Ebene Algebraische Kurven

Wolf P. Barth

Wintersemester 04/05

Version vom 18. Oktober 2004

Mathematisches Institut der Universität
Bismarckstr. 1 1/2, D - 91054 Erlangen
e-mail: barth@mi.uni-erlangen.de

Inhaltsverzeichnis

0 Einführung

0.1 Definition

Eine ebene algebraische Kurve C ist die Lösungsmenge *einer* Polynomgleichung in zwei Variablen:

$$C = \{(x, y) : p(x, y) = 0\}.$$

Hier muss zunächst einiges präzisiert werden:

Ein *Polynom* $p(x, y)$ in zwei Variablen x, y ist eine Funktion der Bauart

$$p(x, y) = \sum_{\mu,\nu=0}^{<\infty} a_{\mu,\nu} x^\mu y^\nu.$$

Das ist also eine *endliche* Linearkombination von Monomen $x^\mu y^\nu$. Dabei kann - wie in der elementaren projektiven Geometrie - ein beliebiger Körper $\mathbb{K}$ zugrunde gelegt werden, aus dem die Koeffizienten $a_{\mu,\nu}$ stammen, und in dem dann $p(x, y)$ seine Werte annimmt, wenn $(x, y) \in \mathbb{K}^2$ gewählt werden. Man schreibt dann auch $p \in \mathbb{K}[x, y]$. Und genauer ist dann

$$C = \{(x, y) \in \mathbb{K}^2 : p(x, y) = 0\}.$$

Natürlich sollte man hier den Fall ausschließen, dass p das Nullpolynom ist. Dann bekommt man als Nullstellenmenge ja keine Kurve, sondern die ganze Ebene.

Für die Anschauung der wichtigste Fall ist $\mathbb{K} = \mathbb{R}$, obwohl die Theorie in diesem Fall viel schwieriger ist als für den unanschaulichen Körper $\mathbb{C}$. Auch der Fall anderer, z.B. endlicher Körper ist von Interesse. Dies führt jedoch aus dem Feld der Geometrie in das der Zahlentheorie.

0.2 Beispiele

Jedem Mathematiker bekannt sind die Kurven

$$\begin{array}{ll} ax + by + c = 0 & \textit{Gerade} \\ ax^2 + bxy + cy^2 + dx + ey + f = 0 & \textit{Kegelschnitt} \end{array}$$

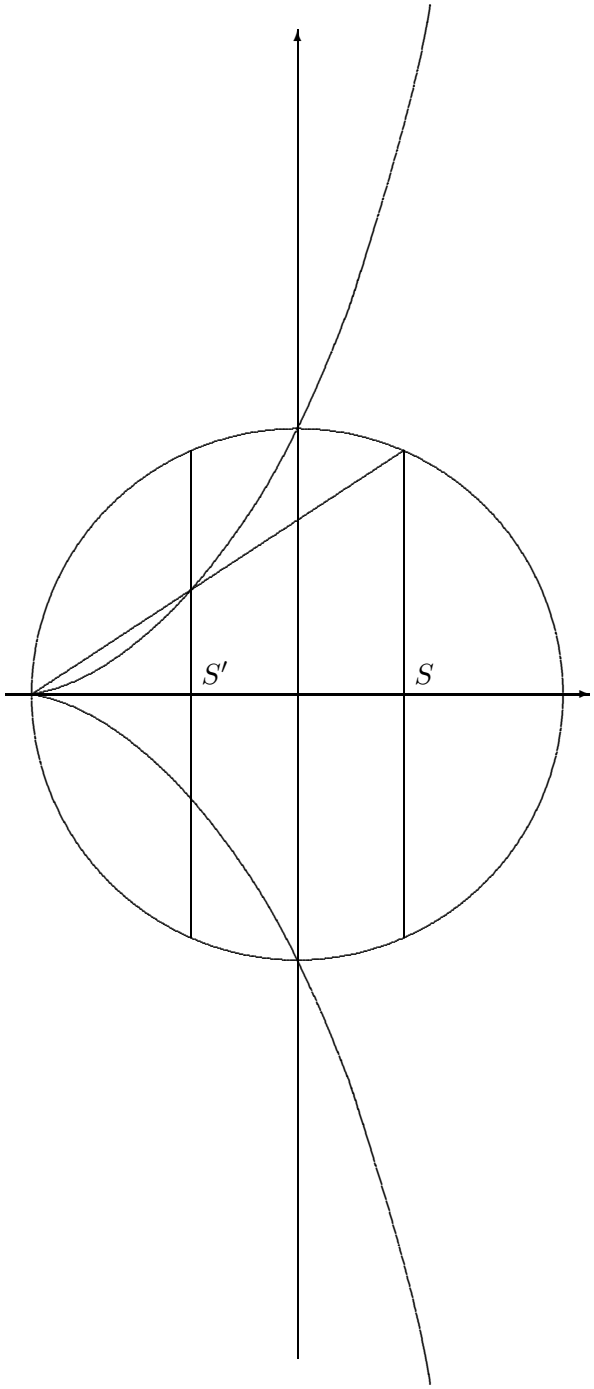
Kegelschnitte wurden von dem Griechen Menaechmus ($\sim$ 350 v.Chr.) erfunden. Es gibt sogar ein ganzes Buch, das ihrer Geschichte gewidmet ist:

