (n-2),$$

was einen Widerspruch zur ersten Abschätzung darstellt. □

So besitzen etwa die Neil'sche Parabel $V(x_2^3 - x_1^2)$, das Blatt von Descartes $V(x_1^3 + x_2^3 - 3x_1x_2)$ und der Newton'sche Knoten $V(x_1^2(x_1+1) - x_2^2)$ jeweils eine Singularität, was der oberen Schranke entspricht. Für das vierblättrige Kleeblatt $V((x_1^2 + x_2^2)^3 - 4x_1^2x_2^2)$ mit einer Singularität ist die obere Schranke zehn äußerst schlecht.

1.4 Der Satz von Cayley-Bacharach

Im letzten Unterkapitel werden zunächst die Begriffe der Filtration und der Graduierung von Algebren eingeführt. Nach grundlegenden Definitionen aus der lokalen Ringtheorie wird anschließend der Satz von Cayley-Bacharach bewiesen und seine Anwendungen erörtert. Die Schnittmultiplizität zweier Kurven vom Standpunkt der lokalen Ringtheorie und die Filtration von Algebren wird in [11], Teil 1, Kapitel 5 und Teil $2B$ ausführlich und allgemein unter die Lupe genommen.

Unter einer $\mathbb{Z}$-*Filtration* einer Algebra S über einem kommutativen Ring R versteht man eine Familie $\mathcal{F} = \{\mathcal{F}_i\}_{i\in\mathbb{Z}}$ von R-Untermoduln $\mathcal{F}_i \subset S$ für $i \in \mathbb{Z}$ mit folgenden vier Eigenschaften:

(1) $\mathcal{F}_i \subset \mathcal{F}_{i+1}$ für alle $i \in \mathbb{Z}$.

(2) $\mathcal{F}_i \cdot \mathcal{F}_j \subset \mathcal{F}_{i+j}$ für alle $i, j \in \mathbb{Z}$.

(3) $1 \in \mathcal{F}_0$.

(4) $\bigcup_{i\in\mathbb{Z}} \mathcal{F}_i = S$.

Eine Algebra S/R mit einer solchen Filtration $\mathcal{F}$, geschrieben $(S/R, \mathcal{F})$ wird *gefilterte Algebra* genannt. $\mathcal{F}$ heißt *separiert*, wenn $\bigcap_{i\in\mathbb{Z}} \mathcal{F}_i = \{0\}$. Aus den Eigenschaften (2) und (3) folgt, dass $\mathcal{F}_0$ ein Unterring von S und jedes $\mathcal{F}_i$ ein $\mathcal{F}_0$-Modul ist.
Ist $\mathcal{F}$ separiert, so lässt sich die Ordnung eines Elements $0 \neq f \in S$ bezüglich $\mathcal{F}$ folgendermaßen definieren:

$$\mathrm{ord}_{\mathcal{F}}(f) := \min\{i \in \mathbb{Z} |\ f \in \mathcal{F}_i\}$$

Wir setzen $\mathrm{ord}_{\mathcal{F}}(0) = -\infty$. Die zu $(S/R, \mathcal{F})$ assoziierte *graduierte Algebra* $\mathrm{gr}_{\mathcal{F}}S$ wird wie folgt konstruiert: Seien $\mathrm{gr}^i_{\mathcal{F}}S := \mathcal{F}_i/\mathcal{F}_{i-1}$ für $i \in \mathbb{Z}$ und sei

$$\mathrm{gr}_{\mathcal{F}}S := \oplus_{i\in\mathbb{Z}}\ \mathrm{gr}^i_{\mathcal{F}}S.$$

Weiters nennen wir $L_{\mathcal{F}}(f) := f + \mathcal{F}_{\mathrm{ord(f-1)}} \in \mathrm{gr}_{\mathcal{F}}S$ den *Leitterm* von f.

Wir betrachten ab jetzt den Spezialfall $S = \mathbb{C}[x_0, x_1, x_2] = \oplus_{0\leq i\in\mathbb{Z}}\ S_i$. Dabei umfassen S_i jeweils alle homogenen Polynome vom Grad i über $\mathbb{C}$. Somit erhalten wir mit

$$\mathcal{F}_i := \oplus_{0\leq k\leq i}\ S_k\ (i \in \mathbb{N})$$

eine separierte Filtration $\mathcal{F} = \{\mathcal{F}_i\}_{i\in\mathbb{Z}}$ von $S/\mathbb{C}$. Diese wird als *Grad-Filtration* bezeichnet. Die Ordnung eines Polynoms $f \in S \setminus \{0\}$ ist in diesem Fall der höchste Grad aller homogenen Komponenten von f. Die $\mathbb{C}$-Untermoduln der assoziierten graduierten Algebra lassen sich auf andere Weise schreiben:

$$\mathrm{gr}^i_{\mathcal{F}} S = \mathcal{F}_i/\mathcal{F}_{i-1} = \oplus_{0\leq k\leq i}\ S_k/\oplus_{0\leq k\leq i-1}\ S_k \cong S_i, \text{ wobei } i \in \mathbb{N}.$$

Damit erhalten wir einen kanonischen Isomorphismus dieser graduierten $\mathbb{C}$-Algebren:

$$\mathrm{gr}_{\mathcal{F}} S \cong S.$$

Unter diesem Isomorphismus identifizieren wir den Leitterm $L_{\mathcal{F}}(f)$ eines Polynoms $f \in S \setminus \{0\}$ mit der homogenen Komponente von f vom höchsten Grad.

Für den Satz von Cayley-Bacharach wird noch eine Reihe von Definitionen benötigt. Dabei wird die Schnittvielfachheit zweier Kurven in einem Punkt p vom Standpunkt der lokalen Ringtheorie erörtert.

Man nennt

$$\mathcal{O}_p := \{\tfrac{\phi}{\psi} \in \mathcal{R}(\mathbb{P}_2(\mathbb{C}))|\ \psi(p) \neq 0\}$$

den *lokalen Ring* von $\mathbb{P}_2(\mathbb{C})$ in p, wobei $\mathcal{R}(\mathbb{P}_2(\mathbb{C}))$ der Körper der rationalen Funktionen auf $\mathbb{P}_2(\mathbb{C})$ mit Elementen $\frac{\phi}{\psi}$ für $\phi, \psi \in \mathbb{C}[x_0, x_1, x_2]$ ist. Sei $F \in \mathbb{C}[x_0, x_1, x_2]$ ein homogenes Polynom über $\mathbb{C}$ von positivem Grad. Dann ist

$$\mathcal{O}_F := \{\tfrac{\phi}{\psi} \in \mathcal{R}(\mathbb{P}_2(\mathbb{C}))|\ F \text{ und } \psi \text{ sind relativ prim}\}$$

ist ein Unterring von $\mathcal{R}(\mathbb{P}_2(\mathbb{C}))$. Er setzt sich aus den rationalen Funktionen zusammen, die auf $V(F)$ definiert sind. Sei weiters $\langle F\rangle = \{G \cdot F|\ G \in \mathbb{C}[x_0, x_1, x_2]\}$ das Ideal von F. Dann heißt

$$I(F)_p := \{\tfrac{\phi}{\psi} \in \mathcal{O}_p|\ \phi \in \langle F\rangle\}$$

das von dem homogenen Polynom F erzeugte *Ideal bezüglich dem Punkt* p und

$$\mathcal{O}_{F_1\cap\ldots\cap F_m,p} := \mathcal{O}_p \diagup \langle I(F_1)_p + \ldots + I(F_m)_p\rangle$$

der *lokale Ring* von $\mathbb{P}_2(\mathbb{C})$ in p *bezüglich der Schnittmenge* $V(F_1) \cap \ldots \cap V(F_m)$.

Damit lässt sich die Schnittvielfachheit zweier Kurven alternativ als Dimension des lokalen Ringes in p über $\mathbb{C}$ definieren.

Definition. Für zwei Kurven $C_1 = V(F_1)$ und $C_2 = V(F_2)$ in $\mathbb{P}_2(\mathbb{C})$ ist

$$\mu_p(C_1, C_2) := \dim_{\mathbb{C}} \mathcal{O}_{F_1\cap F_2,p}$$

die Schnittmultiplizität von F_1 und F_2 im Punkt p.

Wir nennen eine weiteren Kurve $C' := V(G)$ *assoziiert* zu $C_1 \cap C_2$, falls $\dim_{\mathbb{C}} \mathcal{O}_{F_1\cap F_2\cap G,p} = \mu_p(C_1, C_2)$ für alle Punkte $p \in V(F_1) \cap V(F_2)$ gilt. Zur letzten Bedingung ist äquivalent dazu, dass für alle $p \in C_1 \cap C_2$ gilt, dass

$$\dim_{\mathbb{C}} \mathcal{O}_p/\ \langle I(F_1)_p + I(F_2)_p\rangle = \dim_{\mathbb{C}} \mathcal{O}_p\ \langle I(F_1)_p + I(F_2)_p + I(G)_p\rangle.$$

Letzteres bedeutet $I(G)_p \subset I(F_1)_p + I(F_2)_p$ für alle $p \in C_1 \cap C_2$. Falls speziell $\mu_p(C_1, C_2) = 1$ gilt, bedeutet dies, dass $p \in C'$.

Satz 14 (Cayley-Bacharach)**.** *Seien $C_1 := V(F_1)$ und $C_2 := V(F_2)$ zwei Kurven in $\mathbb{P}_2(\mathbb{C})$ ohne gemeinsame Komponente. Seien $q := deg(F_1)$, $r := deg(F_2)$ und $C' := V(G)$ eine weitere Kurve mit $h := deg(G) < q + r - 2$. Falls*

$$\sum_{p \in C_1 \cap C_2} \dim_{\mathbb{C}} \mathcal{O}_{F_1 \cap F_2 \cap G, p} \geq (q-1)(r-1) + h + 1,$$

dann ist C' assoziiert zu $C_1 \cap C_2$.

Beweis: Angenommen, F_1 und F_2 haben keine gemeinsame Komponente und f_1, f_2 und g sind die zugehörigen Polynome zu F_1, F_2 und G in $\mathbb{C}[x_1, x_2]$. Sei γ das Bild von g in $R := \mathbb{C}[x_1, x_2]/\langle f_1, f_2 \rangle$. Nach obiger Überlegung ist C' genau dann assoziiert zu $C_1 \cap C_2$, wenn $I(G)_p \subset I(F_1)_p + I(F_2)_p$ für alle $p \in C_1 \cap C_2$. Sei nun m_p das maximale Ideal in R bezüglich p. Es gilt

$$\mathcal{O}_{F_1 \cap F_2, p} = \mathcal{O}_p/\langle I(F_1)_p + I(F_2)_p \rangle \cong R/m_p \text{ (siehe dazu [11], Theorem 5.1).}$$

Daher ist zur Bedingung $I(G)_p \subset I(F_1)_p + I(F_2)_p$ äquivalent, dass das Bild von γ in R/m_p für alle $p \in C_1 \cap C_2$ verschwindet. Seien $p_1, \ldots, p_s$ die $s = p \cdot q$ Schnittpunkte von C_1 und C_2. Weil die maximalen Ideale $m_{p_1}, \ldots, m_{p_s}$ paarweise relativ prim sind und $\bigcap_{k=1}^{s} m_{p_k} = \{0\}$, ist der chinesische Restsatz anwendbar. Dieser besagt, dass

$$R \cong R/m_{p_1} \times \ldots \times R/m_{p_s}.$$

Daher ist zur Bedingung, dass γ in allen R/m_{p_i} für $i = 1, \ldots, s$ verschwindet, äquivalent, dass γ in R verschwindet, d.h., dass $\gamma = 0$ gilt. Zusammenfassend genügt es also zu zeigen, dass γ als das Bild von g in R verschwindet.
Wir setzen dazu

$$S := \mathrm{gr}_{\mathcal{F}} R = \mathbb{C}[x_1, x_2]/\langle L_{\mathcal{F}}(f_1), L_{\mathcal{F}}(f_2) \rangle.$$

Angenommen, es gelte $\gamma \neq 0$. Dann ist $\gamma^0 := L_{\mathcal{F}}\gamma \neq 0$ ein homogenes Polynom in S vom Grad echt kleiner als $q + r - 2$. Sind ξ und η die Bilder von x_1 und x_2 in S, dann ist $\langle \xi, \eta \rangle \cdot \gamma^0 \neq 0$, weil $\gamma \notin \mathrm{gr}_{\mathcal{F}}^{q+r-2} R$. Daher existiert ein α_1 homogen mit $\deg(\alpha_1) = 1$ und $\alpha_1 \cdot \gamma^0 \neq 0$.
Mittels Induktion über den Grad der homogenen Polynome α_i vom Grad i folgt, dass $\alpha_i \cdot \gamma^0 \neq 0$ für $i = 0, \ldots, q+r-2-h$ und $\alpha_0 = 1$. Diese α_i haben alle unterschiedliche Grade und sind daher linear unabhängig über $\mathbb{C}$. Also ist $\dim_{\mathbb{C}} \langle \gamma \rangle \geq q + r - 1 - h$ und somit

$$\dim_{\mathbb{C}} R/\langle \gamma \rangle \leq q \cdot r - (q + r - 1 - h) = (q-1)(r-1) + h.$$

Nach Voraussetzung gilt jedoch, dass $\dim_{\mathbb{C}} R/\langle \gamma \rangle \geq (q-1)(r-1) + h + 1$. Dieser Widerspruch beweist, dass $\gamma = 0$ sein muss. □

Der Satz von Cayley-Bacharach gilt ebenso für Polynome über einem beliebigen Körper K. Im Folgenden werden einige Anwendungsbeispiele dazu erläutert.

Unter den Annahmen des Satzes bestehe $C_1 \cap C_2$ aus $q \cdot r$ verschiedenen Punkten und C' beinhalte $(q-1)(r-1) + h + 1$ dieser Punkte. Dann geht C' nach dem Satz **??** durch alle $q \cdot r$ Punkte in $C_1 \cap C_2$. Wir können diese Aussage auch auf Systeme algebraischer Gleichungen umdeuten.
Sei das Gleichungssystem

$$F_1(x_0, x_1, x_2) = 0,\ F_2(x_0, x_1, x_2) = 0,\ G(x_0, x_1, x_2) = 0$$

gegeben, wobei F_1, F_2 und G homogene Polynome vom Grad q, r und $h < q+r-2$ sind. Angenommen, das System $F_1 = F_2 = 0$ hat genau $q \cdot r$ verschiedene Lösungen p_i in $\mathbb{P}_2(\mathbb{C})$ und $(q-1)(r-1)+h+1$ davon sind ebenso Lösungen der Gleichung $G = 0$. Dann sind nach dem Satz **??** alle p_i Lösungen von $F_1 = F_2 = G = 0$.

Sei speziell $q = r = h = n \geq 3$. Dann ist die Bedingung $h < q + r - 2$ automatisch erfüllt. Falls $C_1 \cap C_2$ aus n^2 verschiedenen Punkten besteht und falls C' durch $(n-1)^2+n+1 = n(n-1)+2$ davon geht, so sind nach dem Satz **??** alle n^2 Punkte in C' enthalten.
Insbesondere der Fall $q = r = h = 3$ ist von großer Bedeutung. Zum einen lässt sich der Satz von Pascal (Satz **??**) damit alternativ beweisen. Seien unter den gleichen Bedingungen wie in Satz **??**

$$C_1 := L_1 \cup L_3 \cup L_5,\ C_2 := L_2 \cup L_4 \cup L_6 \text{ und } C' := Q \cup L',$$

wobei L' die Gerade durch $P_1' := L_1 \cap L_4$ und $P_2' := L_2 \cap L_5$ ist. Es handelt sich demnach um drei Kubiken. C_1 und C_2 schneiden sich in neun verschiedenen Punkten. C' geht durch acht dieser neun Schnittpunkte. Also muss sie nach dem Satz von Cayley-Bacharach auch durch $P_3' := L_3 \cap L_6$ gehen. Weil aber der Punkt P_3' nach Konstruktion nicht auf Q liegt, liegt er auf L'. Dies bedeutet, dass P_1', P_2' und P_3' auf einer Geraden liegen.
Zum anderen wird derselbe Fall im nächsten Kapitel dazu verwendet, um für die Gruppe der elliptischen Kurven die Assoziativität der Gruppenverknüpfung elegant zu beweisen.

Kapitel 2

Elliptische Funktionen und elliptische Kurven

2.1 Funktionentheoretische Grundlagen

Für die Theorie der elliptischen Funktionen bedarf es zunächst einiger funktionstheoretischer Grundlagen. Die Literaturquellen [5], [13] und [14] sind geeignet, um sich auf dem Gebiet der Funktionentheorie zu vertiefen.
Im Folgenden ist ein Gebiet eine offene zusammenhängende Untermenge von $\mathbb{C}$.
Eine in einem Gebiet $D \subset \mathbb{C}$ komplexwertige Funktion f heißt in einem Punkt $a \in D$ *holomorph* oder *analytisch*, wenn sie in jedem Punkt einer offenen Umgebung von a komplex differenzierbar ist. Funktionen, die in der ganzen komplexen Zahlenebene holomorph sind, werden als ganze Funktionen bezeichnet. Ganze Funktionen sind etwa polynomiale Abbildungen $z \mapsto \sum_{i=0}^{n} a_i z^i$ mit $a_i \in \mathbb{C}$, die Exponentialfunktion exp und die trigonometrischen Funktionen sin und cos.
In keinem $z \in \mathbb{C}$ holomorph sind dagegen die Betragsfunktion $z \mapsto |z|$, die Projektion auf den Realteil $z \mapsto \mathrm{Re}(z)$ bzw. auf den Imaginärteil $z \mapsto \mathrm{Im}(z)$ und die komplexe Konjugation $z \mapsto \overline{z} := \mathrm{Re}(z) - i \cdot \mathrm{Im}(z)$. Wir benötigen für die elliptischen Funktionen den Begriff der „Meromorphie“:

Definition. Eine in einem Gebiet D definierte Funktion
$f : D \to \overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ heißt *meromorph*, wenn

(1) $f^{-1}(\infty) \cap D$ diskret ist, d.h., keine Häufungspunkte besitzt,

(2) f in $D \setminus f^{-1}(\infty)$ analytisch ist,

(3) $f^{-1}(\infty)$ nur Pole enthält.

Man nennt $f(z) := \sum_{n=-\infty}^{\infty} a_n (z-a)^n$ die *Laurentreihe* zu einer meromorphen Funktion f im Punkt $a \in \mathbb{C}$ mit Koeffzizienten $a_n \in \mathbb{C}$ und $n \in \mathbb{Z}$. Die dritte Bedingung in obiger Definition bedeutet, dass für alle $a \in f^{-1}(\infty)$ in der Laurentreihe zu f gilt, dass $a_n \neq 0$ für endlich viele verschiedene $n < 0$.

Beispiele. Jede holomorphe Funktion ist meromorph, weil ihre Polstellenmenge leer ist. Für eine meromorphe Funktion $f \neq 0$ ist ihr Kehrwert $\frac{1}{f}$ ebenfalls meromorph.

Zudem sind rationale Funktionen und die beiden trigonometrischen Funktionen Tangens und Cotangens meromorph.

Weiters wird für eine Umgebung U von a, in der f holomorph ist, der Ausdruck

$$\mathrm{Res}(f;a) := a_{-1} = \frac{1}{2\pi i}\oint_{\partial U} f(\xi)d\xi$$

mit dem *Residuum von f in a* bezeichnet.
Laurentreihen sind wichtige Hilfsmittel der Funktionentheorie. Sie beschreiben komplexe Funktionen, die auf einem Kreisring holomorph sind, so wie Potenzreihen Funktionen beschreiben, die auf einer Kreisscheibe holomorph sind. Für genauere Ausführungen sei an dieser Stelle auf [5] p.144ff verwiesen. Von entscheidender Bedeutung ist folgender Residuensatz, der etwa in [5] p.163ff. bewiesen wird.

Satz 15 (Residuensatz)**.** *Die Funktion f sei in einem einfach zusamenhängenden Gebiet D analytisch bis auf endlich viele Punkte $a_1, \ldots, a_m$ innerhalb einer stückweise glatten geschlossenen Kurve ohne Selbstschnitte $\gamma \subset D \setminus \{a_1, \ldots, a_m\}$. Dann gilt:*

$$\int_\gamma f(\xi)d\xi = 2\pi i \sum_{j=1}^{m} Res(f;a_j).$$

Satz 16 (Liouville)**.** *Jede beschränkte ganze Funktion ist konstant.*

Beweis: Wir zeigen die Negation, also dass eine nichtkonstante ganze Funktion f nicht beschränkt sein kann. Aus der *Cauchy'schen Integralformel* von f in jedem $z \in \mathbb{C}$ (Beweis siehe [13] p.159ff oder [14] p.62f)

$$f'(z) = \frac{1}{2\pi}\oint_{|\xi - z| = r} \frac{f(\xi)}{(\xi - z)^2}d\xi,$$

die für jedes $r > 0$ gilt, folgt mittels Berechnung der Bogenlänge die Abschätzung

$$|f'(z)| \leq \frac{1}{2\pi} \cdot 2\pi r \cdot \frac{c}{r^2} = \frac{c}{r}.$$

Durch den Grenzübergang $r \to \infty$ ergibt sich somit $f'(z) = 0$ für jeden Punkt $z \in \mathbb{C}$, d.h. f ist konstant. □

Aus dem Satz von Liouville folgt unmittelbar der Fundamentalsatz der Algebra:

Satz 17 (Fundamentalsatz der Algebra)**.** *Jedes nichtkonstante Polynom besitzt eine Nullstelle.*

Beweis: Sei $P(z) := a_0 + a_1 z + \ldots + a_n z^n$, $a_i \in \mathbb{C}$, $0 \leq i \leq n$, $n \geq 1$, $a_n \neq 0$. Dann gilt $|P(z)| \to \infty$ für $|z| \to \infty$, d.h. zu jeder Zahl $c > 0$ existiert eine Zahl $r > 0$, sodass aus $|z| \geq r$ folgt, dass $|P(z)| \geq c$ gilt.
Angenommen, P hätte keine Nullstellen. Dann wäre $\frac{1}{P}$ eine beschränkte ganze Funktion, also konstant nach dem Satz von Liouville (Widerspruch). □

Drei weitere Beweise mittels der Mittelwertungleichung, des Cauchy'schen Integralsatz und des Minimumprinzips sind in [13] p.209f angeführt.
Eine Teilmenge $L \subset \mathbb{C}$ heißt *Gitter*, wenn es zwei $\mathbb{R}$-linear unabhängige Vektoren $w_1, w_2 \in \mathbb{C}$ gibt derart, dass

$$L = \mathbb{Z}w_1 + \mathbb{Z}w_2 = \{m_1w_1 + m_2w_2 \mid m_1, m_2 \in \mathbb{Z}\}.$$

Ferner nennt man die Punktmenge

$$\mathcal{F}{=}\mathcal{F}(w_1, w_2) = \{t_1w_1 + t_2w_2 \mid 0 \leq t_1, t_2 \leq 1\}$$

die *Grundmasche* des Gitters L bezüglich der Basis (w_1, w_2). Mit diesen Begriffen lassen sich nun die elliptischen Funktionen definieren.

Definition. Eine *elliptische Funktion* zum Gitter L ist eine meromorphe Funktion $f : \mathbb{C} \to \overline{\mathbb{C}}$ mit der Eigenschaft der doppelten Periodizität, d.h.,

$$f(z + \omega_1) = f(z + \omega_2) = f(z) \text{ für } \omega = (\omega_1, \omega_2) \in L \text{ und } z \in \mathbb{C}.$$

Die Menge der Polstellen $P(f)$ sowie die Menge der Nullstellen $N(f)$ einer elliptischen Funktion f sind periodisch, d.h., liegt $a \in P(f)$ bzw. $N(f)$, so folgt $a + w \in P(f)$ bzw. $N(f)$ für alle $w \in L$. Die Ordnung einer elliptischen Funktion f ist die Anzahl aller mit Vielfachheit gezählten Pole modulo L, d.h.

$$\operatorname{ord}(f) = -\sum_{a \in P(f)/L} \operatorname{ord}(f; a).$$

Weiters ist die b-Stellen-Ordnung einer elliptischen Funktion f, geschrieben $b\text{-ord}(f)$, die Anzahl der mit Vielfachheit gezählten Nullstellen der Funktion $f(z)-b$. Die nachfolgenden drei Liouville'schen Sätze charakterisieren die elliptischen Funktionen.

Satz 18 (1. Satz von Liouville)**.** *Jede elliptische Funktion ohne Pole ist konstant.*

Beweis: Zu jedem Punkt $z \in C$ existiert ein Gitterpunkt $w \in L$, sodass $z - w$ in der Grundmasche $\mathcal{F}$ liegt. Eine elliptische Funktion nimmt somit jeden ihrer Werte schon in $\mathcal{F}$ an. Jede stetige Funktion besitzt auf $\mathcal{F}$ ein Maximum, weil $\mathcal{F}$ beschränkt und abgeschlossen ist. Eine elliptische Funktion ohne Pole ist auf $\mathcal{F}$ und daher auf ganz $\mathbb{C}$ beschränkt. Nach dem Satz von Liouville muss sie folglich konstant sein. □

Satz 19 (2. Satz von Liouville)**.** *Eine elliptische Funktion f hat nur endlich viele Pole modulo $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ und die Summe der Residuen verschwindet, d.h.,*

$$\sum_{a \in P(f)} Res(f; a) = 0.$$

Beweis: Die Polmenge einer elliptischen Funktion ist diskret und geschnitten mit der kompakten Grundmasche $\mathcal{F}$ daher endlich. Also gibt es nur endlich viele Pole modulo L.
Wir wählen eine Translation von $\mathcal{F}$ um a mit der Bezeichnung

$$\mathcal{F}_a := a+\mathcal{F} = \{a+z; z \in \mathcal{F}\}$$

so, dass keine Pole auf dem Rand von $\mathcal{F}_a$ liegen. Wir berechnen nun die Residuensumme nach dem Residuensatz durch Integration längs des Randes dieser modifizierten Grundmasche $\partial\mathcal{F}_a$:

$$2\pi i \sum_{b\in\mathcal{F}_a} \operatorname{Res}(f;b) = \int_{\partial\mathcal{F}_a} f$$

$$= \int_a^{a+w_1} f(\xi)d\xi + \int_{a+w_1}^{a+w_1+w_2} f(\xi)d\xi + \int_{a+w_1+w_2}^{a+w_2} f(\xi)d\xi + \int_{a+w_2}^{a} f(\xi)d\xi = 0.$$

□

Der zweite Liouville'sche Satz besagt also, dass die Polstellenmenge einer elliptischen Funktion modulo L nicht aus einem einzigen Pol erster Ordnung bestehen kann, weil das Residuum eines Pols erster Ordnung stets von Null verschieden ist. Zusammen mit dem ersten Liouville'schen Satz folgt somit, dass eine nichtkonstante elliptische Funktion mindestens Ordnung zwei besitzen muss.

Satz 20 (3. Satz von Liouville)**.** *Für eine nichtkonstante elliptische Funktion f gilt:*

$$\operatorname{ord}(f) = b - \operatorname{ord}(f) \text{ für alle } b \in \overline{\mathbb{C}}.$$

Beweis: An dieser Stelle sei auf [5] p.258f verwiesen. □

Eine nichtkonstante elliptische Funktion nimmt daher auf $\mathbb{C}/L$ jeden mit Vielfachheit gezählten Wert gleich oft an. Insbesondere hat f modulo L gleich viele Null- und Polstellen.

2.2 Die Weierstraß'sche $\wp$-Funktion

Es wird jetzt eine spezielle elliptische Funktion eingeführt, die sogenannte Weierstraß'sche $\wp$-Funktion. Wir werden sehen, dass sie dem Körper der elliptischen Funktionen eine Struktur verleit und insbesondere aus der $\wp$-Funktion alle anderen elliptischen Funktionen auf konstruktive Weise gewonnen werden können.

Definition. Die durch

$$\wp(z;L) = \wp(z) = \begin{cases} \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] & \text{für } z \notin L, \\ \\ \infty & \text{für } z \in L \end{cases}$$

definierte Funktion heißt *Weierstraß'sche $\wp$-Funktion* zum Gitter L. Ferner nennt man die Reihen

$$G_n := \sum_{w\in L\setminus\{0\}} w^{-n}$$

für $n \in \mathbb{N}$ und $n \geq 3$ *Eisensteinreihen.*

Die Weierstraß'sche $\wp$-Funktion zum Gitter L ist in ganz $\mathbb{C}$ meromorph, hat Pole zweiter Ordnung in den Gitterpunkten und ist außerhalb von L analytisch. Ferner stellt sie eine gerade Funktion dar, d.h. $\wp(z) = \wp(-z)$. Hinsichtlich der genauen Begründung der absoluten Konvergenz der $\wp$-Funktion sei auf [5] S.262ff verwiesen.

Satz 21. *Die Weierstraß'sche $\wp$-Funktion lässt sich in der größten offenen Kreisscheibe um 0, die keinen von 0 verschiedenen Gitterpunkt enthält, folgendermaßen schreiben:*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2(n+1)} z^{2n}.$$

Beweis: Wir bestimmen die Laurentreihe der Weierstraß'schen $\wp$-Funktion um den Entwicklungspunkt $z_0 = 0$:

$$\wp(z) = \frac{1}{z^2} + \sum_{n=0}^{\infty} a_{2n} z^{2n}.$$

Die Koeffizienten aus der Taylor'schen Formel für die Funktion $f(z) := \wp(z) - \frac{1}{z^2}$ lauten $a_0 = 0$ und $a_{2n} = \frac{f^{(2n)}(0)}{(2n)!}$. Im Fall $n > 1$ ergibt sich durch Induktion über n, dass

$$f^{(n)}(z) = (-1)^n (n+1)! \sum_{\omega \in L \setminus \{0\}} \frac{1}{(z-\omega)^{n+2}}$$

gilt. Wir erhalten somit

$$a_{2n} = \frac{(2n+1)!}{(2n)!} \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^{2(n+1)}}.$$

□

Die Ableitung der $\wp$-Funktion

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}$$

hat Pole dritter Ordnung in den Gitterpunkten und ist außerhalb von L analytisch. Ferner ist sie ungerade, d.h., $\wp'(-z) = -\wp'(z)$.

Satz 22. *Die Weierstraß'sche $\wp$-Funktion ist eine elliptische Funktion der Ordnung zwei. Ihre Ableitung ist eine elliptische Funktion der Ordnung drei.*

Beweis: Die Ableitung der $\wp$-Funktion ist doppeltperiodisch, d.h., $\wp'(z+\omega_0) = \wp'(z)$ für $\omega_0 \in L$. Daher ist $\wp(z+\omega_0) - \wp(z)$ konstant für $\omega_0 \in L$. Sei o.B.d.A. ω_0 eines der beiden Basiselemente des Gitters L. Wir setzen $z := -\frac{1}{2}\omega_0$ und erhalten den konstanten Wert $\wp(-\frac{1}{2}\omega_0 + \omega_0) - \wp(-\frac{1}{2}\omega_0) = \wp(\frac{1}{2}\omega_0) - \wp(-\frac{1}{2}\omega_0) = 0$, weil $\wp$ eine gerade Funktion ist. □

Lemma. *Ein Punkt $a \in \mathbb{C}$ ist genau dann eine Nullstelle von $\wp'$, wenn $a \notin L$ und $2a \in L$ gilt. Weiters gibt es genau drei einfache Nullstellen von $\wp'$.*

Beweis: Mit der angeführten Eigenschaft von a gilt

$$\wp'(a) \overset{\wp' \text{ elliptisch}}{=} \wp'(a-2a) = \wp'(-a) \overset{\wp' \text{ ungerade}}{=} -\wp'(a)$$

und daher $\wp'(a) = 0$. Die drei komplexen Werte $\frac{w_1}{2}$, $\frac{w_2}{2}$ und $\frac{w_1+w_2}{2}$ sind modulo L paarweise verschiedene Nullstellen von $\wp'$. Nach dem dritten Liouville'schen Satz kann es keine weitere Nullstelle geben und somit sind diese drei Nullstellen einfach. □

Wir nennen

$$e_1 := \wp(\tfrac{w_1}{2}),\ e_2 := \wp(\tfrac{w_2}{2}),\ e_3 := \wp(\tfrac{w_1+w_2}{2})$$

die Halbwerte der $\wp$-Funktion.

2.3 Der Körper der elliptischen Funktionen

Summe, Differenz, Produkt und Quotient zweier elliptischer Funktionen bezüglich des Gitters L sind elliptische Funktionen. Die Menge der elliptischen Funktionen bezüglich eines festen Gitters L bildet also einen Körper mit der Bezeichnung $K(L)$. Ziel dieses Kapitels ist, die Struktur von $K(L)$ zu bestimmen.
Sei nun $f \in K(L)$ eine elliptische Funktion und

$$P(w) := a_0 + a_1 w + \ldots + a_m w^m$$

ein Polynom. Dann ist auch $P(f)$ eine elliptische Funktion.
Sei allgemeiner $R(z)$ eine rationale, also meromorphe Funktion. Dann lässt sie sich als Quotient zweier Polynome P und Q folgendermaßen darstellen:

$$R = \frac{P}{Q}, Q \neq 0.$$

Die elliptische Funktion $\frac{P(f)}{Q(f)}$ ist von der Wahl der Darstellung von R unabhängig, d.h., aus $R(f) = \tilde{R}(f)$ folgt $R = \tilde{R}$. Ist f eine nichtkonstante elliptische Funktion, so definiert mit anderen Worten die Zuordnung $R \mapsto R(f)$ einen Isomorphismus vom Körper der rationalen Funktionen $\mathbb{C}(z)$ auf den Unterkörper von $K(L)$

$$\mathbb{C}(f) := \{g \in K(L);\ g = R(f) \text{ für eine rationale Funktion } R\}.$$

Sei ab jetzt f eine nichtkonstante elliptische Funktion zum Gitter L. Dann gibt es Fallunterscheidungen hinsichtlich der Struktur von f:

(1) f gerade mit Polen nur in L:

Satz 23. *Es sei f eine gerade elliptische Funktion der Ordnung $2n$, deren Polstellenmenge in L enthalten ist. Dann gibt es ein Polynom P vom Grad $n = \frac{\text{ord(f)}}{2}$ derart, dass $f = P(\wp)$.*

Beweis: Weil f nichtkonstant ist, muss sie einen Pol in einem Gitterpunkt und somit in 0 haben. Da ferner f gerade ist, treten in der Laurentreihe von f nur gerade Potenzen auf, d.h.,

$$f(z) = a_{-2n}z^{-2n} + a_{-2(n-1)}z^{-2(n-1)} + \dots.$$

Wegen

$$\wp(z)^n = z^{-2n} + \sum_{k=1}^{\infty} c_{2k}z^{2k}$$

erhalten wir mit

$$g_1 := f - a_{-2n}\wp^n$$

wiederum eine gerade elliptische Funktion mit Polstellenmenge in L. Die Ordnung von g_1 ist kleiner gleich $2(n-1)$ und daher echt kleiner als die Ordnung von f. Wiederholen wir diese Operation, so ergibt sich nach n Schritten

$$g_n(z) = f(z) - \sum_{k=1}^{n} a_k\wp^k(z) = a_0.$$

Damit gilt

$$f(z) = \sum_{k=0}^{n} a_k\wp^k(z) = P(\wp)(z).$$

□

(2) f gerade mit Polen auch außerhalb von L:

Satz 24. *Jede gerade elliptische Funktion ist als rationale Funktion in der Weierstraß'schen $\wp$-Funktion darstellbar.*

Beweis: Sei f eine nichtkonstante gerade elliptische Funktion und a ein Pol von f, der außerhalb von L liegt. Für genügend großes n ist die Funktion

$$z \mapsto \big(\wp(z) - \wp(a)\big)^n f(z)$$

nach a analytisch fortsetzbar. Da f modulo L nur endlich viele Pole hat, gibt es endlich viele Punkte $a_j \in \mathbb{C} \setminus L$ und natürliche Zahlen n_j für $1 \le j \le m$ derart, dass

$$g(z) = f(z)\prod_{j=1}^{m}\big(\wp(z) - \wp(a_j)\big)^{n_j}$$

außerhalb von L keine Pole hat. Folglich ist $g(z)$ ein Polynom in $\wp(z)$. □

Korollar. *Die Weierstraß'sche $\wp$-Funktion zum Gitter $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ mit den drei Halbwerten $e_1 = \wp(\frac{w_1}{2})$, $e_2 = \wp(\frac{w_2}{2})$ und $e_1 = \wp(\frac{w_1+w_2}{2})$ genügt der Differentialgleichung*

$$\wp'^2 = 4\big(\wp(z) - e_1\big)\big(\wp(z) - e_2\big)\big(\wp(z) - e_3\big).$$

Beweis: Weil $\wp'(z)$ ungerade ist, ist $\wp'^2(z)$ gerade und hat doppelte Nullstellen bei e_1, e_2 und e_3. Nach Satz **??** und dem Fundamentalsatz der Algebra (Satz **??**) erhalten wir

$$\wp'^2(z) = c\big(\wp(z) - e_1\big)\big(\wp(z) - e_2\big)\big(\wp(z) - e_3\big)$$

für eine Konstante c. Um c zu erhalten, vergleicht man die Koeffizienten größter Ordnung in den Laurentreihen im Ursprung.
Der Leitterm der Laurentreihe von $\wp'^2(z)$ im Ursprung lautet $(-2z^{-3})^2 = 4z^{-6}$ und von der rechten Seite obiger Gleichung $c(z^{-2})^3 = cz^{-6}$, d.h., $c = 4$. Somit genügt $\wp(z)$ der Differentialgleichung $\wp'^2(z) = f\big(\wp(z)\big)$, wobei

$$f(x) = 4(x - e_1)(x - e_2)(x - e_3) \in \mathbb{C}[x].$$

□

(3) f ungerade:

Satz 25. *Jede ungerade elliptische Funktion ist das Produkt einer geraden elliptischen Funktion und der ungeraden Funktion $\wp'$.*

Beweis: $\frac{f}{\wp'}$ ist gerade in $K(L)$ und somit nach Satz **??** als rationale Funktion von $\wp$ darstellbar, d.h., $f = \wp' \cdot R(\wp)$. □

Satz 26. *Sei f eine elliptische Funktion. Dann existieren rationale Funktionen R und S, sodass*

$$f = R(\wp) + \wp' S(\wp)$$

gilt, d.h.,

$$K(L) = \mathbb{C}(\wp) + \mathbb{C}(\wp)\wp'.$$

Beweis: Jede elliptische Funktion lässt sich als Summe einer geraden und einer ungeraden elliptische Funktion schreiben:

$$f(z) = \frac{1}{2}\big(f(z) + f(-z)\big) + \frac{1}{2}\big(f(z) - f(-z)\big).$$

Mit $f(z)$ ist nämlich auch $f(-z)$ eine elliptische Funktion. Die Sätze **??** und **??** implizieren die gewünschte Behauptung. □

2.4 Die Weierstraß'sche Normalform

Die $\wp$-Funktion genügt einer Differentialgleichung, die in Satz **??** (siehe hinten) bewiesen wird. Aus jener Differentialgleichung geht hervor, dass die Umkehrung der $\wp$-Funktion ein sogenanntes elliptisches Integral erster Gattung ist. Unter einem *elliptischen Integral erster Gattung* verstehen wir ein Integral $\int_a^z \frac{dt}{\sqrt{P(t)}}$, wobei P ein Polynom dritten oder vierten Grades ohne mehrfache Nullstelle ist.

Satz 27. *Zu jedem Polynom $P(t)$ dritten oder vierten Grades ohne mehrfache Nullstelle existiert eine nichtkonstante elliptische Funktion f mit folgender Eigenschaft:* $(*)$ *Ist $D \subset \mathbb{C}$ eine offene Teilmenge, auf welcher f invertierbar ist, und ist $g : f(D) \to \mathbb{C}$ die Umkehrfunktion von f, so gilt*

$$g'(z) = \frac{1}{\sqrt{P(z)}}.$$

Beweis: [5] p.287f. □

Die Reduktion von Polynomen dritten oder vierten Grades auf Polynome dritten Grades ohne quadratischen Term liefert für $g_2 = 60G_4$ und $g_3 = 140G_6$ die *Weierstraß'sche Normalform*:

$$P(t) = 4t^3 - g_2 t - g_3.$$

Dieses Polynom hat genau dann keine mehrfache Nullstelle, wenn die Diskriminante $\mathrm{Res}_{P,P'} = g_2^3 - 27g_3^2$ von Null verschieden ist. Weiters existiert zu je zwei komplexen Zahlen g_2 und g_3 mit $g_2^3 - 27g_3^2$ ein Gitter $L \subset \mathbb{C}$ mit der Eigenschaft $g_2 = g_2(L)$ und $g_3 = g_3(L)$. Für die Reduktion auf die Weierstraß'sche Normalform und den Beweis der letzten Behauptung sei auf [5] p.288 und p.318f verwiesen.

Satz 28. *Sei $L \subset \mathbb{C}$ ein Gitter. Falls $P(t) = 4t^3 - g_2 t - g_3$, $g_2 = g_2(L)$ und $g_3 = g_3(L)$, so hat die Weierstraß'sche $\wp$-Funktion $f(z) := \wp(z)$ zum Gitter L die in letztem Satz angegebene Eigenschaft* $(*)$.

Beweis: Aus der algebraischen Differentialgleichung der $\wp$-Funktion $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ ergibt sich für die in $t \in \mathbb{C}$ mit $P(t) \neq 0$ definierte lokale Umkehrfunktion g von $\wp$

$$g'(t)^2 = \frac{1}{\wp'\big(g(t)\big)^2} = \frac{1}{4\wp^3\big(g(t)\big) - g_2\wp\big(g(t)\big) - g_3} = \frac{1}{P(t)}.$$

□

Die eben im Beweis verwendete Differentialgleichung wird im letzten Unterkapitel in Bezug auf elliptische Kurven bewiesen.

2.5 Gruppenoperationen auf elliptischen Kurven

Als Literatur für die Theorie der elliptischen Kurven ist [3], [4] und [11] geeignet. Die *Charakteristik* eines Körpers K ist definiert als

$$\mathrm{char}(K) := \min\{n \in \mathbb{N} \mid n \cdot 1_K = 0\}.$$

Notwendigerweise ist $\mathrm{char}(K)$ eine Primzahl. Für jede Primzahl p ist beispielsweise $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ ein Körper der Charakteristik p. $\mathbb{C}$, $\mathbb{R}$ und $\mathbb{Q}$ haben die Charakteristik 0.

Betrachten wir die Kurve $y^2 = x^3 - x$ über einem Körper K. Sie ist nur dann wohldefiniert, wenn $\mathrm{char}(K) \neq 2$. Die partiellen Ableitungen von einem Polynom $F := x^3 - x - y^2$ über einem Körper K mit $\mathrm{char}(K) \neq 2$ lauten $\frac{\partial F}{\partial x} = 3x^2 - 1$ und

$\frac{\partial F}{\partial y} = -2y$. Für singuläre Punkte muss also $y = 0$ und $x = \pm\frac{1}{\sqrt{3}}$ gelten. Diese beiden Punkte liegen nicht auf der Kurve. Ist jedoch $\mathrm{char}(K) = 2$, so ist $\frac{\partial F}{\partial y} = 0$ für alle y, und somit ist der Punkt $(0, 0)$ singulär. Sei allgemein $f(x) \in K[x]$ eine Kubik und $y^2 - f(x) = 0$ die Gleichung einer Kurve C. In einem Punkt $(x_0, y_0) \in K \times K$ erhalten wir die beiden partiellen Ableitungen $-f'(x_0)$ und $2y_0$. Falls K kein Körper der Charakteristik zwei ist, verschwinden sie beide genau dann, wenn $y_0 = 0$ und x_0 eine mehrfache Nullstelle von $f(x)$ ist. Folglich ist C genau dann nicht-singulär, wenn die Nullstellen von $f(x)$ paarweise verschieden sind.

Definition. Eine *elliptische Kurve* C über einem Körper K ist eine nicht-singuläre ebene projektive Kurve vom Grad drei.

Beispiel 2.1. Die Fermat-Kurve $x_0^3 + x_1^3 + x_2^3 = 0$ in $\mathbb{P}_2(K)$ ist elliptisch. Die dazu gehörige Hesse-Kurve ist gegeben durch $x_0x_1x_2 = 0$. Die Wendepunkte der Fermat-Kurve sind

$$(1, \xi, 0),\ (1, 0, \xi),\ (0, 1, \xi),$$

wobei ξ eine Lösung der Gleichung $x^3 + 1 = 0$ ist.

Seien nun E eine elliptische Kurve und Θ ein willkürlich gewählter Punkt in E. Sei ferner $A * B$ der dritte Schnittpunkt mit E auf der Geraden durch A und B. Nach dem Satz von Bézout (siehe Kapitel 1) existiert zu A und B genau ein weiterer Schnittpunkt $A * B$ auf E und der Geraden durch A und B. Dieser kann aber gleich A und/oder B sein, falls die Schnittvielfachheit im jeweiligen Punkt zwei oder drei beträgt. Wir definieren nun die Addition zweier Punkte A und B in E folgendermaßen:

$$E \times E \to E,\ (A, B) \mapsto A + B := \Theta(A * B),$$

d.h., $A+B$ ist der dritte Schnittpunkt auf der Geraden durch Θ und $A*B$. Wiederum wenden wir den Satz von Bézout auf den Schnitt von E mit der Geraden durch Θ und $A * B$ an. Gilt speziell $A = B$, so ist $A * A$ der Schnitt der Tangente an A mit E. Da E nicht-singulär ist, gibt es genau eine Tangente in A. Damit ist die Addition auf elliptischen Kurven wohldefiniert.