J.L.Coolidge: A history of the conic sections and quadric surfaces. Dover 1968

Um ihre klassischen Probleme

- Verdoppelung des Würfels (Delisches Problem)
- Dreiteilung des Winkels

zu bearbeiten, haben die Griechen auch noch kompliziertere Kurven verwendet. Dabei haben sie allerdings keine Koordinaten x, y benutzt, weil sie die nicht gekannt haben. Ähnlich wie die Kegelschnitte als Schnitte von Kegel und Ebene haben sie die Kurven angegeben, indem sie eine geometrische Erzeugung formulierten. Ich möchte einige Beispiele dafür diskutieren (nach Brieskorn-Knörrer):



Die Kissoide des Diocles ($\sim$ 200 v. Chr.)

Man fixiert zwei aufeinander senkrechte Geraden (heutzutage die Koordinatenachsen) und einen Kreis um deren Schnittpunkt (heutzutage den Einheitskreis). Dann bewegt man einen Stab $S: x = c$ parallel zur y-Achse vom rechten Schnittpunkt $(1, 0)$ des Kreises mit der x-Achse zum linken $(-1, 0)$. Der Stab schneidet den Kreis in den Punkten $(x, \pm\sqrt{1-x^2})$. Beide Punkte verbindet man mit dem Punkt $(-1, 0)$ durche gerade Linien. Die Schnittpunkte dieser Linien mit einem zweiten Stab $S': x = -c$ parallel zur y-Achse in derselben Entfernung wie S, aber auf der anderen Seite, beschreiben die Kissoide.

Zuerst wollen wir mal deren Gleichung ausrechnen: Die beiden Verbindungslinien parametrisieren wir durch

$$(-1, 0) \pm t \cdot (c+1, \sqrt{1-c^2}), \quad t \in \mathbb{R}.$$

Zu $x = -c$ gehört der Parameter

$$t = \frac{1-c}{1+c}$$

und der y-Wert

$$y = t \cdot \sqrt{1-c^2} = \frac{1-c}{1+c} \cdot \sqrt{1-c^2} = \frac{\sqrt{1-c}^3}{\sqrt{1+c}}.$$

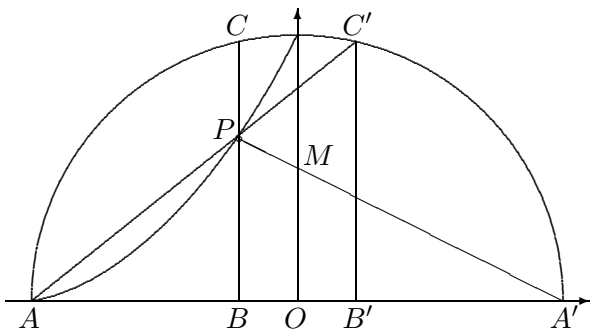
Quadriert man hier und setzt $c = -x$, so erhält man die Gleichung

$$y^2(1-x) = (1+x)^3, \quad p(x,y) := y^2(1-x) - (1+x)^3 = 0.$$

Das Delische Problem besteht darin, zu gegebenem y eine Zahl x mit

$$x^3 = 2y^3$$

zu kostruieren. Dabei genügt es, eine solche Konstruktion für ein einziges $y > 0$ zu finden, für alle anderen $y > 0$ bekommt man dann das zugehörige x aus ähnlichen Dreiecken. Wir beschriften unsere Figur wie folgt:



Dabei ist M der vertikale von O ausgehenden Kreisradius. Der Schlüssel ist die Konstruktion von P als Schnittpunkt der Gerade $A'M$ mit der Kissoide. Wir definieren nun die Strecken

$$x := BA', \quad y := BC, \quad z := AB.$$

Aus dem Strahlensatz am Dreieck $A'BP$ folgt

$$\frac{A'B}{PB} = \frac{A'O}{MO} = 2, \quad PB = \frac{x}{2}.$$

Durch raffiniertes Ausnützen ähnlicher rechtwinkliger Dreiecke sieht man

$$\begin{aligned} \frac{A'B}{BC} &= \frac{CB}{BA} && A'BC \sim CBA \\ &= \frac{C'B'}{B'A'} && CBA \sim C'B'A' \\ &= \frac{AB'}{B'C'} && C'B'A' \sim AB'C' \\ &= \frac{AB}{BP} && AB'C' \sim ABP \end{aligned}$$