Satz 29. *$(E, +)$ ist eine Abel'sche Gruppe mit dem neutralen Element Θ.*

Beweis: (1) Für beliebiges $A \in E$ ist Θ wegen $A + \Theta = \Theta(A * \Theta) = A$ das neutrale Element. Die Addition ist kommutativ.

(2) Die Inverse von A lautet $-A = A(\Theta * \Theta)$, weil

$$A + (-A) = \Theta\big(A * (-A)\big) = \Theta(\Theta * \Theta) = \Theta.$$

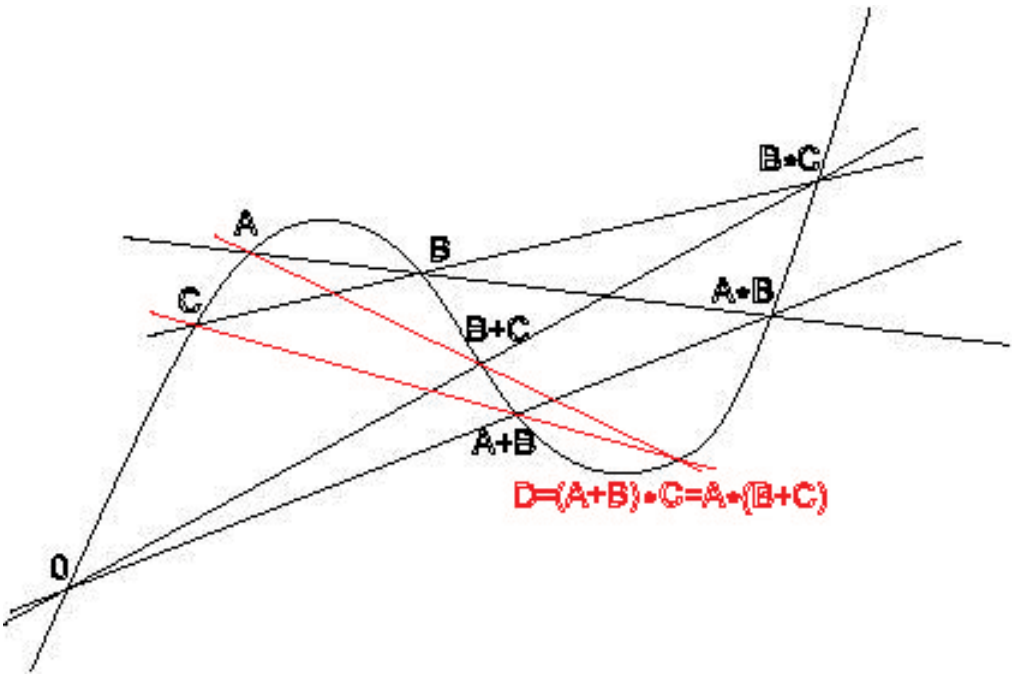
(3) Die Verifikation der Assoziativität ist komplizierter. Man braucht dazu einen Spezialfall des Satzes von Cayley-Bacharach (Satz **??**).
Seien A, B, C Punkt auf der elliptischen Kurve E. Für die zu beweisende Behauptung $(A + B) + C = A + (B + C)$ ist es ausreichend zu zeigen, dass

$$(A + B) * C = A * (B + C),$$

d.h., der Schnittpunkt D der beiden Geraden durch $A+B$ und C bzw. A und $B+C$ liegt auf E. Wir erhalten zwei je aus drei Geraden bestehende Kubiken $C_1 := g(A,B) \cup g(A+B,C) \cup g(\Theta, B*C)$ und $C_2 := g(B,C) \cup g(A,B+C) \cup g(\Theta, A*B)$, die sich in folgenden Punkten schneiden:

$$C_1 \cap C_2 = \{\Theta, A, B, C, A*B, A+B, B*C, B+C, D\},$$

d.h., $\#(C_1 \cap C_2) = 9$. Die nachfolgende Skizze soll die Situation veranschaulichen:



Nach Konstruktion geht E durch acht der neun Schnittpunkte, nämlich durch $(C_1 \cap C_2) \setminus D$. Nach dem Satz von Cayley-Bacharach muss E somit auch durch D gehen. □

Definition. Angenommen, eine elliptische Kurve E ist über einem Unterkörper $K_0 \subset K$ definiert. Dann nennen wir $E(K_0)$ die Menge der K_0-*rationalen* Punkte auf E.

Falls Θ in $E(K_0)$ liegt, so sind für $A, B \in E(K_0)$ ebenso $A+B \in E(K_0)$ und $-A \in E(K_0)$. Somit ist $\big(E(K_0), +\big)$ eine Untergruppe von $(E,+)$.
Insbesondere ist für eine elliptische Kurve E über $\mathbb{Q}$ die Menge der rationalen Punkte von E eine Untergruppe von $(E,+)$. Nach dem *Theorem von Mordell-Weil* ist diese Gruppe endlich erzeugt (siehe [4] p.64-88).

Satz 30. *Seien E eine elliptische Kurve, Θ das neutrale Element der Gruppe $(E,+)$ und A, B, C drei Punkte auf $L \cap E$ für eine beliebige Gerade L. Dann ist Θ genau dann ein Wendepunkt, wenn*

$$A+B+C = \Theta$$

gilt.

Beweis: Das neutrale Element Θ ist genau dann ein Wendepunkt, wenn die Tangente an E durch Θ die elliptische Kurve E mit Vielfachheit drei schneidet. Nach dem Satz von Bézout kann es keinen weiteren Schnittpunkt dieser Tangente mit E geben und damit gilt $\Theta * \Theta = \Theta$. Die Behauptung folgt aus einer elementaren Umformung:

$$A + B + C = \Theta(A * B) + C = \Theta\big(\Theta(A * B) * C\big) = \Theta * \Theta.$$

□

2.6 Klassifikation von elliptischen Kurven

Wir betrachten bei der Klassifikation elliptischer Kurven Körper, die weder Charakteristik zwei noch drei besitzen. Für letztere Fälle sei auf [3] verwiesen.

Falls Q ein Wendepunkt einer elliptischen Kurve E ist, so kann das Koordinatensystem derart gewählt werden, dass $Q = (0, 0, 1)$ und $x_0 = 0$ die Wendetangente an E in Q ist. In jenem Koordinatensystem hat E eine Gleichung der Form

$$F := a_0 x_2^3 + a_1 x_2^2 + a_2 x_2 + a_3 = 0, \ (\star)$$

wobei $a_i \in K[x_0, x_1]$ homogene Polynome vom Grad i für $0 \leq i \leq 3$ sind. Wegen $Q = (0, 0, 1) \in E$ muss $a_0 = 0$ gelten. Dehomogenisierung hinsichtlich x_2 liefert die affine Gleichung

$$a_1(x_1, x_2) + a_2(x_1, x_2) + a_3(x_1, x_2) = 0.$$

Weil $x_0 = 0$ die Tangente von E in Q ist, lässt sich $a_1 = cx_1$ für $0 \neq c \in K$ schreiben. Sei o.B.d.A. $c = 1$. Aus $\mu_Q(E, x_0) = 3$ folgt, dass x_1 Teiler von a_2. Also hat die Gleichung $(\star)$ für $\alpha, \beta \in K$ die Form

$$x_0 x_2^2 + x_0(\alpha x_0 + \beta x_1)x_2 + a_3(x_0, x_1) = 0.$$

Durch Verwenden der linearen Transformation

$$x_2 \mapsto x_2 - \tfrac{1}{2}(\alpha x_0 + \beta x_1),\ x_1 \mapsto x_1,\ x_0 \mapsto x_0$$

erhalten wir die Gleichung

$$x_0 x_2^2 + a_3(x_0, x_1) = 0.$$

Es darf x_0 nicht a_3 teilen, weil ansonsten die Wendetangente in Q eine Komponente von E wäre. Folglich kann die letzte Gleichung für $a, b, c \in K$ in folgende Gleichung umgeschrieben werden:

$$F := x_0 x_2^2 - (x_1 - ax_0)(x_1 - bx_0)(x_1 - cx_0) = 0. \ (\Delta)$$

Die drei Koeffizienten a, b, c sind verschieden. Wären sie nämlich gleich, so hätte E bei $(1, a, 0)$ eine Singularität, was man unmittelbar an den partiellen Ableitungen $\frac{\partial F}{\partial x_0} = 3abcx_0^2 + (a + b + c)x_1^2 + x_2^2 - 2(ab + ac + bc)x_0 x_1$, $\frac{\partial F}{\partial x_1} = -(ab + ac + bc)x_0^2 - 3x_1^2 + 2(a + b + c)x_0 x_1$ und $\frac{\partial F}{\partial x_2} = 2x_0 x_2$ erkennt.

Die Polare $P_Q(F)$ von E bezüglich Q ist durch $\frac{\partial F}{\partial x_2} = 2x_0x_2 = 0$ gegeben. Sie besteht aus der unendlich fernen Geraden $x_0 = 0$ und der affinen x_1-Achse. Die Polare schneidet die Kurve E zusätzlich zum Punkt Q in den Punkten mit den affinen Koordinaten $(a, 0)$, $(b, 0)$, $(c, 0)$. Diese sind also die Berührpunkte derjenigen Tangenten von Q an E, die von der Wendetangente verschieden sind. Damit ist der folgende Satz gezeigt.

Satz 31. *Ist Q ein Wendepunkt einer elliptischen Kurve E, dann gibt es neben der Wendetangente genau drei weitere Tangenten an E, die durch Q gehen. Die Berührpunkte dieser Tangenten sind kollinear.*

Indem wir auf die Gleichung (Δ) die Substitution

$$x_0' = (b-a)x_0,\ x_1' = x_1 - ax_0,\ x_2' = (\sqrt{b-a})^{-1} \cdot x_2$$

anwenden, erhalten wir die nächste Gleichung

$$x_0'x_2'^2 - x_1'(x_1' - x_0')(x_1' - \lambda x_0') = 0 \text{ mit } \lambda := \frac{c-a}{b-a} \neq 0, 1. \ (\star\star)$$

Wir bezeichnen eine elliptische Kurve E in der Form von $(\star\star)$ zu einem $\lambda \neq 0, 1$ mit E_λ. Mit obigen Umformungen ist der folgende Satz bewiesen.

Satz 32. *Jede elliptische Kurve E_λ für $\lambda \in K \setminus \{0, 1\}$ ist in einem geeigneten Koordinatensystem durch die Gleichung*

$$x_0x_2^2 - x_1(x_1 - x_0)(x_1 - \lambda x_0) = 0$$

gegeben.

Lemma. *Sind A und B zwei Wendepunkte einer elliptischen Kurve E, so existiert eine Koordinatentransformation φ in $\mathbb{P}_2(K)$ mit $\varphi(E) = E$ und $\varphi(A) = B$.*

Beweis: O.B.d.A. sei $A \neq B$. Die Punkte A und B sind zu einem dritten Wendepunkt P kollinear. Wir wählen wie oben den Punkt im Unendlichen $P = (0, 0, 1)$ und schreiben die Gleichung von E in der Form von $(\star\star)$. Die dazugehörige affine Gleichung lautet

$$y^2 - x(x-1)(x-\lambda) = 0. \ (\bullet)$$

Die Gerade durch A und B mit der Bezeichnung $g(A, B)$ ist parallel zur x_2-Achse, weil sie P enthält. Die Gleichung $(\bullet)$ ist bezüglich der Substitution $x_2 \mapsto -x_2$ invariant und $g(A, B)$ wird auf sich selbst abgebildet. Weil Wendepunkte auf Wendepunkte abgebildet werden, werden die Punkte A und B durch die Substitution vertauscht. □

Satz 33. *Eine elliptische Kurve E_λ lässt sich genau dann anhand einer Koordinatentransformation auf eine weitere elliptische Kurve $E_{\overline{\lambda}}$ abbilden, wenn*

$$\overline{\lambda} \in M_\lambda := \{\lambda, \lambda^{-1}, 1-\lambda, (1-\lambda)^{-1}, \lambda(\lambda-1)^{-1}, (\lambda-1)\lambda^{-1}\}.$$

Beweis: [11] p.95. □

Definition. Zwei elliptische Kurven E_λ und $E_{\overline{\lambda}}$ heißen projektiv äquivalent, falls sich E_λ durch eine Koordinatentransformation auf $E_{\overline{\lambda}}$ abbilden lässt.

Die durch

$$j(\lambda) := \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

für $\lambda \neq 0, 1$ gegebene Funktion j ist invariant bezüglich den Substitutionen

$$\lambda \mapsto \lambda,\ \lambda \mapsto \lambda^{-1},\ \lambda \mapsto 1 - \lambda.$$

Infolgedessen ist j eine Invariante der Klasse aller zu E_λ projektiv äquivalenten Kurven. Wir setzen $j(E) := j(\lambda)$ für alle elliptischen Kurven E in der Klasse von E_λ.

Definition. Man nennt $j(E)$ die j-Invariante einer elliptischen Kurve E.

Satz 34. *Für jedes $a \in K$ existiert bis auf projektive Äquivalenz genau eine elliptische Kurve E mit $j(E) = a$.*

Beweis: Für jedes $a \in K$ hat die Gleichung

$$(\lambda^2 - \lambda + 1)^3 - a\lambda^2(\lambda - 1)^2 = 0\ (\circ)$$

eine Lösung $\lambda_0 \neq 0, 1$, und alle Elemente von M_{λ_0} sind ebenso Lösungen. Es gilt $j(E_{\lambda_0}) = a$, und jedes λ_0' mit $j(E_{\lambda_0'}) = a$ löst $(\circ)$. Falls M_{λ_0} aus sechs verschiedenen Werten besteht, so sind sie alle Lösungen jener Gleichung vom Grad sechs und wir sind fertig. Falls sich M_{λ_0} aus weniger als sechs Elementen zusammensetzt, so gibt es nur folgende zwei Fälle:

$$M_{-1} = M_{\frac{1}{2}} = M_2 = \{-1, \tfrac{1}{2}, 2\},$$

$$M_p = M_{p^{-1}} = \{p, p^{-1}\}, \text{ wobei } p := \tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}.$$

Im ersten Fall beträgt $a = \frac{27}{4}$, im zweiten Fall $a = 0$. In beiden Fällen umfasst M_{λ_0} alle Lösungen von $(\circ)$. □

Die elliptischen Kurven lassen sich damit folgendermaßen klassifizieren: Die j-Invariante bildet die projektiven Äquivalenzklassen elliptischer Kurven bijektiv auf den Körper K ab.

2.7 Parametrisierung elliptischer Kurven durch elliptische Funktionen

Ziel ist es nun, die Koeffizienten $a, b, c, d \in \mathbb{C}$ einer Kubik $f(x) = ax^3 + bx^2 + cx + d$ ohne mehrfache Nullstellen zu finden, sodass die Gleichung

$$\wp'(z) = a\wp^3(z) + b\wp^2(z) + c\wp(z) + d$$

erfüllt ist. Für Details sei im Voraus auf [12] p.25f verwiesen. Aus Satz **??** ergeben sich die Laurentreihen von $\wp(z)$, $\wp^2(z)$, $\wp^3(z)$, $\wp'(z)$ und $\wp'^2(z)$ im Ursprung wie folgt:

$$\begin{array}{rcl}
\wp(z) & = & \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \ldots, \\
\wp'(z) & = & -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \ldots, \\
\wp'^2(z) & = & \frac{4}{z^6} - \frac{24}{z^2} G_4 - 80G_6 + (36G_4^2 - 168G_8) z^2 + \ldots, \\
\wp^2(z) & = & \frac{1}{z^4} + 6G_4 + 10G_6 z^2 \ldots, \\
\wp^3(z) & = & \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2) z^2 + \ldots.
\end{array}$$

Eine aufwändige Rechnung liefert

$$\wp'^2(z) - 4\wp^3(z) + 60G_4\wp(z) = -140G_6 + (108G_4^2 - 252G_8)z^2 + \ldots$$

Die linke Seite dieser Gleichung ist eine elliptische Funktion ohne Pole, also nach dem ersten Satz von Liouville konstant. Durch Einsetzen von $z = 0$ ergibt sich die Konstante $-140G_6$. Mit der üblichen Schreibweise

$$g_2 = g_2(L) := 60G_4 \text{ und}$$

$$g_3 = g_3(L) := 140G_6$$

erhalten wir als Resultat jener Rechnungen folgenden Satz:

Satz 35. *Die Weierstraß'sche $\wp$-Funktion genügt der Differentialgleichung $\wp'^2(z) = f\big(\wp(z)\big)$, wobei*

$$f(x) = 4x^3 - g_2 x - g_3 \in \mathbb{C}[x].$$

Diese Differentialgleichung lässt sich folgendermaßen geometrisch interpretieren. Wir betrachten die Einbettung

$$(\star)\ \mathbb{C}/L \to \mathbb{P}^2_{\mathbb{C}},\ z \mapsto \begin{cases} \big(1 : \wp(z) : \wp'(z)\big) & \text{für } z \neq 0, \\ (0, 1, 0) & \text{für } z = 0. \end{cases}$$

Das Bild eines beliebigen Punktes $0 \neq z \in \mathbb{C}/L$ ist ein Punkt in der xy-Ebene mit komplexen Koordinaten, dessen x- und y-Koordinaten wegen Satz **??** die Gleichung $y^2 = f(x)$ erfüllen. Für jeden x-Wert mit der Ausnahme von e_1, e_2, e_3 und ∞ existieren genau zwei verschiedene Punkte $z_1, z_2 \in \mathbb{C}/L$ mit $\wp(z_1) = \wp(z_2) = x$. Für $i = 1, 2$ ergibt sich $\wp'(z_i) = \pm\sqrt{f(\wp(z_i))} = \pm\sqrt{f(x)}$. Falls x eine Nullstelle von $f(x)$ ist, so existiert nur ein Punkt $z \in \mathbb{C}/L$ mit $\wp(z) = x$, und die dazugehörige y-Koordinate ist $y = \wp'(z) = 0$. Damit ist folgender Satz gezeigt:

Satz 36. *Die Abbildung* $(\star)$ *ist ein Isomorphismus zwischen* $\mathbb{C}/L$ *und der elliptischen Kurve* $y^2 = 4x^3 - g_2(L)x - g_3(L)$ *in* $\mathbb{P}_2(\mathbb{C})$.

Es gilt nach Satz **??**, dass jede elliptische Funktion als rationaler Ausdruck in $\wp(z)$ und $\wp'(z)$ darstellbar ist. Algebraisch ergibt sich zusammen mit Satz **??**, dass der Körper der elliptischen Funktionen $K(L)$ isomorph ist zu

$$\mathbb{C}(x)[y]/\langle y^2 - (4x^3 - g_2x - g_3)\rangle.$$

Kapitel 3

Reelle Nullstellen von Polynomen

Ziel dieses Kapitels ist, die Anzahl der Lösungen eines Polynoms ohne Vielfachheit in einer Variablen gegebenfalls mit Nebenbedingungen in einem reell abgeschlossenen Körper R zu bestimmen. Als ergänzende Literatur ist [16], Kapitel I.3 und [18], Kapitel VII, §54 zu empfehlen. In Ermangelung von Quellen wird in diesem Kapitel im Wesentlichen nach [16] vorgegangen.

Definition. Sei K ein Körper.

(1) Eine *Anordnung* von K ist eine totale Ordnungsrelation $\leq$ auf der Menge K, welche
(a) $a \leq b \Rightarrow a + c \leq b + c$ und
(b) $a \leq b$, $c \geq 0 \Rightarrow ac \leq bc$
für alle $a, b, c \in K$ erfüllt.

(2) Ein angeordneter Körper ist ein Paar $(K, \leq)$ aus einem Körper K und einer Anordnung $\leq$ von K.

Ein Körper K heißt *reell*, wenn er mindestens eine Anordnung besitzt.

Beispiele. (1) $(\mathbb{R}, \leq)$ ist ein angeordneter Körper. Der Körper $\mathbb{R}$ ist also reell.

(2) Jeder Teilkörper eines reellen Körpers ist selbst reell, z.B. $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Definition. Ein Körper K heißt *reell abgeschlossen*, wenn er reell ist, aber keine echte algebraische reelle Erweiterung hat. In anderen Worten: Es gibt keinen Körper L zwischen K und einem algebraischen Abschluss $\overline{K}$ von K, der reell und von K verschieden ist.

Der Körper $\mathbb{R}$ etwa ist reell abgeschlossen. Weiters ist die Menge aller reellen Zahlen, die Nullstellen eines Polynoms über $\mathbb{Q}$ sind, genannt algebraischer Abschluss von $\mathbb{Q}$ in $\mathbb{R}$, reell abgeschlossen.

3.1 Obere Schranken

Zunächst zeigen wir, dass sich alle Nullstellen eines Polynoms in einer Variablen über einem reell abgeschlossenen Körper durch seine Koeffizienten beschränken lassen. Mit technischen Hilfsmitteln wie dem Satz von Rolle und dem Lemma von Descartes werden wir anschließend erkennen, dass eine Schranke für die Anzahl der Nullstellen eines Polynoms existiert, die von der Anzahl der im Polynom vorkommenden Monome abhängt.

Lemma. *Sei R ein reell abgeschlossener Körper und*

$$f = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

ein normiertes Polynom in $R(\sqrt{-1})[x]$. Dann gilt für jede Nullstelle z von f in $R(\sqrt{-1})$ die Abschätzung

$$|z| \leq \max\{1, |a_1| + \ldots + |a_n|\}.$$

Beweis: O.B.d.A. sei $|z| > 1$. Daher darf man die Gleichung $f(z) = 0$ durch z^{n-1} dividieren, wodurch sich

$$-z = a_1 + \frac{a_2}{z} + \ldots + \frac{a_n}{z^{n-1}}$$

ergibt. Mittels Anwendung der Dreiecksungleichung erhält man somit

$$|z| \leq |a_1| + \frac{|a_2|}{|z|} + \ldots + \frac{|a_n|}{|z|^{n-1}} \leq |a_1| + \ldots + |a_n|.$$

□

Ist speziell $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$ ein Polynom, dessen Nullstellen alle reell sind, so liegen diese innerhalb des Intervalls mit den Endpunkten

$$x_{1,2} = -\frac{a_{n-1}}{n} \pm \frac{n-1}{n}\sqrt{a_{n-1}^2 - \frac{2n}{n-1}a_{n-2}}.$$

Beispiel 3.1. Das Polynom $x^4 + 5x^3 + 5x^2 - 5x - 6$ hat die vier reellen Nullstellen $-3, -2, -1$ und 1. Alle Nullstellen liegen somit im Intervall

$$[-\frac{5}{4} - \frac{3}{4}\sqrt{\frac{35}{3}}, -\frac{5}{4} + \frac{3}{4}\sqrt{\frac{35}{3}}] = [-3.81, 1.31].$$

Wir benötigen im Folgenden den *Quotientenkörper* über dem Ring $R[x]$, beschrieben durch $R(x) := \{\frac{P}{Q} |\ P, Q \in R[x], Q \neq 0\}$.

Lemma. *Sei $0 \neq f \in R(t)$. Die logarithmische Ableitung $\frac{f'}{f}$ von f wechselt in jeder Nullstelle von f in R das Vorzeichen von minus nach plus.*

Beweis: Sei a eine Nullstelle von f und $f(x) := (x-a)^n \cdot g(x)$, wobei $n \in \mathbb{N}$ und $g \in R(x)$ mit $g(a) \neq 0$. Dann ist

$$\frac{f'(x)}{f(x)} = \frac{n}{x-a} + \frac{g'(x)}{g(x)}.$$

Daher gilt

$$\operatorname{sign}\tfrac{f'(x)}{f(x)} = \begin{cases} +1, & \text{wenn } x < a, \\ -1, & \text{wenn } x > a, \end{cases}$$

woraus die Behauptung folgt. □

Satz 37. *Sei R ein reell abgeschlossener Körper, sei $f \in R(x)$ und seien $a < b$ in R mit $f(a) = f(b) = 0$. Hat f in $]a,b[$ weder Pole noch Nullstellen, so ist die Anzahl der mit Vielfachheit gezählten Nullstellen von f' im Intervall $]a,b[$ ungerade.*

Beweis: Wähle $a < c < d < b$ in R derart, dass f' in $]a,c] \cup [d,b[$ keine Nullstellen hat. Nach dem letzten Lemma ist dann

$$\frac{f'(c)}{f(c)} \cdot \frac{f'(d)}{f(d)} < 0.$$

Infolgedessen ist die Zahl der Nullstellen von $\frac{f'}{f}$ in $[c,d]$ ungerade. Diese ist auch die Zahl der Nullstellen von f' in $]a,b[$. □

Satz 38 (Rolle)**.** *Ist $f \in R(x)$, sind $a < b$ in R mit $f(a) = f(b)$, und hat f in $[a,b]$ keine Pole, so hat f' im Intervall $]a,b[$ eine Nullstelle.*

Beweis: Sei o.B.d.A. $f(a) = f(b) = 0$. Wir ersetzen nun b durch die kleinste Nullstelle c von f mit $c > a$. Somit sind wir in der Situation des vorigen Satzes (Satz **??**). □

Sei $f \in R(x)$ und seien $a < b$ in R so, dass f in $[a,b]$ keinen Pol hat. Durch Anwenden des Satzes von Rolle auf die Funktion

$$g(x) = f(x) - \frac{x-a}{b-a}\big(f(b) - f(a)\big),$$

die $g(a) = g(b)$ erfüllt, ergibt sich der Mittelwertsatz. Dieser besagt, dass ein $c \in]a,b[$ existiert mit

$$f'(c) = \frac{f(b) - f(a)}{b-a}.$$

Definition. Für eine endliche Folge $(c_1, \ldots, c_n)$ in R bezeichne

$$\operatorname{Var}\Big(c_1, \ldots, c_n\Big)$$

die Anzahl der Vorzeichenwechsel in der Folge nach Streichen aller Nullen.

Satz 39 (Lemma von Descartes)**.** *Sei* $f = \sum_{i=0}^{n} a_i x^i$ *ein nicht-verschwindendes Polynom in* $R[x]$*. Die Anzahl der strikt positiven reellen Nullstellen von* f *beträgt höchstens* $\mathrm{Var}\Big(a_n, \ldots, a_1, a_0\Big)$.

Beweis: Der Beweis erfolgt mittels Induktion über den Grad n von f. Für $n = 1$ besitzt die Gerade $f(x) = ax + b$ genau dann eine positive reelle Nullstelle, wenn $\mathrm{sign}(a) \neq \mathrm{sign}(b)$. Sei nun $n = \deg(f) > 1$. Wir können ferner $a_0 = f(0) \neq 0$ annehmen. Sei r der kleinste Index ≥ 1 mit $a_r \neq 0$. Nach Induktionsannahme besitzt $f' = na_n t^{n-1} + \ldots + ra_r t^{r-1}$ höchstens $\mathrm{Var}\Big(a_n, \ldots, a_r\Big)$ positive Nullstellen. Sei c die kleinste von ihnen (bzw. $c = \infty$, falls es keine gibt). Nach dem Satz von Rolle hat f höchstens $1 + \mathrm{Var}\Big(a_n, \ldots, a_r\Big)$ positive Nullstellen. Wir können annehmen, dass diese Grenze angenommen wird, weil wir sonst fertig sind. Damit muss f eine Nullstelle in $]0, c\,[$ haben. Dies impliziert $a_0 a_r < 0$ und somit $1 + \mathrm{Var}\Big(a_n, \ldots, a_r\Big) = \mathrm{Var}\Big(a_n, \ldots, a_0\Big)$. □

Satz 40. *Sei* $f \in R[x]$ *ein aus* m *Termen bestehendes Polynom. Dann hat* f *höchstens* $2m - 1$ *Nullstellen in* R*.*

Beweis: $f(x)$ und $f(-x)$ haben nach dem Lemma von Descartes jeweils höchstens $m - 1$ positive Nullstellen. Also hat f höchstens $2m - 2$ von null verschiedene Nullstellen. □

Beispiel 3.2. Sei das Polynom $f = x \cdot (x^2 - a_1) \cdot \ldots \cdot (x^2 - a_m)$ mit $0 \neq a_i \in R$ gegeben. $\frac{f}{x}$ ist ein Polynom in x^2 vom Grad m. f hat folglich höchstens $m + 1$ Terme und daher hat f nach dem letzten Satz (Satz **??**) höchstens $2m + 1$ reelle Nullstellen.

Bevor wir zwei Verfahren zur exakten Bestimmung der Anzahl von reellen Nullstellen eines Polynoms $f \in R[x]$ kennenlernen, werden wir mittels Zerlegung reller Polynome erörtern, wie die Anzahl der reellen Nullstellen von f mit dem Grad von f zusammenhängt.
Sei dazu $f = a_0 + \ldots + a_n x^n \in R[x]$, $a_n \neq 0$, $n \geq 1$. Besitzt f eine reelle Nullstelle a, so spaltet f in $R[x]$ den Linearfaktor $x - a$ ab. Hat f dagegen keine reelle Nullstelle, so nach dem Fundamentalsatz der Algebra wenigstens eine im algebraischen Abschluss $\overline{R}$ von R. Sei $c = \alpha + i\beta$ mit $\alpha, \beta \in R$, $\beta \neq 0$ eine solche Nullstelle. Man findet sofort eine weitere Nullstelle, nämlich $\overline{c} = \alpha - i\beta \neq c$. Denn es ist

$$0 = \overline{f(c)} = \overline{a_0} + \overline{a_1 c} + \ldots + \overline{a_n c^n} = a_0 + a_1 \overline{c} + \ldots + a_n \overline{c}^n = f(\overline{c}).$$

Weiters ist $h := (x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c}$ ein Teiler von f in $\overline{R}[x]$. Wegen $c + \overline{c} = 2\alpha \in R$ und $c\overline{c} = \alpha^2 + \beta^2 \in R$ ist $h \in R[x]$. Es ist daher klar, dass sich f aus dem Produkt von Linearfaktoren vom Typ $x - a$, $a \in R$ und von quadratischen Polynomen vom Typ $x^2 - (c + \overline{c})x + c\overline{c}$, $c \in \overline{R} \setminus R$ zusamensetzt. Die Faktoren dieses Produktes sind eindeutig bestimmt, da man sie aus den Nullstellen von f in $\overline{R}$ ablesen kann. Daraus erhalten wir eine Folgerung in Bezug auf die Anzahl der reellen Nullstellen von f.

Folgerung. *Sei $f \in R[x]$, $\deg(f) = n \geq 0$. Dann ist die Anzahl N der mit Vielfachheit gezählten reellen Nullstellen von f kongruent zu $n \mod 2$, d.h., 2 teilt $N - n$. Ist insbesondere n ungerade, so besitzt f wenigstens eine reelle Nullstelle.*

Beispiel 3.3. Ein reelles quadratisches Polynom $f = ax^2 + bx + c$, $a \neq 0$, besitzt zwei, eine doppelte oder keine reelle Nullstelle. Aus der Darstellung

$$f = a\big((x + \frac{b}{2a})^2 - \frac{b^2 - 4ac}{4a^2}\big)$$

folgt, dass f genau dann wenigstens eine reelle Nullstelle hat, wenn man in R die Quadratwurzel aus $b^2 - 4ac$ ziehen kann, d.h., $b^2 - 4ac \geq 0$.

3.2 Zählverfahren

3.2.1 Sturm'sche Ketten

Sei jetzt $f \in R[x]$ ein nichtkonstantes Polynom, und seien $a < b$ in R mit $f(a)f(b) \neq 0$. Im Folgenden werden Verfahren behandelt, mit denen die Anzahl der Nullstellen von f in einem reell abgeschlossenen Körper R im Intervall $[a, b]$ bestimmt werden kann, wobei ohne Vielfachheit gezählt wird.

Definition. Die *Sturm'sche Kette* zu f ist die rekursiv definierte Folge $(f_0, f_1, \ldots, f_r)$ von Polynomen in $R[x]$, definiert durch $f_0 := f$ und $f_1 := f'$ und

$$\begin{array}{rcl} f_0 & = & q_1 f_1 - f_2, \\ f_1 & = & q_2 f_2 - f_3, \\ & \vdots & \\ f_{r-2} & = & q_{r-1} f_{r-1} - f_r, \\ f_{r-1} & = & q_r f_r. \end{array}$$

Dabei seien die f_i, q_i Polynome mit $f_i \neq 0$ für $1 \leq i \leq r$, und es gelte $\deg(f_i) < \deg(f_{i-1})$ für $2 \leq i \leq r$. Dadurch sind $r \in \mathbb{N}$ sowie die f_i und g_i eindeutig bestimmt. Für $x \in \mathrm{R}$ setzen wir ferner

$$v_f(x) := \mathrm{Var}\Big(f_0(x), f_1(x), \ldots, f_r(x)\Big).$$

Es gilt insbesondere $f_r = \mathrm{ggT}(f, f')$. Die Sturm'sche Kette entspricht nämlich bis auf die negativen Vorzeichen der Restterme dem euklidischen Algorithmus für das Paar (f, f').

Satz 41 (Sturm, ohne Nebenbedingung)**.** *Für $a < b$ in R mit $f(a)f(b) \neq 0$ ist $v_f(a) - v_f(b)$ die Anzahl der Nullstellen von f im Intervall $[a, b]$ (ohne Vielfachheit).*

Beweis: Wir untersuchen im Folgenden $v_f(x)$ als Funktion von x. Zunächst sei angenommen, dass alle Nullstellen von f einfach sind. Dann gilt für die Folge $(f_0, f_1, \ldots, f_r)$: (1) $\mathrm{ggT}(f_0, f_1) = 1$.

(2) In jeder Nullstelle von f_0 wechselt $f_0 f_1$ das Vorzeichen von minus nach plus.

(3) Für $1 \leq i \leq n$ und jede Nullstelle c von f_i gilt $f_{i-1}(c)f_{i+1}(c) < 0$.

(1) folgt unmittelbar aus der Einfachheit aller Nullstellen von f, (2) aus dem letzten Lemma und (3) aus $f_{i-1} = g_i f_i - f_{i+1}$ und $\mathrm{ggT}(f_{i-1}, f_i) = 1$.
Seien $c \in R$ und $0 \leq i < r$ mit $f_i(c) = 0$. Dann ist $f_{i+1}(c) \neq 0$ nach (1) bzw. (3). Wir setzen $\epsilon := \mathrm{sign}(f_{i+1}(c))$. In den nachfolgenden Vorzeichenschemata stehe $c_\pm$ symbolisch für Werte x mit $\mathrm{sign}(x - c) = \pm 1$ und $|x - c|$ genügend klein.

Für $i = 0$ folgt aus (2):

	$x = c_-$	$x = c$	$x = c_+$
$f_0(x)$	$-\epsilon$	0	ϵ
$f_1(x)$	ϵ	ϵ	ϵ
Beitrag zu $v_f(x)$	1	0	0

Für $1 \leq i < r$ folgt aus (3):

	$x = c_-$	$x = c$	$x = c_+$
$f_{i-1}(x)$	$-\epsilon$	$-\epsilon$	$-\epsilon$
$f_i(x)$	?	0	?
$f_{i+1}(x)$	ϵ	ϵ	ϵ
Beitrag zu $v_f(x)$	1	1	1

Fazit: Die Funktion $v_f(x)$ fällt in jeder Nullstelle von f um 1 und ist außerhalb der endlich vielen Nullstellen von f lokal konstant. Für $a < b$ in R ist daher $v_f(a) - v_f(b)$ die Anzahl der Nullstellen von f im Intervall $[a, b]$.
Jetzt bleibt es zu zeigen, dass Letzteres auch für Funktionen mit mehrfachen Nullstellen gilt, d.h., f_r ist auch als nichtkonstantes Polynom zugelassen. Wir setzen $g_i := \frac{f_i}{f_r}$ für $0 \leq i \leq r$. Dann erfüllt die Folge von Polynomen $(g_0, g_1, \ldots, g_r)$ die vorigen drei Eigenschaften:
(1) wegen $\mathrm{ggT}(g_0, g_1) = \mathrm{ggT}(\frac{f_0}{f_r}, \frac{f_1}{f_r}) = \frac{1}{f_r}\mathrm{ggT}(f_0, f_1) = 1$, (2) und (3) wegen $f_r^2 > 0$.
Sei $d \in R$ mit $f_r(d) \neq 0$. Die beiden Folgen $\big(g_0(d), \ldots, g_r(d)\big)$ und $\big(f_0(d), \ldots, f_r(d)\big)$ haben dieselbe Anzahl von Vorzeichenwechsel, weil sie durch Multiplikation mit der Konstanten $f_r(d)$ auseinander hervorgehen. Zudem haben f_0 und g_0 dieselben Nullstellen. Damit lassen sich Funktionen mit mehrfachen Nullstellen auf solche mit einfachen Nullstellen zurückführen, für die wir die Behauptung bereits gezeigt haben. □

Beispiel 3.4. Für das Polynom $f := x^4 - 2x^3 - 2x^2 + 4x$ ergibt sich die Sturm'sche Kette

$$\begin{aligned} f_0 &= x^4 - 2x^3 - 2x^2 + 4x, \\ f_1 &= 4x^3 - 6x^2 - 4x + 4, \\ f_2 &= \tfrac{7}{4}x^2 - \tfrac{5}{2}x - \tfrac{1}{2}, \\ f_3 &= \tfrac{160}{49}x - \tfrac{192}{49}, \\ f_4 &= \tfrac{49}{50}. \end{aligned}$$

Wegen $v_f(-3) = \mathrm{Var}\Big(+1,-1,+1,-1,+1\Big) = 4$ und $v_f(3) = \mathrm{Var}\Big(+1,+1,+1,+1,+1\Big) = 0$ besitzt f im Intervall $]-3,3[$ 4 reelle Nullstellen.

Für $0 \le i \le r$ sei $d_i := \deg(f_i)$ und a_i der Leitkoeffizient von f_i. Dann ist

$$v_f(-\infty) := \mathrm{Var}\Big((-1)^{d_0}a_0, (-1)^{d_1}a_1, \ldots, (-1)^{d_r}a_r\Big)$$

und

$$v_f(+\infty) := \mathrm{Var}\Big(a_0, a_1, \ldots, a_r\Big).$$

Infolgedessen ist die Anzahl aller verschiedenen reellen Nullstellen von f gleich $v_f(-\infty) - v_f(+\infty)$.

Im Folgenden wird die Verallgemeinerung des Sturm'schen Satzes behandelt. Seien $f, g \in R[x]$ mit f nichtkonstant und $g \neq 0$. Ziel ist es nun, die Nullstellen c von f mit der Nebenbedingung $g(c) > 0$ zählen zu können.

Definition. Die *verallgemeinerte Sturm'sche Kette* zu f und g wird folgendermaßen gebildet: Sei $f_0 := f$, $f_1 := f'g$ und seien $f_2, \ldots, f_r$ analog wie ohne Nebenbedingungen durch $f_{i-1} = g_i f_i - f_{i+1}$ und $\deg(f_{i+1}) < \deg(f_i)$ für $1 \le i \le r-1$, sowie $f_i \neq 0$ und $f_r | f_{r-1}$ definiert. Für $x \in R$ setzen wir

$$v_{f,g}(x) := \mathrm{Var}\Big(f_0(x), f_1(x), \ldots, f_r(x)\Big).$$

Satz 42 (Sturm, mit Nebenbedingung)**.** *Für $a < b$ in R mit $f(a)f(b) \neq 0$ ist*

$$v_{f,g}(a) - v_{f,g}(b) = \sum_{\substack{a<c<b \\ f(c)=0}} \mathit{sign}\big(g(c)\big).$$

Letzteres ist also die Anzahl der Nullstellen c von f in $[a,b]$ mit $g(c) > 0$ minus der Anzahl der Nullstellen c von f in $[a,b]$ mit $g(c) < 0$. Man kennt die Anzahl der Nullstellen c von f, in denen $g(c) \neq 0$ und kann somit die Anzahl der Nullstellen c von f mit $g(c) > 0$ berechnen. Die zuvor gegebene Version ist der Spezialfall $g = 1$.

Beweis: Man geht analog wie beim Beweis des Sturm'schen Satzes ohne Nebenbedingung vor und nimmt zunächst $\mathrm{ggT}(f, f'g) = 1$ an, d.h., f_r ist eine Konstante. Für die Folge $(f_0, \ldots, f_r)$ gelten (1), (3) von oben und
(2′) In jeder Nullstelle c von f_0 wechselt $f_0 f_1$ das Vorzeichen von $-\mathrm{sign}(g(c))$ nach

$+\text{sign}(g(c))$. $(2')$ ergibt sich aus dem letzten Lemma.

Erneut untersuchen wir, wie sich $v_{f,g}(x)$ beim Durchgang durch eine Nullstelle c von f_i ändert. Für $i \geq 1$ ändert sich $v_{f,g}(x)$ wie früher nicht. Für $i = 0$ und $\epsilon := \text{sign}(f_1(c))$ erhalten wir folgendes Vorzeichenschema:

	$x = c_-$	$x = c$	$x = c_+$
$f_0(x)$	$-\epsilon \cdot \text{sign}(g(c))$	0	$\epsilon \cdot \text{sign}(g(c))$
$f_1(x)$	ϵ	ϵ	ϵ
Beitrag zu $v_f(x)$			
falls g(c)<0	0	0	1
falls g(c)>0	1	0	0

Damit ist $v_{f,g}(c_-) - v_{f,g}(c_+) = \text{sign}(g(c))$. Lässt man auch mehrfache Nullstellen zu, so ersetzt man wiederum die Folge $\big(f_0, \ldots, f_r\big)$ durch die Folge $\big(\frac{f_0}{f_r}, \ldots, \frac{f_r}{f_r}\big)$. (1), $(2')$ und (3) gelten ebenso für die neue Folge. Weil beide Folgen dieselbe Anzahl an Vorzeichenwechsel aufweisen, ergibt sich somit die Behauptung. □

3.2.2 Methode von Hermite und Sylvester

Im Folgenden wird eine zweite Methode erläutert, wie man reelle Nullstellen von Polynomen zählen kann.

Sei nun $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ ein normiertes, nichtkonstantes Polynom über einem reell abgeschlossenen Körper R. Sei ferner $\overline{R}$ der algebraische Abschluss von R, d.h., $\overline{R}$ ist die kleinste Menge, sodass alle Nullstellen von Polynomen über R in $\overline{R}$ liegen. Die komplexen Zahlen $\mathbb{C}$ sind beispielsweise der algebraische Abschluss zu den reellen Zahlen $\mathbb{R}$.

Definition. Für die Nullstellen $\alpha_1, \ldots, \alpha_n$ von f in $\overline{R}$ heißt

$$w_r(f) = w_r := \alpha_1^r + \ldots + \alpha_n^r$$

die r-te *Newton'sche Summe*.

Mittels Einsetzen jeder Nullstelle in f und Aufsummierung der resultierenden Gleichungen ergibt sich für alle $k \geq 0$ die Newton'sche Identität

$$w_k + w_{k-1}a_1 + \ldots + w_1 a_{k-1} + k a_k = 0,$$

wobei $a_k := 0$ für $k > n$. Aus dieser Gleichung kann man iterativ die Newton'schen Summen berechnen. Es sind

$$\begin{aligned}
w_0 &= n, \\
w_1 &= -a_1, \\
w_2 &= a_1^2 - 2a_2, \\
w_3 &= -a_1^3 + 3a_1a_2 - 3a_3, \\
w_4 &= a_1^4 - 4a_{12} + 3a_1a_3 + a_1^2 + 2a_2^2, \\
&\vdots
\end{aligned}$$

Definition. Eine komplexe, quadratische Matrix A heißt *Hermite-Matrix*, wenn sie gleich ihrer konjugierten transponierten Matrix $\overline{A}^T$ ist. Wir bezeichnen

$$H(f) := \big(w_{j+k-2(f)}\big)_{1\le j,k\le n} = \begin{pmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_1 & w_2 & \cdots & w_n \\ \vdots & \vdots & \ddots & \vdots \\ w_{n-1} & w_n & \cdots & w_{2n-2} \end{pmatrix} \in R^{n\times n}$$

als die *Hermite-Matrix* von f.

Allgemein existiert für eine hermitesche Matrix $A \in \mathrm{M_n(R)}$ eine invertierbare Matrix $S \in \mathrm{Gl_n(K)}$, sodass $S^T A S = \mathrm{diag}(d_1, \ldots, d_n)$ eine Diagonalmatrix ist, wobei $d_1, \ldots, d_n$ die Eigenwerte zu A sind. Dies wird in [15] p.278 bewiesen.

Definition. Die ganze Zahl

$$\mathrm{sign}(A) := \sum_{i=1}^{n} \mathrm{sign}(d_i)$$

heißt die *Signatur* von A.

Der Satz von Sylvester besagt, dass die Signatur einer hermiteschen Matrix A nur von A selbst, aber nicht von S abhängt. An dieser Stelle sei auf [15] p.281f verwiesen.

Satz 43 (Hermite)**.** *Sei R ein reell abgeschlossener Körper und $f \in R[x]$ ein normiertes, nichtkonstantes Polynom. Dann gilt:*

(1) $\mathrm{rk}\big(H(f)\big)$ = *Anzahl der verschiedenen Nullstellen von f in $R(\sqrt{-1})$,*

(2) $\mathrm{sign}\big(H(f)\big)$ = *Anzahl der verschiedenen Nullstellen von f in R.*

Beweis: Seien $\alpha_1, \ldots, \alpha_n$ die Wurzeln von f in $R(\sqrt{-1})$. Mit

$$V := \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

gilt dann $V \cdot V^t = H(f)$. Setze

$$L_\alpha(x) := \sum_{k=1}^{n} \alpha^{k-1} x_k.$$

Damit folgt für $x \in R^n$

$$x \cdot H(f) \cdot x^t = \big(xV\big) \cdot \big(xV\big)^t = \sum_{j=1}^{n} L_{\alpha_j}(x)^2.$$

Seien nun $\alpha_1, \ldots, \alpha_m$ für $m \le n$ die verschiedenen Wurzeln von f in $R(\sqrt{-1})$. Dann sind die Linearformen $L_{\alpha_1}, \ldots, L_{\alpha_m}$ linear unabhängig. Somit ist $\mathrm{rank}\big(H(f)\big) = m$.

Außerdem ist für $x \in R^n$

$$L_\alpha(x)^2+L_{\overline{\alpha}}(x)^2 = L_\alpha(x)^2+\overline{L_\alpha(x)}^2 = 2\big(\frac{1}{2}(L_\alpha(x)+L_{\overline{\alpha}}(x))\big)^2-2\big(\frac{1}{2i}(L_\alpha(x)-L_{\overline{\alpha}}(x))\big)^2$$

$$= 2\,\mathrm{Re}\big(L_\alpha(x)\big)^2 - 2\,\mathrm{Im}\big(L_\alpha(x)\big)^2.$$

Für $\mathrm{Im}(\alpha) \neq 0$ erzeugen die Linearformen $L_\alpha, L_{\overline{\alpha}}$ und $\mathrm{Re}(L_\alpha), \mathrm{Im}(L_\alpha)$ denselben zweidimensionalen Unterraum. Daraus folgt die Behauptung über die Signatur. □

Beispiele. (1) Gegeben sei das Polynom $f := x^5 + ax^2 + b$ mit $a, b \in \mathbb{R}$. Gesucht ist die Anzahl von reellen Nullstellen von f in Abhängigkeit von a und b.

Die dazugehörige Sturm'sche Kette lautet

$$\begin{array}{rcl} f_0 & = & x^5 + ax^2 + b, \\ f_1 & = & 5x^4 + 2ax, \\ f_2 & = & -\frac{3a}{5}x^2 - b, \\ f_3 & = & -2ax - \frac{125b^2}{9a^2}, \\ f_4 & = & \frac{3125b^4}{108a^5} + b. \end{array}$$

Somit ist

$$v_f(-\infty) = \mathrm{Var}\Big(-1, 1, -a, a, f_4\Big)$$

und

$$v_f(+\infty) = \mathrm{Var}\Big(1, 1, -a, -a, f_4\Big).$$

Im Fall $a = 0$ hat f daher eine reelle Nullstelle. Ist $a \neq 0$ und $D := 3125b^4 + 108a^5b$, so hat f genau dann eine bzw. drei Nullstellen, wenn $D > 0$ bzw. $D < 0$.

(2) Sei $f := x^3 + ax^2 + bx + c$ ein Polynom dritten Grades über $\mathbb{R}$. Wir wissen nach einer Folgerung im ersten Unterkapitel, dass f mindestens eine reelle Nullstelle besitzen muss. Eine aufwändige Rechnung liefert die entsprechende Sturm'sche Kette

$f_0 = x^3 + ax^2 + bx + c = \big(\frac{1}{3}x + \frac{1}{9}a\big)\big(3x^2 + 2ax + b\big) + \big(\frac{2}{3}b - \frac{2}{9}a^2\big)x - \frac{1}{9}ab + c,$

$f_1 = 3x^2 + 2ax + b$

$= \big(\frac{27}{2(a^2-3b)}x + \frac{9(4a^3-15ab+27c)}{4(a^2-3b)^2}\big)\big((\frac{2}{9}a^2 - \frac{2}{3}b)x + \frac{1}{9}ab - c\big) - \frac{(ab+ac)(4a^3-15ab+27c)}{4(a^2-3b)^2} + b,$

$f_2 = \big(\frac{2}{9}a^2 - \frac{2}{3}b\big)x + \frac{1}{9}ab - c,$

$f_3 = \frac{(ab+ac)(4a^3-15ab+27c)}{4(a^2-3b)^2} - b.$ Damit ergibt sich wiederum

$$v_f(-\infty) = \mathrm{Var}\Big(-1, 1, -(a^2 - 3b), (ab + ac)(4a^3 - 15ab + 27c) - 4b(a^2 - 3b)^2\Big)$$

und

$$v_f(-\infty) = \mathrm{Var}\Big(1, 1, a^2 - 3b, (ab + ac)(4a^3 - 15ab + 27c) - 4b(a^2 - 3b)^2\Big).$$

Also hat man eine hinreichende Bedingung für die Anzahl von reellen Nullstellen von Polynomen dritten Grades gefunden: Das Polynom $x^3 + ax^2 + bx + c$ besitzt dann eine reelle Nullstelle, wenn

$$(ab + ac)(4a^3 - 15ab + 27c) - 4b(a^2 - 3b)^2 < 0 \text{ oder } a = 0 \text{ und } b \geq 0.$$

Es besitzt ferner drei reelle Nullstellen, wenn

$$(ab + ac)(4a^3 - 15ab + 27c) - 4b(a^2 - 3b)^2 > 0 \text{ oder } a = 0 \text{ und } b < 0.$$

Betrachten wir speziell das Polynom

$$f = x^3 + x^2 - x - 1.$$

Über $\mathbb{C}$ hat es die drei Nullstellen $\alpha_1 = 1$, $\alpha_2 = i$ und $\alpha_3 = -i$. Nach Berechnung der Newton'schen Summen erhalten wir die Hermite-Matrix von f

$$H(f) = \begin{pmatrix} 3 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 3 \end{pmatrix}.$$

Diese hat vollen Rang. Daher besitzt f nach dem Satz von Hermite drei Nullstellen über $\mathbb{C}$. Zudem ist $\operatorname{sign}\big(H(f)\big) = 1$ und folglich hat f genau eine reelle Nullstelle.

Gegeben sei das Polynom

$$f := x^4 - 4x^3 + \frac{21}{4}x^2 - 4x + \frac{17}{4}.$$

Eine mühsame Rechnung liefert die Hermite-Matrix

$$H(f) = \begin{pmatrix} 4 & 14 & \frac{11}{2} & -115 \\ 4 & \frac{11}{2} & -115 & -16 \\ \frac{11}{2} & -115 & -16 & \frac{101}{4} \\ -115 & -16 & \frac{101}{4} & \frac{2423}{8} \end{pmatrix}.$$

Diese hat vollen Rang, jedoch Signatur null und somit keine reelle Nullstelle. Die vier komplexen Nullstellen lauten $i, -i, 2 - \frac{1}{2}i, 2 + \frac{1}{2}i$.

Wie schon beim Sturm'schen Algorithmus hat auch die Methode von Hermite eine Verallgemeinerung, mit der man die reellen Nullstellen eines Polynoms f über einem reell abgeschlossenen Körper unter Nebenbedingungen zählen kann.

Seien $f \in K[x]$ normiert vom Grad $n \geq 1$ und für $\alpha_j \in \overline{K}$

$$f = \prod_{j=1}^{n} (x - \alpha_j).$$

Für eine weiteres Polynom $g \in K[x]$ definiere die allgemeinen Newton'schen Summen durch

$$w_k(f, g) := \widetilde{w_k} = \sum_{j=1}^{n} \alpha_j^k g(\alpha_j)$$

für $k \geq 0$ und die verallgemeinerte Hermite-Matrix zu f und g durch

$$H(f,g) := (\widetilde{w}_{j+k-2})_{1\leq j,k\leq n} = \begin{pmatrix} \widetilde{w}_0 & \widetilde{w}_1 & \cdots & \widetilde{w}_{n-1} \\ \widetilde{w}_1 & \widetilde{w}_2 & \cdots & \widetilde{w}_n \\ \vdots & \vdots & \ddots & \vdots \\ \widetilde{w}_{n-1} & \widetilde{w}_n & \cdots & \widetilde{w}_{2n-2} \end{pmatrix}.$$

Ist $g = \sum_j b_j x^j$, so erhält man $\tilde{w}_k$ aus den Newton'schen Summen $w_k(f,1)$ wie folgt:

$$\widetilde{w_k} = w_k(f,g) = \textstyle\sum_l \alpha_l^k \sum_j b_j \alpha_l^j = \sum_j b_j \sum_l \alpha_l^{j+k} = \sum_j b_j w_{j+k}(f).$$

Satz 44 (Verallgemeinerung des Satzes von Hermite)**.** *Sei R ein reell abgeschlossener Körper und $f \in R[x]$ normiert,* $\deg(f) = n \geq 1$*. Für jedes Polynom $g \in R[x]$ ist dann*

$$rk\big(H(f,g)\big) = \{\alpha \in \overline{R} : f(\alpha) = 0 \text{ und } g(\alpha) \neq 0\}$$

und

$$sign\big(H(f,g)\big) = \sum_{\substack{\alpha\in R \\ f(\alpha)=0}} sign(g(\alpha)).$$

Beweis: Siehe [16] p.22. □

Man kann auch Nullstellen mit beliebig, aber endlich vielen Nebenbedingungen zählen. Seien dazu $f, g_1, \ldots, g_r \in R[x]$ mit $f \neq 0$. Für $e = (e_1, \ldots, e_r) \in \{1,2\}^r$ seien

$$g^e := \prod_{i=1}^{r} g_i^{e_i}$$

und

$$N_e := \sum_{\substack{c\in R \\ f(c)=0}} \operatorname{sign}(g^e(c)).$$

Wir können die N_e wahlweise algorithmisch ermitteln, nämlich entweder aus der verallgemeinerten Sturm'schen Kette zum Paar (f, g^e) oder mit der verallgemeinerten Hermite'schen Methode als $N_e = \operatorname{sign}(H(f, g^e))$.

Lemma. *Seien $f, g_1, \ldots, g_r \in R[x]$ mit $f \neq 0$ und $r \geq 0$. Dann ist*

$$\frac{1}{2^r} \sum_{e\in\{1,2\}^r} N_e = \{c \in R : f(c) = 0, g_1(c) > 0, \ldots, g_r(c) > 0\}.$$

Beweis: Man zeigt zunächst die Behauptung

$$\sum_{e\in\{1,2\}^r} \operatorname{sign}\big(g_1(c)^{e_1} \cdot \ldots \cdot g_r(c)^{e_r}\big) = \prod_{i=1}^{r} \Big(\operatorname{sign}\big(g_i(c)\big) + \operatorname{sign}\big(g_i^2(c)\big)\Big)$$

mittels Induktion über r.
Für $r = 1$ ist die Gleichung erfüllt. Die gewünschte Behauptung folgt aus

$$\sum_{e\in\{1,2\}^r} \operatorname{sign}\big(g_1(c)^{e_1}\cdot\ldots\cdot g_r(c)^{e_r}\cdot g_{r+1}(c)^{e_{r+1}}\big)$$

$$= \sum_{e\in\{1,2\}^r} \operatorname{sign}\big(g_1(c)^{e_1}\cdot\ldots\cdot g_r(c)^{e_r}\big)\cdot \sum_{e\in\{1,2\}^r} \operatorname{sign}\big(g_{r+1}(c)^{e_{r+1}}\big)$$

$$= \prod_{i=1}^{r+1}\Big(\operatorname{sign}\big(g_i(c)\big) + \operatorname{sign}\big(g_i^2(c)\big)\Big).$$

Die Behauptung des Lemmas ergibt sich somit unmittelbar:

$$\frac{1}{2^r}\sum_{e\in\{1,2\}^r} N_e$$

$$= \sum_{\substack{c\in R\\ f(c)=0}} \sum_{e\in\{1,2\}^r} \operatorname{sign}\big(g_1(c)^{e_1}\cdot\ldots\cdot g_r(c)^{e_r}\big)$$

$$= \sum_{\substack{c\in R\\ f(c)=0}} \prod_{i=1}^{r}\Big(\operatorname{sign}\big(g_i(c)\big) + \operatorname{sign}\big(g_i^2(c)\big)\Big).$$

□

Kapitel 4

Eine Anwendung des Satzes von Bernstein

4.1 Grundlagen

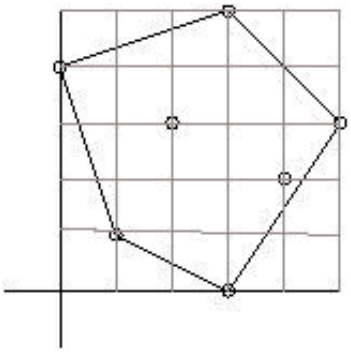
Im Folgenden werden die grundlegenden Begriffe für den Satz von Bernstein in kurzer Form dargelegt. Anschließend wird der Satz von Bernstein ohne Beweis (siehe dazu [7] p.346 ff) vorgestellt.

Gegeben seien n Polynome $f_1, \ldots, f_n$ mit $f_i \in \mathbb{C}[x_1, \ldots, x_n]$. Ziel ist es nun, die Anzahl der gemeinsamen Nullstellen der $f_1, \ldots, f_n$ in $\mathbb{C}^n$ zu finden.

Definition. Für $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha$ heißt

$$\operatorname{supp}(f) := \{\alpha \in \mathbb{N}^n; c_\alpha \neq 0\}$$

der *Träger* von f. Ferner nennt man die konvexe Hülle $N(f)$ des Trägers von f das *Newtonpolytop* von f.



Das Newtonpolytop von
$f = a_1x^5y^3 + a_2x^4y^2 + a_3x^3y^5 + a_4x^3 + a_5x^2y^3 + a_6xy + a_7y^4$

Für zwei Polytope $P_1, P_2 \subset \mathbb{R}^n$ ergibt die *Minkowskisumme* $P_1 + P_2 = \{p_1 + p_2 : p_1 \in P_1, p_2 \in P_2\}$ wiederum ein Polytop. Wir verwenden das übliche Volumen des $\mathbb{R}^n$ und bezeichnen es mit V. Das *Minkowskivolumen* ist unter Translation und Drehung von

Polytopen invariant und lässt sich in allgemeiner Form als Linearkombination der Volumina von Minkowskisummen folgendermaßen darstellen:

$$\begin{aligned}
\mathrm{MV}\big(\mathrm{P}_1,\ldots,\mathrm{P}_\mathrm{n}\big) &= V\big(P_1+\ldots+P_n\big)\\
&- \textstyle\sum_{i=1}^{n} V\big(P_1+\ldots+\hat{P}_i+\ldots+P_n\big)\\
&+ \textstyle\sum_{i<j} V\big(P_1+\ldots+\hat{P}_i+\ldots+\hat{P}_j+\ldots+P_n\big)\\
&\mp \quad\vdots\\
&+ (-1)^{n-2}\textstyle\sum_{i<j} V\big(P_i+P_j\big)\\
&+ (-1)^{n-1}\textstyle\sum_{i=1}^{n} V\big(P_i\big).
\end{aligned}$$

Für $n=2$ ergibt sich somit folgende einfache Formel:

$$\mathrm{MV}\big(P,Q\big) = V\big(P+Q\big) - V\big(P\big) - V\big(Q\big).$$

Das Minkowskivolumen ist insbesondere symmetrisch, d.h., $\mathrm{MV}\big(P_1,\ldots,P_n\big) = \mathrm{MV}\big(P_{\sigma(1)},\ldots,P_{\sigma(n)}\big)$ für jede Permutation σ der Zahlen $1,\ldots,n$ und multilinear, d.h., $\mathrm{MV}\big(\lambda\cdot P_1+\mu\cdot P_1',P_2,\ldots,P_n\big) = \lambda\cdot\mathrm{MV}\big(P_1,\ldots,P_n\big)+\mu\cdot\mathrm{MV}\big(P_1',\ldots,P_n\big)$ für ein weiteres Polytop $P_1'\subset\mathbb{R}^n$ und $\lambda,\mu\in\mathbb{R}_{\geq 0}$.

Sei nun $\Phi\subset\mathbb{C}[x_1,\ldots,x_n]$ die Menge aller Polynome über $\mathbb{C}$ in n Variablen zu einem festen Träger. Jedes $f\in\Phi$ kann als Punkt im Raum $\mathbb{C}^k$ für $k=\#\mathrm{supp}(f)$ aufgefasst werden, wenn wir seine Koeffizienten als Unbestimmte ansehen und somit f in $\mathbb{C}^k$ variieren. Es lässt sich erkennen, dass die Anzahl der gemeinsamen Nullstellen von Polynomen $f_1,\ldots,f_n\in\mathbb{C}[x_1,\ldots,x_n]$ fast immer endlich und unabhängig von den Koeffizienten und somit von der Wahl der Punkte in $\mathbb{C}^{k_i}$ ist, wobei $k_i=\#\mathrm{supp}(f_i)$. So ist die Anzahl der gemeinsamen Nullstellen endlich, wenn die Resultante zweier Polynome f_k und f_l für $1\leq k,l\leq n$ und $k\neq l$ als ein Polynom in den Koeffizienten von f_k und f_l nicht verschwindet. Dies suggeriert die folgende Definition:
Wir nennen die Koeffizienten der Polynome $f_1,\ldots,f_n\in\mathbb{C}[x_1,\ldots,x_n]$ in diesem Zusammenhang *generisch*, wenn ein Polynom ungleich 0 in den Koeffizienten der f_i existiert, das für jedes f_i mit diesen Koeffizienten nicht verschwindet. Dabei sei betont, dass für jedes f_i sein Träger festgehalten wird und seine Koeffizienten variieren. Beispielsweise sind die Koeffizienten $a,b,c\in\mathbb{C}$ eines quadratischen Polynoms $f=ax^2+bx+c$ generisch, wenn f zwei verschiedene komplexe Nullstellen besitzt. Dies ist nämlich genau dann der Fall, wenn die Diskriminante b^2-4ac als ein Polynom in den Koeffizienten von f nicht verschwindet. Ein mathematisch-präzises Kriterium, wann unabhängig von der Wahl der Koeffizienten mit endlich vielen gemeinsamen Nullstellen der $f_1,\ldots,f_n\in\mathbb{C}[x_1,\ldots,x_n]$ gerechnet werden kann, wird hier nicht in Erwägung gezogen, weil die Anwendung des Satzes von Bernstein im Vordergrund steht.

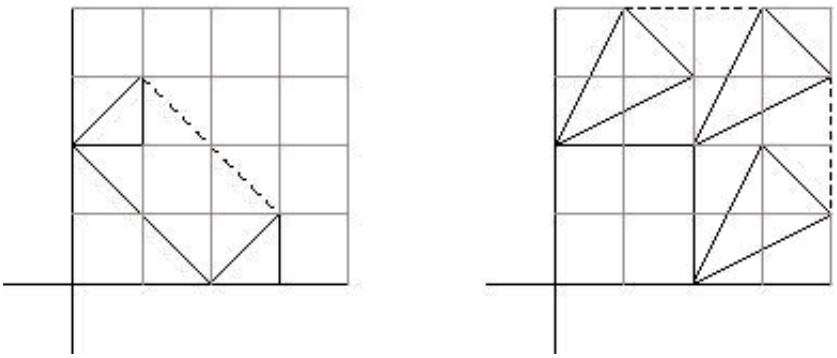
Satz 45 (Bernstein)**.** *Seien $f_1,\ldots,f_n$ Polynome über $\mathbb{C}$ mit endlich vielen gemeinsamen Nullstellen in $(\mathbb{C}\setminus 0)^n$. Sei ferner P_i das Newtonpolytop von f_i im $\mathbb{R}^n$. Dann ist die Anzahl der gemeinsamen Nullstellen der f_i in $(\mathbb{C}\setminus 0)^n$ durch das Minkowskivolumen $\mathrm{MV}\big(P_1,\ldots,P_n\big)$ der Newtonpolytope beschränkt. Falls die Koeffizienten in*

den f_i generisch sind, dann beträgt die Anzahl der gemeinsamen Nullstellen genau $\mathrm{MV}\big(P_1,\ldots,P_n\big)$.

Für den Beweis sei auf [7] p.346 ff verwiesen.

Beispiele. (1) Seien $f := x^2+y^2-3$, $g := xy+x-1$ und $P = N(f)$ und $Q = N(g)$ die beiden entsprechenden Newtonpolytope mit den Volumina $V\big(P\big) = 2$ und $V\big(Q\big) = \frac{1}{2}$. Die Minkowskisumme $V\big(P+Q\big)$ beträgt $\frac{13}{2}$. Die Anzahl der gemeinsamen Nullstellen von f und g ist das Minkowskivolumen von P und Q $\mathrm{MV}\big(P,Q\big) = V\big(P+Q\big) - V\big(P\big) - V\big(Q\big) = 4$.

(2) Seien $f := c_0 + c_1x^2y + c_2xy^2$, $g := d_0 + d_1x^2 + d_2y^2 + d_3x^2y^2 = 0$ und $c_1c_2d_1d_2d_3 \neq 0$. Dann ergibt sich aus $V\big(P\big) = \frac{3}{2}$, $V\big(Q\big) = 4$ und $V\big(P+Q\big) = \frac{27}{2}$ das Minkowskivolumen $\mathrm{MV}\big(P,Q\big) = 8$.



Minkowskisummen der Newtonpolytope aus den Beispielen (1) und (2)

Es wird im Folgenden erörtert, wann alle Polynome eines festen Trägers mit allen Polynomen eines weiteren festen Trägers unter variierenden Koeffizienten genau zwei bzw. drei verschiedene Nullstellen in der affinen Ebene $\mathbb{C}^2$ gemeinsam haben. Dabei sollen die Koeffizienten der Polynome im Sinn der obigen Definition generisch sein. Betrachten wir dazu zwei ebene Kurven $C_1 = V(f_1)$ und $C_2 = V(f_2)$ in der affinen Ebene $\mathbb{C}^2$. Seien $f_1 := \sum_{i,j} a_{ij}x^iy^j$, $f_2 = \sum_{i,j} b_{ij}x^iy^j \in \mathbb{C}[x,y]$ reduzierte bzw. quadratfreie nicht-verschwindende Polynome. Zunächst überlegen wir uns, was die generische Eigenschaft der Koeffizienten von f_1 und f_2 im Fall $n = 2$ bedeutet. Wir stellen folgende Bedingungen an die Koeffizienten:

(1) Zum einen sollen sich C_1 und C_2 nur in endlich vielen Punkten schneiden. Sie sollen also keine gemeinsame Komponente besitzen, d.h., es gelte $\mathrm{Res}_{f_1,f_2} \neq 0$.

(2) Zum anderen soll keine gemeinsame Nullstelle von f_1 und f_2 mehrfach sein. Demzufolge sollen C_1 und C_2 keine gemeinsame Tangente besitzen, woraus sich die Bedingung

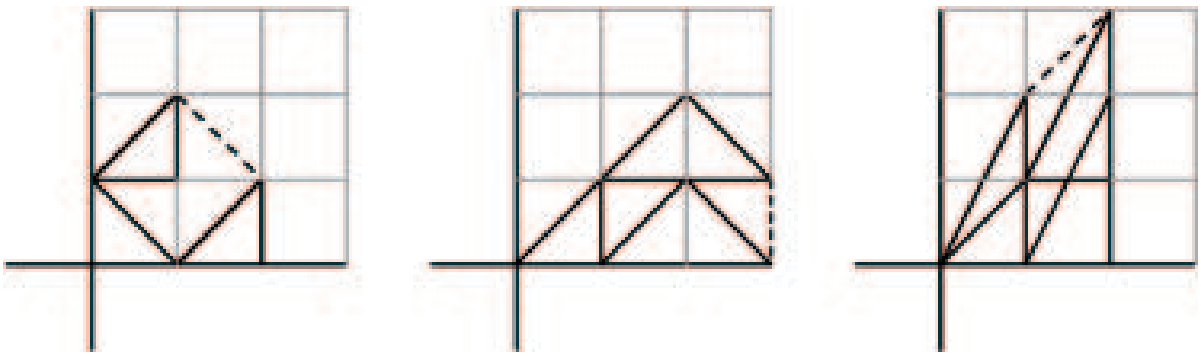
$$\tfrac{\partial f_1}{\partial x}(p)\cdot x + \tfrac{\partial f_1}{\partial y}(p)\cdot y \neq \tfrac{\partial f_2}{\partial x}(p)\cdot x + \tfrac{\partial f_2}{\partial y}(p)\cdot y \text{ für alle } p \in C_1 \cap C_2$$

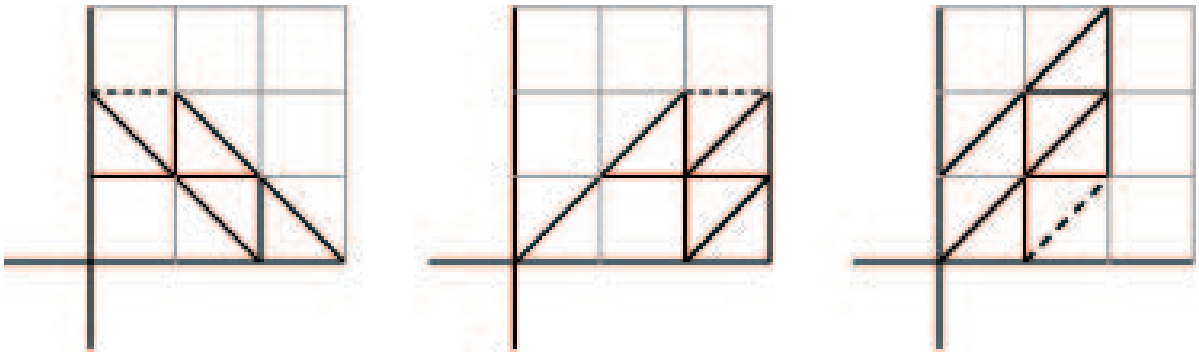
ergibt. Damit muss entweder $\frac{\partial f_1}{\partial x}(p) - \frac{\partial f_2}{\partial x}(p) \neq 0$ oder $\frac{\partial f_1}{\partial y}(p) - \frac{\partial f_2}{\partial y}(p) \neq 0$ für alle $p \in C_1 \cap C_2$ erfüllt sein.

(3) Weiters gelte o.B.d.A $f_1(0,0) \neq 0$ und $f_2(0,0) \neq 0$.

Von jetzt an sollen alle Polynome jene drei Bedingungen erfüllen. Unter dieser Voraussetzung vergleichen wir jetzt alle Polynome eines festen Trägers mit allen Polynomen eines anderen festen Trägers. Dabei wird der Träger zu einem Polynom $f = \sum_{i,j\in\mathbb{N}} c_{ij}x^iy^j \in \mathbb{C}[x,y]$ durch die Gitterpunkte $\{(i,j) \in \mathbb{N}^2 |\ c_{ij} \neq 0\}$ beschrieben. Wir berechnen mit Hilfe des Satzes von Bernstein alle Trägerpaare, für die zwei Polynome aus dem jeweils anderen Träger mit generischen Koeffizienten genau zwei verschiedene gemeinsame Nullstellen besitzen. Das Trägerpaar $\Big(\{(1,0),\{(2,0),(0,2)\}\Big)$bedeute in folgender Auflistung beispielsweise, dass jedes Polynom vom Typ $ax+b$ mit $a,b \in \mathbb{C}\setminus\{0\}$ und ein weiteres Polynom vom Typ $\alpha x^2+\beta y^2+\gamma$ mit $\alpha,\beta,\gamma \in \mathbb{C}\setminus\{0\}$ mit jeweils generischen Koeffizienten genau zwei gemeinsame Nullstellen besitzen. Es ergeben sich 39, also insgesamt (mit Spiegelung der Newtonpolytope an der Diagonalen) 78 Trägerpaare:

$\Big(\{(1,0)\},\{(2,0),(0,2)\}\Big), \Big(\{(1,0)\},\{(1,0),(0,2)\}\Big), \Big(\{(1,0)\},\{(1,0),(1,2)\}\Big), \Big(\{(1,0)\},\{(2,2),(0,2)\}\Big),$
$\Big(\{(1,0)\},\{(2,1),(1,2)\}\Big), \Big(\{(1,0)\},\{(1,0),(0,3)\}\Big), \Big(\{(1,0)\},\{(1,1),(0,2)\}\Big), \Big(\{(1,0)\},\{(2,0),(1,2)\}\Big),$
$\Big(\{(1,0)\},\{(2,1),(0,2)\}\Big), \Big(\{(1,0)\},\{(2,0),(2,2)\}\Big), \Big(\{(1,0)\},\{(1,0),(1,1),(0,2)\}\Big),$
$\Big(\{(1,0)\},\{(1,0),(0,1),(1,2)\}\Big), \Big(\{(1,0)\},\{(1,1),(0,1),(1,2)\}\Big), \Big(\{(1,0)\},\{(1,0),(1,2),(0,2)\}\Big),$
$\Big(\{(1,0)\},\{(1,0),(2,2),(1,2)\}\Big), \Big(\{(1,0)\},\{(1,1),(1,2),(0,2)\}\Big), \Big(\{(1,1)\},\{(1,0),(0,1)\}\Big),$
$\Big(\{(1,1)\},\{(2,0),(2,2)\}\Big), \Big(\{(1,1)\},\{(2,1),(1,2)\}\Big), \Big(\{(1,1),\{(1,1),(0,2)\}\Big),$
$\Big(\{(1,1)\},\{(1,0),(1,1),(0,1)\}\Big), \Big(\{(1,1)\},\{(2,0),(2,1),(1,1)\}\Big), \Big(\{(1,1)\},\{(1,0),(2,1),(0,1)\}\Big),$
$\Big(\{(1,1)\},\{(1,0),(2,2),(1,2)\}\Big), \Big(\{(1,0),(0,1)\},\{(2,0),(0,1)\}\Big), \Big(\{(1,0),(0,1)\},\{(2,0),(1,1)\}\Big),$
$\Big(\{(1,0),(0,1)\},\{(1,0),(1,1)\}\Big), \Big(\{(1,0),(0,1)\},\{(2,0),(0,2)\}\Big), \Big(\{(1,0),(0,1)\},\{(1,0),(1,1),(0,1)\}\Big),$
$\Big(\{(1,0),(0,1)\},\{(2,0),(1,1),(0,1)\}\Big), \Big(\{(1,0),(1,1)\},\{(1,0),(1,2)\}\Big), \Big(\{(1,0),(1,1)\},\{(1,1),(0,1)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(2,0),(2,1)\}\Big), \Big(\{(1,0),(1,1)\},\{(2,0),(2,2)\}\Big), \Big(\{(1,0),(1,1)\},\{(2,0),(1,1)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(1,0),(1,1),(0,1)\}\Big), \Big(\{(1,0),(1,1)\},\{(0,1),(1,2),(1,1)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(2,0),(2,1),(1,1)\}\Big), \Big(\{(1,0),(1,1),(0,1)\},\{(1,0),(1,1),(0,1)\}\Big).$

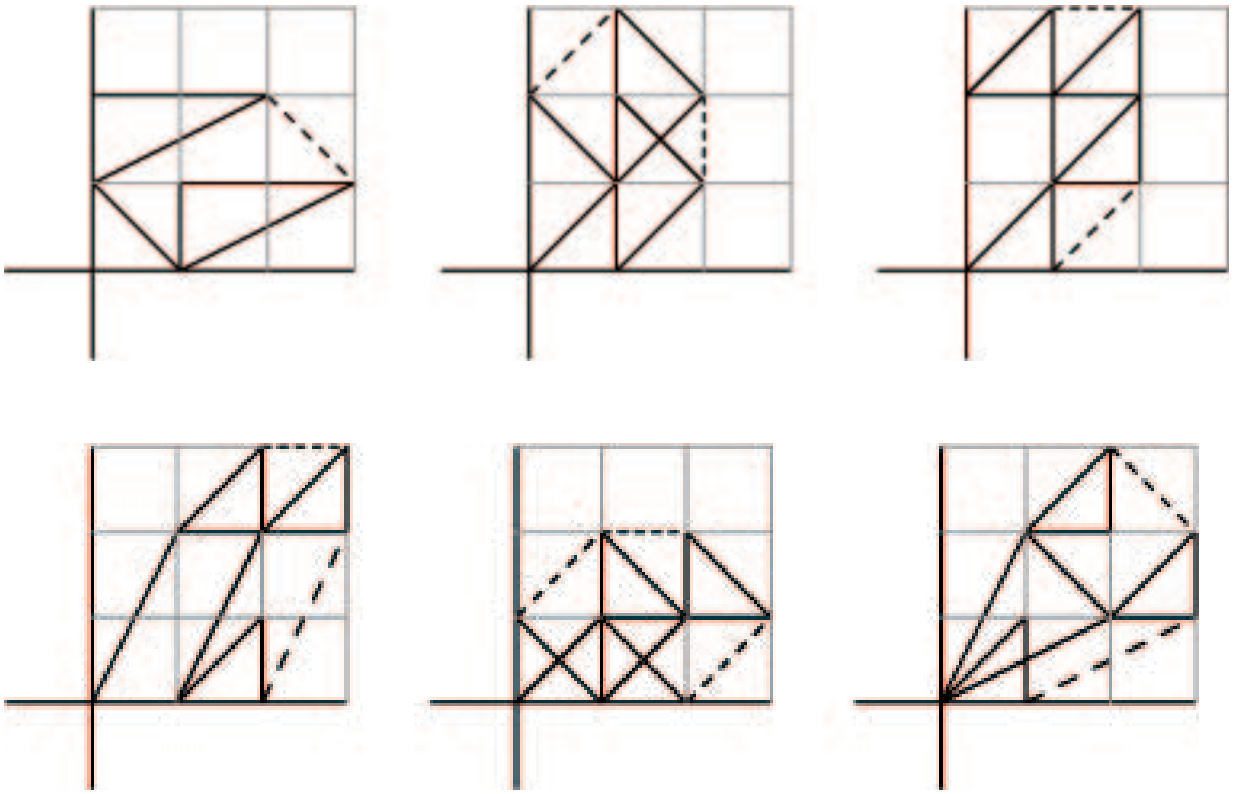




exemparisch sechs Trägerpaare aus obigen 39

Ebenso wurden mit Hilfe des Satzes von Bernstein alle Trägerpaare ermittelt, für die zwei Polynome in $\mathbb{C}[x,y]$ aus dem jeweils anderen Träger mit generischen Koeffizienten genau drei verschiedene gemeinsame Nullstellen besitzen. Wir setzen voraus, dass die Polynome mindestens aus zwei nichtkonstanten linear unabhängigen Termen bestehen, um die Menge überschaubar zu halten. Es ergeben sich mit derselben Notation wie oben 29 Trägerpaare, also insgesamt (mit Spiegelung der Newtonpolytope an der Diagonalen) 58 Trägerpaare::

$\Big(\{(1,0),(0,1)\},\{(2,0),(0,2)\}\Big), \Big(\{(1,0),(0,1)\},\{(2,0),(2,1)\}\Big), \Big(\{(1,0),(0,1)\},\{(2,1),(0,1)\}\Big),$
$\Big(\{(1,0),(0,1)\},\{(2,1),(1,2)\}\Big), \Big(\{(1,0),(0,1)\},\{(3,0),(0,1)\}\Big),$
$\Big(\{(1,0),(0,1)\},\{(1,0),(2,1),(1,1)\}\Big), \Big(\{(1,0),(0,1)\},\{(1,0),(2,1),(0,1)\}\Big),$
$\Big(\{(1,0),(0,1)\},\{(2,0),(2,1),(1,1)\}\Big), \Big(\{(1,0),(0,1)\},\{(3,0),(1,1),(0,1)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(1,0),(0,2)\}\Big), \Big(\{(1,0),(1,1)\},\{(2,0),(0,1)\}\Big), \Big(\{(1,0),(1,1)\},\{(0,1),(2,1)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(2,0),(1,2)\}\Big), \Big(\{(1,0),(1,1)\},\{(2,1),(1,2)\}\Big), \Big(\{(1,0),(1,1)\},\{(1,1),(0,2)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(2,0),(1,1),(0,1)\}\Big), \Big(\{(1,0),(1,1)\},\{(1,0),(1,1),(0,2)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(1,0),(2,1),(0,1)\}\Big), \Big(\{(1,0),(1,1)\},\{(0,2),(1,1),(1,2)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(1,0),(0,1),(1,3)\}\Big), \Big(\{(1,0),(1,1)\},\{(1,0),(2,2),(1,2)\}\Big),$
$\Big(\{(1,0),(1,1)\},\{(0,1),(2,2),(2,1)\}\Big), \Big(\{(1,0),(1,1),(0,1)\},\{(2,0),(0,1)\}\Big),$
$\Big(\{(1,0),(1,1),(0,1)\},\{(2,0),(1,1)\}\Big), \Big(\{(1,0),(1,1),(0,1)\},\{(1,0),(1,2)\}\Big),$
$\Big(\{(1,0),(1,1),(0,1)\},\{(1,0),(2,1),(1,1)\}\Big), \Big(\{(1,0),(1,1),(0,1)\},\{(2,0),(1,1),(0,1)\}\Big),$
$\Big(\{(1,0),(1,1),(0,1)\},\{(1,0),(2,1),(0,1)\}\Big), \Big(\{(1,0),(1,1),(0,1)\},\{(2,0),(2,1),(1,1)\}\Big).$



exemparisch sechs Trägerpaare aus obigen 29

4.2 Wavelets als Anwendung

Vor der eigentlichen Anwendung des Satzes von Bernstein werden jetzt Wavelets als ein wichtiges Werkzeug in der Signal- und Bildverarbeitung marginal erörtert. Detaillierte Ausführungen findet man in [6] und [7].
Wir betrachten dazu den Vektorraum der quadratintegrablen Funktionen über $\mathbb{R}$

$$L^2(\mathbb{R}) := \{f : \mathbb{R} \to \mathbb{R} | \int_{-\infty}^{\infty} |f(x)|^2 \, dx < \infty\}.$$

Der Träger eines $f \in L^2(\mathbb{R})$ ist hier definiert durch

$$\text{supp}(f(x)) = \{x \in \mathbb{R} |\ f(x) \neq 0\}.$$

Man nennt $\psi \in L^2(\mathbb{R})$ ein *orthogonales Wavelet*, wenn seine Translationen und Dilationen $\psi_{jk}(x) = 2^{-\frac{j}{2}}\psi(2^{-j}x - k)$ für $j, k \in \mathbb{Z}$ eine Orthonormalbasis des $L^2(\mathbb{R})$ bilden. Dies ist genau dann der Fall, wenn zwei Bedingungen erfüllt sind. Zum einen muss für alle $j, k \in \mathbb{Z}$ die Normierung $\|\psi_{j,k}\|_2 = 1$ gelten. Zum anderen muss zu jedem $\epsilon > 0$ für alle quadratintegrablen Funktionen $f \in L^2(\mathbb{R})$ mit kompaktem Träger Koeffizienten $a_{jk} \in \mathbb{R}$ existieren mit $\|f - \sum_{j,k\in\mathbb{Z}} a_{jk}\psi_{jk}\|_2 < \epsilon$.
Die Konstruktion von orthogonalen Wavelets erfolgt durch sogenannte *skalierende*

Funktionen. Indem man für die skalierende Funktion $\varphi(x)$ Normalisierung, Orthonormalität und die Trägerbedingung $\text{supp}(\varphi(x)) = [1-n, n]$ für eine ganze Zahl n voraussetzt, erhält man durch

$$\psi(x) := \sum_{k=1-n}^{n} (-1)^k h_{1-k} \varphi(2x-k)$$

ein Wavelet. Dabei werden die Konstanten $h_k \in \mathbb{C}$ als Filterkoeffizienten bezeichnet. Es ergibt sich folgendes Gleichungssystem mit $2n$ unbestimmten Filterkoeffizienten h_k und $2n+1$ algebraischen Gleichungen, wobei $1-n \leq k \leq n$, $0 \leq l \leq n-1$:

(1)
$$\sum_{k=1-n}^{n} h_k = 2,$$

(2)
$$\sum_{k=1-n}^{n} h_k h_{k-2l} = 2\delta_{0,l},$$

(3)
$$\sum_{k=1-n}^{n} (-1)^k k^l h_{1-k} = 0,$$

(4)
$$h_k = 0 \text{ für } k < 1-n \text{ oder } k > n.$$

Speziell für $n = 1$ erhalten wir $h_0 = h_1 = 1$.
Ziel dieses Kapitels ist es zu zeigen, dass die Anzahl der Lösungen dieses Gleichungssystems durch eine Zahl beschränkt ist, die nur von n abhängt. Das Gleichungssystem der Filterkoeffizienten lässt sich durch lineare Koordinatenwechsel in ein neues System umschreiben (siehe dazu [6] S.70 ff). Wir erhalten folgendes System mit n Gleichungen in n Unbekannten Q_j:

(1′)
$$\sum_{j=0}^{n-1} 2^{-j} Q_j = 2^{2-2n}.$$

(2′)
$$\sum_{i,j=0}^{n-1} \binom{4n-i-j-2}{2n+2l-i-1} Q_i Q_j = 0 \text{ für } l = 1, \ldots, n-1.$$

Der folgende Satz untermauert, dass die Systeme (1), (2), (3), (4) und (1′), (2′) äquivalente Beschreibungen derselben Nullstellenmenge sind. Sei X bzw. Y die algebraische Lösungsmenge des Gleichungssystems (1), (2), (3), (4) bzw. (1′), (2′).

Satz 46. *Es existiert ein lineare Abbildung φ zwischen $\mathbb{C}^n$ und $\mathbb{C}^{2n}$ die Y isomorph auf X abbildet.*

Für den Beweis sei auf [6] p.72 ff verwiesen. Ein *n-dimensionaler Simplex der Seitenlänge* $k \in \mathbb{N}$ ist die konvexe Hülle der Gitterpunkte $(0,\dots,0)$, $(k,0,\dots,0)$, $(0,k,0,\dots,0)$, $\dots,(0,\dots,0,k) \in \mathbb{N}^n$. Wir symbolisieren ihn mit $\triangle_k^n$. Mit diesen Grundlagen kann der nächste Satz unter Zuhilfenahme des Satzes von Bernstein bewiesen werden.

Satz 47. *Die beiden Systeme* (1), (2), (3), (4) *und* (1′), (2′) *besitzen höchstens* 2^{n-1} *verschiedene Lösungen in* $\mathbb{C}$.

Beweis: Sei o.B.d.A. $Q_j \neq 0$ für alle $j = 0,\dots,n-1$ und $n \geq 2$. Weil die Gleichung (1′) in den Unbekannten Q_j linear ist, erhalten wir als Newtonpolytop $P = \triangle_1^n$. Die $n-1$ Gleichungen aus (2′) sind quadratisch in den Unbekannten Q_j, woraus sich jeweils das Newtonpolygon $Q = \triangle_2^n$ ergibt. Nach dem Satz von Bernstein lässt sich die Anzahl der gemeinsamen Nullstellen der n Gleichungen aus (1′) und (2′) durch das Minkowskivolumen über $n-1$ mal Q und einmal P nach oben abschätzen.
Das Volumen der folgenden Minkowskisumme lässt sich leicht berechnen:

$$V\big(l \cdot P\big) = \frac{l^n}{n!} \text{ für } l \in \mathbb{N}.$$

Mit Hilfe der allgemeinen Formel für das Minkowskivolumen erhalten wir

$$MV\big(\underbrace{Q,\dots,Q}_{n-1},P\big) = \mathrm{MV}\big(\underbrace{2P,\dots,2P}_{\mathrm{n-1}},\mathrm{P}\big) \overbrace{=}^{\text{MV multilinear}} 2^{\mathrm{n-1}}\mathrm{MV}\big(\underbrace{P,\dots,P}_{\mathrm{n}}\big)$$

$$\begin{aligned}
= 2^{n-1}\Big(& V\big(n \cdot P\big) \\
- & \tbinom{n}{1} V\big((n-1)\cdot P\big) \\
+ & \tbinom{n}{2} V\big((n-2)\cdot P\big) + \\
\mp & \quad \vdots \\
+ & (-1)^{n-1}\tbinom{n}{n-1} V\big(P\big)\Big)
\end{aligned}$$

$$= 2^{n-1}\Big(\frac{1}{n!}\sum_{k=0}^{n-1}(-1)^k\binom{n}{k}(n-k)^n\Big).$$

Es genügt daher zu zeigen, dass

$$\sum_{k=0}^{n-1}(-1)^k\binom{n}{k}(n-k)^n = n!.$$

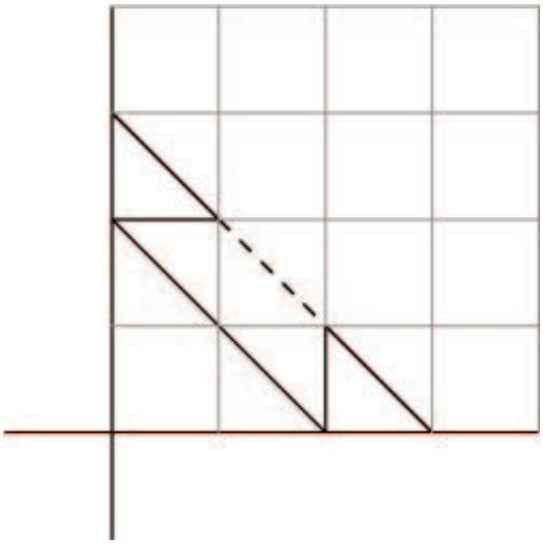
Dieses kombinatorische Problem wird nun mittels Abzählung von bijektiven Abbildungen auf sich selbst (i.e. Permutationen) gelöst. Im Folgenden sei $[n] := \{1,\dots,n\}$ eine aus n verschiedenen Elementen bestehende Menge.

Es gibt $n!$ Möglichkeiten, $[n]$ auf sich selbst abzubilden. Diese Anzahl an Möglichkeiten lässt sich auch anhand von einer komplizierteren Abzählung bestimmen.

Man betrachtet dazu alle Abbildungen von $[n]$ nach $[n]$. Davon existieren n^n, weil dies der Anzahl entspricht, aus n verschiedenen Elementen n geordnete Elemente mit Wiederholung auszuwählen. Dabei ist n^n der erste Summand in obiger Summe. Jetzt werden alle nicht-injektiven Abbildungen subtrahiert, demnach die Anzahl aller Abbildungen von $[n]$ nach $[n-1]$, wobei $[n-1]$ für eine $(n-1)$-elementige Menge der Dimension n steht. Insgesamt ergeben sich $\binom{n}{1}(n-1)^n$ Abbildungen, was dem zweiten Summanden entspricht.

Nun wurden aber einige Abbildungen doppelt abgezogen. Zum Beispiel haben wir sowohl die Anzahl aller Abbildungen von $[n]$ nach $\{1,\ldots,n-2,n-1\}$ als auch von $[n]$ nach $\{1,\ldots,n-2,n\}$ subtrahiert. Somit wurden in diesem Fall die Abbildungen von $[n]$ nach $\{1,\ldots,n-2\}$ doppelt gezählt. Weil jeweils zwei der n $(n-1)$-elementigen Bildmengen genau $n-2$ gemeinsame Elemente besitzen, erhalten wir insgesamt $\binom{n}{2}(n-2)^n$ zu addierende Abbildungen (dritter Summand).

Mittels Iteration gelangt man zur gewünschten, alternierenden Summe. Somit ist gezeigt, dass die zwei Systeme höchstens 2^{n-1} verschiedene Lösungen besitzen. □



Minkowskisumme der Newtonpolytope $\triangle_1^2$ und $\triangle_2^2$ aus $(1')$ und $(2')$ für $n=2$

In diesem Zusammenhang habe ich gezeigt, dass 2^{n-1} eine obere Schranke für die Differenz von Volumina n-dimensionaler Simplices mit unterschiedlichen Seitenlängen $V\big(\triangle_3^n\big) - V\big(\triangle_2^n\big) - V\big(\triangle_1^n\big)$ ist. Der entsprechende dieses Kapitel abschließende Satz wird in dieser Diplomarbeit zwar nicht konkret angewandt. Er wird aber trotzdem aufgrund seiner gewissen Aussagekraft eingebaut.

Satz 48. *Es gilt*

$$V\big(\triangle_3^n\big) - V\big(\triangle_2^n\big) - V\big(\triangle_1^n\big) = \frac{1}{n!}3^n - \frac{1}{n!}2^n - \frac{1}{n!} \leq 2^{n-1}$$

für $n \in \mathbb{N}$ *und* $n \geq 2$.

Beweis: Für $n = 2$ ist die Ungleichung erfüllt.
Unter der Annahme, dass die Ungleichung für n gilt, ist also

$$3^{n+1} - 2^{n+1} \leq (n+1)! \cdot 2^n + 1$$

zu zeigen. Man schreibt dazu

$$3^{n+1} - 2^{n+1} = (3-2)(3^n + 3^{n-1} \cdot 2 + \ldots + 3 \cdot 2^{n-1} + 2^n) = 3^n + 2^n + \sum_{j=1}^{n-1} 2^j \cdot 3^{n-j}.$$

Wir zeigen jetzt mittels einer weiteren Induktion, dass die Behauptung

$$\sum_{j=1}^{m-1} 2^j \cdot 3^{m-j} = 2 \cdot 3^m - 2^m \cdot 3$$

gilt: Für $m = 2$ stimmt die Behauptung. Man bildet nun den Induktionsschluss von $m-1$ auf m:

$$\sum_{j=1}^{m} 2^j \cdot 3^{m+1-j} = 2 \sum_{j=1}^{m-1} 2^j \cdot 3^{m-j} + 2 \cdot 3^m = 2 \cdot (2 \cdot 3^m - 2^m \cdot 3) + 2 \cdot 3^m = 2 \cdot 3^{m+1} - 2^{m+1} \cdot 3.$$

Zu zeigen ist also

$$3^n - 2^n + 2 \cdot 3^n - 2^n \cdot 3 \leq (n+1)! \cdot 2^n - 2^{n+1} + 1.$$

Nach Induktionsvoraussetzung gilt aber $3^n - 2^n \leq n! \cdot 2^{n-1} + 1$. Wegen $2^{n+1} \leq 3 \cdot 2^n$ genügt es zu zeigen, dass

$$\frac{n!}{2} + \frac{3^n}{2^{n-1}} \leq (n+1)!.$$

Für $2 \leq n \leq 6$ ist diese Ungleichung erfüllt. Sei jetzt $n \geq 7$. Dann ist $3^n \leq n!$ und es gilt

$$\frac{n!}{2} + \frac{3^n}{2^{n-1}} \leq \frac{n!}{2} + \frac{n!}{2} \leq n! \leq (n+1)!.$$

□

Kapitel 5

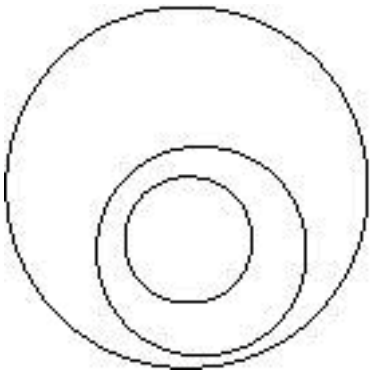
Schubert-Kalkül

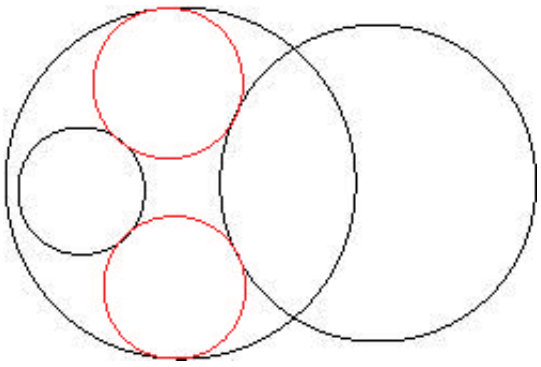
Das Schubert-Kalkül gehört zur abzählenden Geometrie, deren Ziel es ist, alle Fragen von folgender Form zu beantworten:

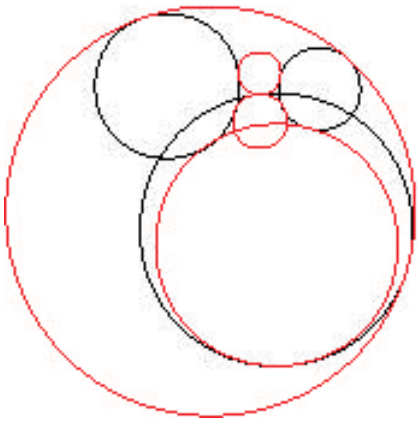
Wieviele geometrische Gebilde erfüllen gewisse gegebene Bedingungen?

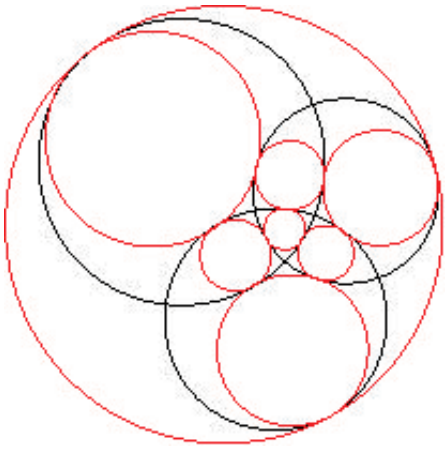
Die entsprechenden Anzahlen hängen demnach sowohl von der jeweiligen Definition der Gebilde als auch von den Bedingungen ab, die jene Gebilde erfüllen sollen. Es wird vorausgesetzt, dass man die Gebilde und ihre Bedingungen durch algebraische Gleichungen über einem algebraisch abgeschlossenen Körper ausdrücken kann. Die Notwendigkeit der algebraischen Abgeschlossenheit sieht man an folgendem

Beispiel 5.1. Die Anzahl von reellen Kreisen, die zu drei gegebenen reellen Kreisen tangential sind, ist null, zwei, vier oder acht, was die vier Abbildungen unten visualisieren. Im Komplexen dagegen gibt es stets acht Kreise, weil wir nach dem Prinzip von der Erhaltung der Anzahl (siehe unten) annehmen dürfen, dass sich die drei gegebenen Kreise paarweise schneiden.









Schubert nennt im dreidimensionalen Raum c die Konstantenzahl eines Gebildes, wenn zur analytisch-geometrischen Darstellung dieses Gebildes c Konstanten benötigt werden. Sie entspricht also der kleinstmöglichen Anzahl von Zahlen, die zur eindeutigen Beschreibung eines Gebildes mit gewissen Bedingungen notwendig sind.

Beispiele. Die Konstantenzahl
(1) eines Punktes wie einer Ebene ist im Raum 3, einer Geraden 4,
(2) eines Punktepaares $2 \cdot 3$, einer Strecke von bestimmter Länge $2 \cdot 3 - 1$,
(3) eines Dreiecks im Raum 9, eines Dreiecks in fester Ebene 6,
(4) eines n-eckigen Polyeders mit Dreiecken als Grenzflächen $3 \cdot n$,
(5) eines ebenen n-Ecks im Raum $2 \cdot n + 3$,
(6) einer geraden Punktgruppe (Gerade mit n darauf liegenden Punkten) $4 + n$,
(7) eines Geradenbündels 5,
(8) eines aus n in einem Geradenbündel liegenden Geraden bestehendes Gebildes $5 + n$.

Satz 49. *Die Konstantenzahl eines beliebigen Polyeders mit k Kanten beträgt $k+6$.*

Beweis: Seien e ,f, k die Anzahl der Ecken, Flächen, Kanten eines Polyeders. Man zerlege jedes eine Fläche bildende n-Eck durch Ziehen von $n-3$ Diagonalen in $n-2$ Dreiecke. Auf den f Flächen seien nun d Diagonalen zur Zerlegung erforderlich. Wenn nun δ die Anzahl der entstandenen Dreiecke ist, dann ist δ um f größer als d, weil auf jeder Fläche ein Dreieck mehr entsteht, als Diagonalen zur Zerlegung notwendig sind. Daher gilt

$$\delta = d + f.$$

Ferner sind die 3δ Seiten der δ Dreiecke zum einen Teil die d Diagonalen, zum anderen Teil die k Kanten. Weil aber jede der d Diagonalen und jede der k Kanten zweimal als Dreiecksseite auftritt, gilt

$$3\delta = 2d + 2k.$$

Aus beiden Gleichungen folgt

$$d = 2k - 3f.$$

Man kann ein Polyeder, das zur Zerlegung der Flächen in Dreiecke d Diagonalen erfordert, als ein Dreieckspolyeder ansehen mit der zusätzlichen Eigenschaft, dass

an d Kanten der Neigungswinkel der zusammenstoßenden Flächen den speziellen Wert 180 Grad besitzt. Folglich ist die Konstantenzahl c eines beliebigen Polyeders um d kleiner als die eines Dreieckspolyeders von gleicher Eckenzahl e. Es ergibt sich also

$$c = 3e - d$$

und nach Substitution des abgeleiteten Wertes für d

$$c = 3e + 3f - 2k.$$

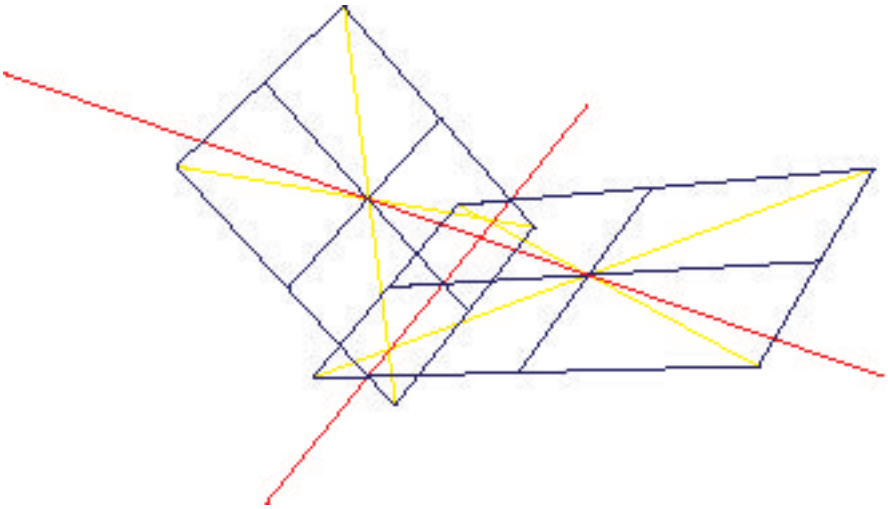
Die Euler'sche Gleichung $f + e - k = 2$ liefert das gewünschte Resultat

$$c = k + 6.$$

□

Das *Stetigkeitsprinzip von Poncelet* besagt, dass die Anzahl von Lösungen unter stetiger Transformation der jeweiligen Objekte gleich bleibt. Zwei Kreise schneiden sich beispielsweise stets in zwei Punkten, sei es, dass diese reell und verschieden sind, durch Verschieben der Kreise zusammenfallen oder imaginär und verschieden werden. Eine Verallgemeinerung des Poncelet'schen Stetigkeitsprinzips stellt das *Prinzip von der Erhaltung der Anzahl* von Schubert dar. Dieses bedeutet, dass die Anzahl von Lösungen eines abzählenden Problems mit Vielfachheit dieselbe bleibt, wenn die Parameter der Bedingung verändert werden, vorausgesetzt die Zahl bleibt endlich. Insbesondere wenn man die Koeffizienten eines homogenen Polynoms abändert, bleibt die Anzahl der Nullstellen mit Vielfachheit erhalten oder das Polynom verschwindet. Geometrisch bedeutet dies Folgendes: Eine endliche Anzahl räumlicher Individuen wird unendlich oder bleibt erhalten, wenn gegebene Gebilde zueinander spezielle Lagen im Raum einnehmen oder ausarten.

Beispiel 5.2. Gesucht sei die Anzahl von Geraden, die durch vier gegebene Geraden im Raum gehen. Nach dem Prinzip von der Erhaltung der Anzahl können wir annehmen, dass sich jeweils zwei Geraden schneiden. Die Annahme jedoch, dass sich drei Geraden in einem Punkt schneiden, wäre unzulässig, weil dann die Anzahl der Lösungen unendlich würde.
Es treten zwei Geraden auf, die durch vier gegebene Geraden gehen, nämlich die eine durch die beiden Schnittpunkte und die andere als Schnittgerade der beiden Schnittebenen.



Vier gegebene Geraden (gelb) und die zwei gesuchten Geraden (rot)

Schubert nennt die Anwendung dieser Technik das Kalkül der abzählenden Geometrie. Das Schubert-Kalkül zu verwenden bedeutet, gegebene Bedingungen in Standardbedingungen, also das originale Problem in eine Reihe von bereits gelösten Problemen zu zerlegen.
Die grundlegende Idee des Schubert-Kalküls ist, dass ein algebraisches Symbol für eine geometrische Bedingung steht. Wenn zwei unabhängige Bedingungen mit den Symbolen x und y gegeben sind, dann wird die neue Bedingung, welche entweder x oder y erfüllt, durch die Summe $x + y$, und diejenige, die beide erfüllt, durch das Produkt $x \cdot y$ dargestellt. Das Gleichheitszeichen zwischen Summen und Produkte der algebraischen Symbole steht für die Äquivalenz zwischen den Bedingungen auf der linken Seite und den Bedingungen auf der rechten Seite der Gleichung. Die Gleichung drückt ferner aus, dass die Anzahl von Gebilden auf der linken und rechten Seite der Gleichung, welche die jeweiligen Bedingungen erfüllen, gleich ist. Eine Bedingung kann durch Multiplikation symbolisch zu null werden, wenn sie nicht eintreten kann.

Im Folgenden werden algebraische Symbole eingeführt, welche Bedingungen der drei Hauptelemente Punkt, Gerade und Ebene symbolisieren. Dabei ist ein festes Hauptelement gegeben, wenn man seine wesentlichen Konstanten zur analytisch-geometrischen Darstellung kennt. Weil aber das jeweilige Hauptelement variiert, bedeutet „gegeben“ in diesem Zusammenhang einen situationsbedingten Zustand (Sprechweise „immer dann, wenn...“).

Definition. (1) Für einen Punkt P bedeute

(a) p die Bedingung, dass P gleich einem gegebenen Punkt ist,
(b) p_g die Bedingung, dass P auf einer gegebenen Gerade liegt,
(c) p_e die Bedingung, dass P auf einer gegebenen Ebene liegt.

(2) Steht E für eine Ebene, so bezeichne

(a) e die Bedingung, dass E gleich einer gegebenen Ebene ist,

(*b*) e_p die Bedingung, dass E durch einen gegebenen Punkt geht,
(*c*) e_g die Bedingung, dass E durch eine gegebene Gerade geht.

(3) Für eine Gerade G bedeute

(*a*) g die Bedingung, dass G gleich einer gegebenen Gerade ist,
(*b*) g_p die Bedingung, dass G durch einen gegebenen Punkt geht,
(*c*) g_e die Bedingung, dass G in einer gegebenen Ebene liegt,
(*d*) g_s die Bedingung, dass G in einem gegebenen Geradenbündel liegt,
(*e*) $g_\cap$ die Bedingung, dass G eine gegebene Gerade schneidet.

Es sei darauf hingewiesen, dass diese Form der Notation mathematisch inkorrekt ist. Das Produkt $p_e \cdot p_e$ bedeutet etwa, dass der Punkt P auf zwei verschiedenen Ebenen liegt. Zur Bewahrung der Übersichtlichkeit soll ein dritter Parameter vermieden werden.
Weiters sollen die Gebilde im Raum nach dem Prinzip der Erhaltung der Anzahl keine speziellen Lagen zueinander einnehmen. Für die Bedingung $p_e \cdot p_g$ bedeutet dies etwa, dass die gegebene Gerade nicht in der gegebenen Ebene liegt, weil ansonsten unendlich viele Punkte jene Bedingung erfüllten. Von jetzt an seien die Gebilde stets in genügend allgemeiner Lage, also *generisch*, d.h., sie nehmen keine so speziellen Lagen zueinander ein noch arten sie derart aus, dass die Anzahl der Lösungen unendlich wird.

Die Bedingung, dass ein Punkt P auf zwei Ebenen liegt, ist äquivalent zur Bedingung, dass P auf der Schnittgerade der beiden Ebenen liegt. Mit obiger Festsetzung der Symbole bedeutet Letzteres

$$p_e^2 = p_g.(*)$$

Zudem gilt

$$p_e \cdot p_g = p,$$

weil sich Ebene und Gerade in genau einem Punkt schneiden. Multiplikation von $(*)$ mit p_e liefert

$$p_e^3 = p_e \cdot p_g = p.$$

Folglich schneiden sich drei generische Ebenen in einem Punkt. Analog ergibt sich aus den Gleichungen

$$e_p^2 = e_g$$

und

$$e_p \cdot e_g = e$$

die Gleichung

$$e_p^3 = e_p \cdot e_g = e.$$

Damit ist eine Ebene bereits eindeutig festgelegt, wenn man drei nicht kollineare Punkte kennt, die sie enthält.

Wir zeigen nun anhand dieser neuen Methode das Resultat obigen Beispiels:

Satz 50. *Es existieren genau zwei Geraden, die durch vier gegebene Geraden gehen.*

Es sei noch einmal darauf hingewiesen, dass alle Gebilde als generisch angenommen werden. Im folgenden Beweis wird das Schubert-Kalkül verwendet, d.h., das Problem in eine Reihe von lösbaren Problemen zerlegt.

Beweis: Die Bedingung an eine Gerade G, dass sie in einem gegebenen Geradenbündel liegt, ist äquivalent zur Bedingung, dass sie durch einen gegebenen Punkt (i.e. Knoten des Geradenbündels) geht und eine gegebene Gerade schneidet. Die erste Bedingung ist ebenso erfüllt, wenn G eine gegebene Gerade schneidet und in einer gegebenen Ebene liegt. Dabei ist der Knoten des Geradenbündels der Schnittpunkt der gegebenen Ebene mit der gegebenen Geraden. Somit gelten

$$g_\cap \cdot g_p = g_s.$$

und

$$g_\cap \cdot g_e = g_s.$$

Weiters gibt es genau eine Gerade, die in einem gegebenen Geradenbündel liegt und eine gegebene und nicht in der vom Geradenbündel aufgespannten Ebene befindliche Gerade schneidet, d.h.,

$$g_\cap \cdot g_s = g.$$

Schneidet eine Gerade zwei gegebene Geraden, so kann man nach dem Prinzip der Erhaltung der Anzahl annehmen, dass sich die beiden gegebenen Geraden schneiden. Dann muss die Gerade aber entweder durch jenen Schnittpunkt gehen oder in der von den beiden Geraden aufgespannten Ebene liegen. Daher gilt

$$g_\cap^2 = g_p + g_e.$$

Insgesamt erhalten wir durch Multiplikation mit $g_\cap$

$$g_\cap^3 = g_\cap \cdot g_p + g_\cap \cdot g_e = 2g_s$$

und

$$g_\cap^4 = 2g_\cap \cdot g_s = 2g.$$

□

Das im Folgenden näher betrachtete Gebilde besitze eine Gerade G und auf derselben einen Punkt P. Dann lassen sich folgende auf G und P bezogene Bedingungen angeben:

$$p_e^2, p_e, g_p, p_e \cdot g_\cap.$$

Die letzte Bedingung bedeutet, dass der Punkt P auf einer gegebenen Ebene liegt und zugleich die Gerade G eine gegebene Gerade schneidet. Nach dem Prinzip von der Erhaltung der Anzahl dürfen wir die gegebene Gerade in die gegebene Ebene legen. Ist die Gerade G nicht in der gegebenen Ebene enthalten, so muss sie die gegebene Gerade in P schneiden. Andernfalls liegt G in der gegebenen Ebene und somit erhalten wir folgende Formel:

$$p_e \cdot g_\cap = p_g + g_e = p_e^2 + g_e.(\#)$$

Multiplikation mit p_e und $g_\cap$ liefert die Resultate

$$p_e^2 \cdot g_\cap = p_e^3 + p_e \cdot g_e$$

und

$$p_e \cdot \underbrace{g_\cap^2}_{g_p+g_e} = p_e^2 \cdot g_\cap + \underbrace{g_e \cdot g_\cap}_{g_s}.$$

Eingesetzt erhält man mit den Formeln aus dem Beweis von Satz **??**

$$p_e \cdot g_e + p_e \cdot g_p = p_e^2 \cdot g_\cap + g_s,$$

woraus sich durch Addition

$$p_e \cdot g_p = p_e^3 + g_s$$

ergibt.
Durch Multiplikation von (#) mit p_e^2, g_p und g_e erhalten wir weiters

$$\underbrace{p_e^3}_{p} \cdot g_\cap = 0 + p_e^2 \cdot g_e,$$

$$p_e \cdot \underbrace{g_\cap \cdot g_p}_{g_s} = p_e^2 \cdot g_p + 0,$$

und

$$p_e \cdot \underbrace{g_e \cdot g_\cap}_{g_s} = p_e^2 \cdot g_e + g.$$

Die letzten drei Formeln führen zu folgender Gleichung:

$$p_e \cdot g_s = p_e^2 \cdot g_p = p \cdot g_\cap + g = p_e^2 \cdot g_e + g.(\Delta)$$

Das erste Gleichheitszeichen in (Δ) besagt, dass genau dann ein Punkt P in einer Ebene liegt und eine Gerade G durch P einem Geradenbündel angehört, wenn P auf zwei gegebenen Ebenen, also auf einer Geraden (Schnitt des Geradenbündels mit der Ebene) liegt und zusätzlich G durch einen gegebenen Punkt (Knoten des Geradenbündels) geht.
In unserer Situation gehen G und eine weitere gegebene Gerade jeweils durch P. Falls G und die gegebene Gerade zusammenfallen, ist G gleich einer gegebenen Geraden und damit bereits eindeutig festgelegt. Falls dies nicht eintritt, so muss P gleich einem gegebenen Punkt sein und G die gegebene Gerade schneiden, was die zweite Gleichung bedeutet. Die eben genannte Bedingung ist äquivalent dazu, dass P in einer gegebenen Gerade und G in einer gegebenen Ebene liegt.

Schubert baut auf diesen fundamentalen Formeln ein äußerst komplexes Konstrukt auf. Im Zuge dessen bewältigt er beispielsweise folgende, scheinbar-unlösbare Probleme:

(1) Die Anzahl von Kegelschnitten, die zu fünf gegebenen Kegelschnitten tangential sind, beträgt 3264 ([10] p.97).

(2) Es gibt 666841088 Quadriken, die zu neun gegebenen Quadriken tangential sind ([10] p.106).

(3) Die Anzahl von gedrehten Kubiken, die zu zwölf quadratischen Flächen tangential sind, beträgt 5819539783680 ([10] p.184).

Kapitel 6

Sperner-Lemma

In diesem Kapitel wird das Sperner-Lemma behandelt. Es liefert einen elementaren Beweis des Brouwer'schen Fixpunktsatzes.
Betrachten wir eine stetige Funktion f vom Einheitskreis S^1 in die reellen Zahlen $\mathbb{R}$. Es existiert eine bijektive Abbildung von S^1 in ein halboffenes Intervall der Länge 2π in $\mathbb{R}$. Daher können wir $f : [0, 2\pi[\to \mathbb{R}$ annehmen. Weil $f(0) = f(\pi)$, ist die Anzahl der Vorzeichenwechsel von f gerade.
Sei nun o.B.d.A. $f(0) = 0$. Interpretieren wir $\bullet$ bzw. $\circ$ als denjenigen Bereich, in dem f positiv bzw. negativ ist, so ist die Anzahl der zweifarbigen Intervalle in $[0, 2\pi[$ um eins geringer als die Anzahl der Vorzeichenwechsel von f in $[0, 2\pi[$ und daher ungerade.
Die Färbungen innerhalb eines Intervalls lassen sich im nachfolgenden Sperner-Lemma auf Färbungen eines triangulierten Dreiecks erweitern.

Lemma (Sperner)**.** *Ein Dreieck werde beliebig in kleinere Dreiecke trianguliert. Jedem Knoten werde ferner genau eine Farbe mit der jeweiligen Bezeichnung* 1*,* 2 *oder* 3 *nach folgenden Rechenregeln zugewiesen:*

(1) *Die Eckpunkte des Dreiecks sind verschieden gefärbt.*

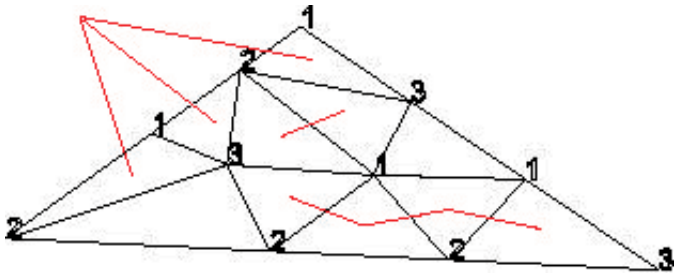
(2) *Alle Knoten auf der i, j-Seite des Dreiecks sind entweder mit der Farbe i oder j gefärbt.*

(3) *Alle inneren Knoten dürfen beliebig gefärbt werden.*

Dann gibt es ein dreifarbiges Dreieck. Ferner ist die Anzahl der dreifarbigen Dreiecke ungerade.
Im Folgenden sind drei Beweise des Sperner-Lemmas angeführt. Der erste Beweis erfolgt mittels graphentheoretischer Überlegung:

Beweis 1. Man betrachte den dualen Graphen zu der Triangulierung mit eingeschränkter Kantenmenge: Seien nur diejenigen Kanten berücksichtigt, die $1, 2$-Kanten in der Triangulierung kreuzen. Dieser Teilgraph des dualen Graphen hat einen Knoten außerhalb des großen Dreiecks. Weil nach obiger Überlegung an der Seite des Dreiecks zwischen 1 und 2 die Anzahl an Vorzeichenwechseln zwischen 1- und 2-gefärbten Ecken ungerade ist, hat der äußere Knoten ungeraden Grad.
Jede Kante in einem Graphen hat zwei Eckpunkte, daher beträgt die Summe der

Grade aller Ecken zweimal die Anzahl aller Kanten des Graphen. Eine Summe von ganzen Zahlen ist aber genau dann gerade, wenn die Anzahl der ungeraden Summanden gerade ist. Daher besitzt das Dreieck innerhalb eine ungerade Anzahl von Knoten ungeraden Grades und somit eine ungerade Anzahl von dreifarbigen Dreiecken. □



Beispiel eines triangulierten Dreiecks mit dem dualen Graphen wie im Beweis

Sei nun ein beliebig-trianguliertes Polygon mit der Eckenfärbung $1, 2, 3$ gegeben. Für einen weiteren Beweis des Sperner-Lemmas mit Hilfe des Index-Lemmas bedarf es der Zählung von Kanten mit Orientierung.

Definition. Der *Inhalt* V ist die Anzahl der mit Orientierung gezählten dreifarbigen Dreiecke im Polygon, d.h.

$$V = \begin{cases} +1, & \text{falls } 123 \circlearrowleft, \\ \\ -1, & \text{falls } 123 \circlearrowright . \end{cases}$$

Der *Index* I ist die Anzahl der mit Orientierung gezählten Kanten 12 rund um das Polygon.

Beweis 2. Es sei ein Polygon ohne Selbstschnitte mit beliebig vielen Ecken gegeben. Es werde beliebig trianguliert und die Ecken sollen willkürlich die drei Farbenbezeichnungen $1, 2, 3$ tragen. Das *Index-Lemma* besagt, dass der Inhalt V gleich dem Index I sein muss.
Beweis des Index-Lemmas. Sei S die Anzahl an Kanten 12 innerhalb des Polygons, wobei wiederum mit Orientierung gezählt und jedes Dreieck unabhängig von den anderen betrachtet wird.

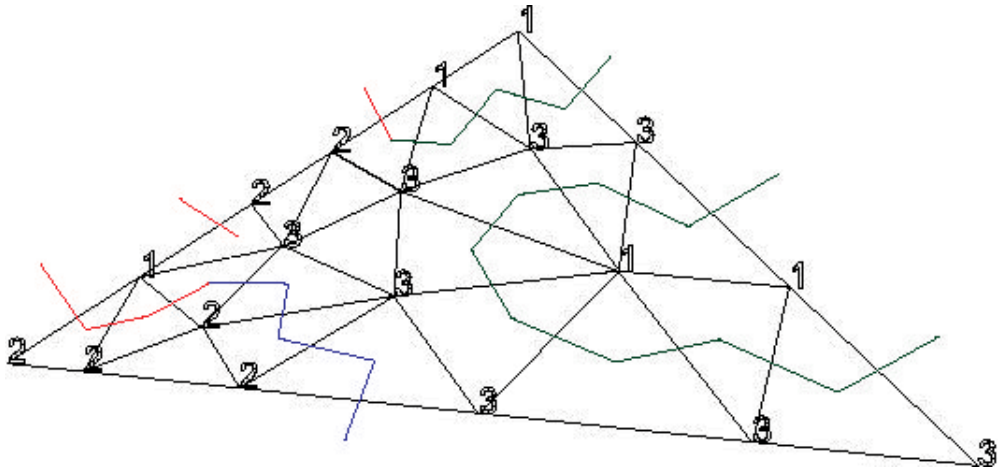
(1) $V = S$: Ein Dreieck vom Typ 123 bzw. 132 bewirkt beiderseits ± 1, vom Typ 121 oder 212 jeweils ± 0.

(2) $S = I$: Sei 12 eine beliebige Kante. Liegt diese im Inneren des Polygons, so ist sie Kante zwischen 2 Dreiecken und ändert somit S nicht ab.

Mit Hilfe des Index-Lemmas genügt es zu zeigen, dass der Index I ungerade ist. Dieser entspricht aber der Anzahl an zweifarbigen Intervallen auf einer Seite des Dreiecks, die nach obiger Überlegung ungerade ist. □

Der dritte Beweis erfolgt mittels Pfaden:
Beweis 3. Wir betrachte die $1,2$-Seite des Dreiecks und definieren einen Pfad durch die Dreiecke wie folgt: Wir überqueren nur $1,2$-Kanten. Wir betreten das Dreieck durch die erste $1,2$-Kante.
1.Fall: Wir befinden uns in einem dreifarbigen Dreieck und sind fertig.
2.Fall: Es gibt genau eine weitere $1,2$-Kante, über die wir den Pfad fortführen.
Auf diese Weise finden wir entweder ein dreifarbiges Dreieck, oder verlassen das große Dreieck auf seiner $1,2$-Seite durch eine $1,2$-Kante. Weil es eine ungerade Anzahl von $1,2$-Kanten gibt, können wir das Dreieck wieder durch eine solche betreten. Weil der Pfad zykelfrei ist, existiert ein dreifarbiges Dreieck.
Folgen wir von einem dreifarbigen Dreieck aus allen $1,2$-Kanten, so gelangen wir entweder über die $1,2$-Seite des großen Dreiecks nach außen oder wir erreichen ein anderes dreifarbiges Dreieck. Von ersteren gibt es eine ungerade Anzahl und von letzteren muss es immer eine gerade Anzahl geben. Somit ist die gesamte Anzahl dreifarbiger Dreiecke ungerade. □

Die folgende Grafik zeigt ein trianguliertes und gemäß dem Sperner-Lemma gefärbtes Dreieck und die entsprechenden im letzten Beweis verwendeten Pfade.



Das Sperner-Lemma lässt sich auf höhere Dimensionen erweitern.

Satz 51 (Verallgemeinerung des Sperner-Lemmas)**.** *Partioniert man einen n-dimensionalen Simplex $\triangle_n$ beliebig in weitere $\triangle_n$, so ist bei Färbung der Ecken mit gleichen Regeln wie im zweidimensionalen Fall die Anzahl der $(n+1)$-farbigen $\triangle_n$ ungerade.*

Beweis: Der Beweis erfolgt mittels Induktion über n. Für $n = 2$ wurde es in dreifacher Ausfertigung bewiesen.
Wir machen nun den Induktionsschritt von $n-1$ auf n: $\triangle_n$ hat $n+1$ Eckpunkte,

$n+1$ verschiedene Farben und $n+1$ $(n-1)$-dimensionale Hyperflächen. Letztere entsprechen $\triangle_{n-1}$ mit n Eckpunkten. Die durch die Partionierung in kleinere $\triangle_{n-1}$ induzierten Eckpunkte dürfen nur n der $n+1$ Farben annehmen. Nach Induktionsvoraussetzung ist die Anzahl der n-färbigen $\triangle_{n-1}$ auf einer festen Hyperfläche des $\triangle_n$ ungerade. Verwendet man diese als Türen, so erhält man wie im dritten Beweis des Sperner-Lemmas einen zykelfreien Pfad und kommt mit analoger Begründung zum Schluss, dass die Anzahl der $(n+1)$-färbigen $\triangle_n$ ungerade sein muss. □

Mit Hilfe des Sperner-Lemmas lässt sich der *Brouwer'sche Fixpunktsatz* elementar beweisen.

Satz 52 (Brouwer)**.** *Jede stetige Transformation eines Dreiecks auf sich selbst besitzt einen Fixpunkt.*

Beweis: Sei D ein Dreieck und $f : D \to D$ eine stetige Transformation von D auf sich selbst. O.B.d.A. sei die Basis von D horizontal, die dritte Ecke oberhalb, und D sei spitzwinkelig. Für jedes $P \in D$ sei $v(P) := f(P) - P$ der Vektor von P nach $f(P)$. Annahme: $v(P) \neq 0$ (ansonsten sind wir fertig).
Man bildet nun eine Folge von Triangulierungen T_n von D, sodass der maximale Durchmesser $d(T_n)$ für $n \to \infty$ gegen 0 konvergiert. Eine Ecke P der Triangulierung erhalte die Bezeichnung

$$\begin{cases} 1, & \text{falls } v(P) \text{ zwischen O und N ,} \\ 2, & \text{falls } v(P) \text{ zwischen N+ und W ,} \\ 3 & \text{sonst.} \end{cases}$$

Diese Bezeichnungen erfüllen die Bedingungen einer zulässigen Sperner-Färbung. Nach dem Sperner-Lemma enthalten die Triangulationen T_n folglich jeweils ein dreifarbiges Dreieck D_n für alle n.
Der Satz von *Bolzano-Weierstrass* besagt unter anderem, dass jede beschränkte Folge komplexer Zahlen mit unendlich vielen Folgegliedern mindestens einen Häufungspunkt enthält. In diesem Fall liegen drei Punktfolgen der D_n mit den Eckenbezeichnungen 1,2,3 vor. Damit hat jede dieser unendlichen Folgen mindestens einen Häufungspunkt. Weil $d(T_n)$ gegen 0 konvergiert, existiert ein Häufungspunkt P aller drei Folgen. Aufgrund der Stetigkeit von f muss $v(P)$ gleich 0 sein, was bedeutet, dass P ein Fixpunkt von f ist. □

Abschließend wird noch vorgestellt, wie man ähnlich wie im dritten Beweis des Sperner-Lemmas mittels Pfaden durch Triangulierungen ebene reelle algebraische Kurven konstruieren kann. Auf Beweise wird in diesem Teil verzichtet und auf [17] verwiesen. Zunächst benötigen wir folgende Definition.

Definition. Eine Abbildung f zwischen topologischen Räumen X und Y ist dann und nur dann ein *Homöomorphismus*, wenn f bijektiv und stetig ist, und die Umkehrfunktion f^{-1} ebenfalls stetig ist.

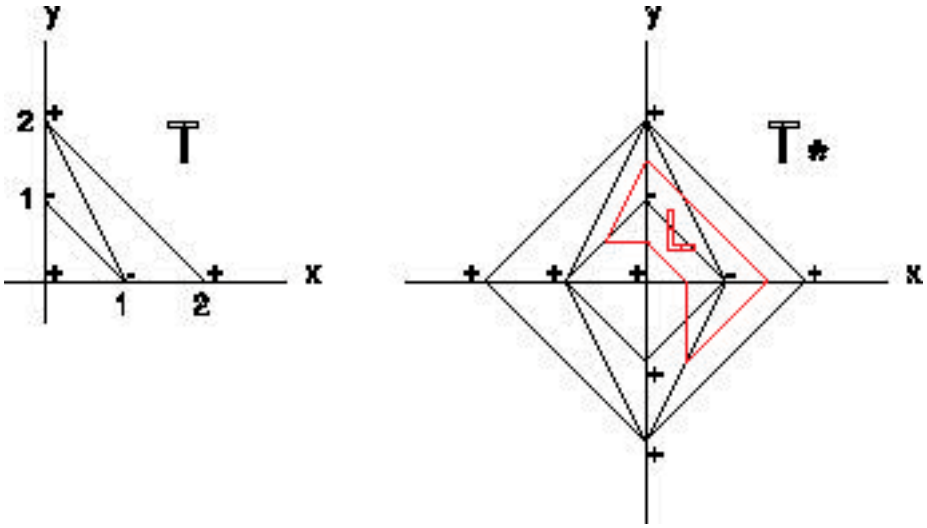
Sei jetzt T ein Dreieck in $\mathbb{R}^2$ mit den Eckpunkten $(0,0),(m,0),(0,m)$ für $m \in \mathbb{N}$. Sei $\mathcal{T}$ eine Triangulierung von T, sodass die Eckpunkte von $\mathcal{T}$ nur ganzzahlige Koordinaten besitzen. Weiters nehmen wir an, dass die Triangulierung $\mathcal{T}$ *konvex* ist. Das bedeutet, dass eine konvexe stückweise-lineare Funktion von T nach $\mathbb{R}$ existiert, die auf jedem Dreieck von $\mathcal{T}$ linear ist, auf der Vereinigung zweier Dreiecke von $\mathcal{T}$ jedoch nicht linear ist. Ferner werden die Eckpunkte von $\mathcal{T}$ mit Vorzeichen (plus oder minus) versehen. Dabei wird das Vorzeichen an einem Eckpunkt (i,j) mit $\sigma_{i,j}$ symbolisiert.
Wir konstruieren im Folgenden eine stückweise lineare Kurve. Seien s_x und s_y Spiegelungen an der $x-$ und $y-$Achse und $s = s_x \circ s_y$ die Komposition beider Spiegelungen. Wir betrachten

$$T_x := s_x(T), T_y := s_y(T), T_{xy} := s(T)$$

und bezeichnen das Quadrat $T \cup T_x \cup T_y \cup T_{xy}$ mit T_*. Die Triangulierung $\mathcal{T}$ wird zu einer symmetrischen Triangulierung von T_* erweitert. Die Eckpunkte der erweiterten Triangulierung werden nach folgender Regel mit den Vorzeichen $\sigma_{i,j}$ versehen:

$$\sigma_{i,j}\sigma_{i\epsilon,j\delta}\epsilon^i\delta^j = 1 \text{ wobei } \epsilon, \delta = \pm 1.$$

Letzteres bedeutet, dass wenn wir von einem Eckpunkt auf einen seiner an der $x-$ oder $y-$Achse gespiegelten Punkte übergehen, das Vorzeichen gleich bleibt, falls der Abstand des Eckpunktes zur Spiegelachse gerade ist, und wechselt, falls er ungerade ist.
Nun konstruieren wir ähnlich wie im dritten Beweis des Sperner-Lemmas einen Pfad von Linien. Zwischen zwei Eckpunkten der Triangulierung von T_* mit verschiedenen Vorzeichen wird dazu eine Trennlinie gebildet. Wir fügen nun diese Trennlinien zusammen und erhalten ein Polygon in T, das wir mit L bezeichnen.



Anfangsdaten und das resultierende Polygon

Sei jetzt $\overline{T_*}$ die projektive Erweiterung von T_* und $\mathcal{L}$ das Bild von L in $\overline{T_*}$.

Satz 53. *Unter sämtlichen bisherigen Voraussetzungen existiert eine nicht-singuläre reelle algebraische ebene affine Kurve vom Grad m und ein Homöomorphismus von*

der Ebene $\mathbb{R}^2$ auf das Quadrat T_*, der die Menge der reellen Punkte dieser Kurve auf L abbildet. Weiters existiert ein Homöomorphismus $\mathbb{P}_2(\mathbb{R}) \to \overline{T_*}$, der die Menge der reellen Punkte des projektiven Abschlusses der affinen Kurve auf $\mathcal{L}$ abbildet.

Abschließend wird noch erörtert, wie man die definierenden Polynome dieser sogenannten *T-Kurven* konstruiert. Sei μ die konvexe Funktion, die sicherstellt, dass die Triangulierung von T konvex ist. Seien

$$f_t(x, y) := \sum_{(i,j)\in\mathcal{T}} \sigma_{i,j} x^i y^j t^{\mu(i,j)}$$

und F_t die dazugehörigen homogenen Polynome:

$$F_t(x_0, x_1, x_2) = x_0^m f_t(\frac{x_1}{x_0}, \frac{x_2}{x_0}).$$

Eine detaillierte Version des Satzes besagt dann, dass ein $t_0 > 0$ existiert, sodass für alle $t \in (0, t_0]$ die gesuchte affine Kurve $C = V(\lambda \cdot f_t)$ mit $\lambda \in \mathbb{R} \setminus \{0\}$ ist, sodass das Paar $(\mathbb{R}^2, C)$ homöomorph ist zum Paar (T_*, L). Ferner ist für den projektiven Abschluss von C, nämlich $\overline{C} = V(\lambda \cdot F_t)$ das Paar $(\mathbb{P}_2(\mathbb{R}), \overline{C})$ homöomorph zum Paar $(\mathcal{T}, \mathcal{L})$. Wichtige Anwendungen dieses Satzes stehen in [17].

Literaturverzeichnis

[1] Egbert Brieskorn, Horst Knörrer: *Plane Algebraic Curves*. Birkhäuser-Verlag, Basel, 1986.

[2] Gerd Fischer: *Ebene algebraische Kurven*. Vieweg-Verlag, Braunschweig/Wiesbaden, 1994.

[3] Dale Husemöller: *Elliptic Curves*. Springer-Verlag, 1996.

[4] Joseph Silverman und John Tate: *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.

[5] Eberhard Freitag und Rolf Busam: *Funktionentheorie*. Springer-Verlag, Berlin, 1993.

[6] Frédéric Chyzak, Peter Paule, Otmar Scherzer, Armin Schoisswohl, Burkhard Zimmermann: *The Construction of Orthonormal Wavelets Using Symbolic Methods and a Matrix Analytical Approach for Wavelets on the Interval*, Experimental Mathematics 10:1, p. 67-85, Springer-Verlag, 2003.

[7] I. Daubechies: *Ten lectures on wavelets*. CBMS-NSF Regional Conference Series in Applied Mathematics 61, Philadelphia, 1992.

[8] David Cox, John Little, Donal O'Shea: *Using Algebraic Geometry*. Springer-Verlag, 2006.

[9] I.R. Shafarevich: *Basic Algebraic Geometry*. Springer-Verlag, 1974.

[10] Hermann Schubert: *Kalkül der abzählenden Geometrie*. Springer-Verlag, New York, 1979.

[11] Ernst Kunz: *Einführung in ebene algebraische Kurven*. Birkhäuser-Verlag, Boston, 2005.

[12] Neal Koblitz: *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag, 1984.

[13] Reinhold Remmert: *Funktionentheorie 1*. Springer-Verlag, 1989.

[14] Wolfgang Fischer, Ingo Lieb: *Funktionentheorie*. Vieweg-Verlag, 1980.

[15] Siegfried Bosch: *Lineare Algebra*. Springer-Verlag, 2001.

[16] Claus Scheiderer: *Reelle Algebra und Geometrie*. Vorlesungsskriptum, 2004.

[17] Oleg Viro, Ilia Itenberg: *Patchworking algebraic curves disproves the Ragsdale conjecture*. The Mathematical Intelligence, 18:1, 19-28, 1996.

[18] Günter Scheja, Uwe Storch: *Lehrbuch der Algebra*. Teil 2, B.G. Teubner Verlag, 1980.