Also ist insbesondere

$$\frac{x}{y} = \frac{y}{z} = \frac{z}{x/2}.$$

Eliminiert man hier

$$z = \sqrt{\frac{xy}{2}},$$

so erhält man

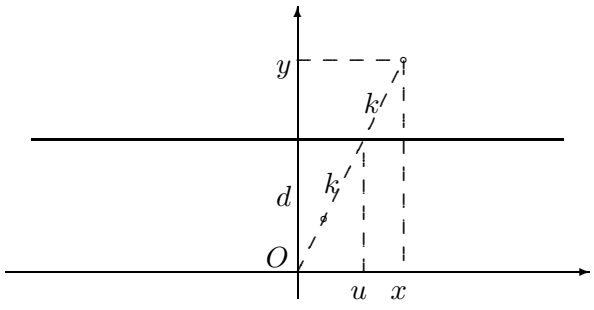
$$x\sqrt{\frac{xy}{2}} = y^2, \quad x\sqrt{x} = y\sqrt{2y}, \quad x^3 = 2y^3.$$

Diese Schlussweise ist typisch für die Mathematik im antiken Griechenland. Der Name der Kurve kommt übrigens vom griechischen Wort für Efeu. Die Griechen betrachteten nämlich nur den im Inneren des Kreises liegenden Teil der Kurve, und der zusammen mit einem Teil des Kreises selbst erinnert an die Form des Efeublattes.

Die Konchoide des Nicomedes ($\sim$ 180 v. Chr.)

Man fixiert eine Gerade, etwa die x-Achse und einen Punkt O im Abstand d von dieser Gerade, etwa $O = (0, -d)$. Dann dreht man einen Stab um diesen Punkt. Wenn der nicht parallel zur Geraden ist, schneidet er die Gerade in einem Punkt. Von diesem trägt man auf dem Stab in beiden Richtungen eine feste Strecke k ab. Die Endpunkte beider Strecken sind Kurvenpunkte. Damit besteht die Kurve aus zwei Teilen: einem unterhalb und einem oberhalb der Gerade.

Wieder wollen wir zuerst die Gleichung der Kurve herleiten:

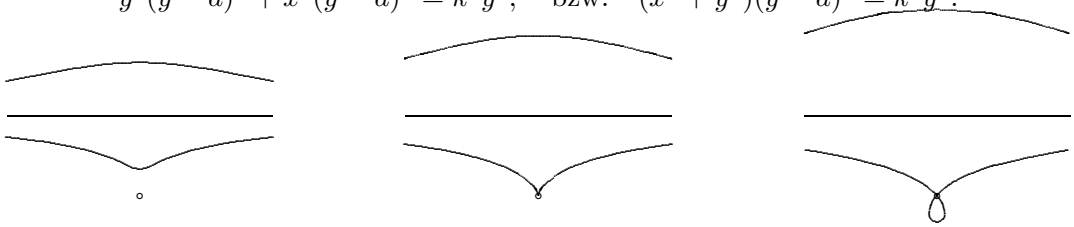


Mit dem Strahlensatz folgt $u = x \cdot d/y$ und dann

$$(y-d)^2 + (x-u)^2 = (y-d)^2 + (x - x \cdot \frac{d}{y})^2 = k^2.$$

Nach Multiplikation mit y^2 wird aus dieser Gleichung

$$y^2(y-d)^2 + x^2(y-d)^2 = k^2y^2, \quad \text{bzw.} \quad (x^2+y^2)(y-d)^2 = k^2y^2.$$



$k < d$ $\qquad$ $k = d$ $\qquad$ $k > d$

Die Kurve hat ihren Namen vom griechischen Wort für Muschel.

Mit dieser Konchoide löst man das zweite klassische Problem, die Dreiteilung des Winkels wie folgt: Man fällt das Lot von O auf die fixierte Gerade. Der Fußpunkt sei B. Dann trägt man in O den Winkel α an, der eine Schenkel sei OB, der andere OA, wobei auch A auf der fixierten Gerade liegt. Nun benutzt man die Kissoide mit $k = 2OA$. Verlängert man OA bis zum Schnittpunkt mit der Kissoide, so ist die Strecke, um die verlängert wird gerade $k = 2OA$. Der Schlüssel ist hier der Schnittpunkt C der Kissoide mit der Gerade durch A senkrecht zur fixierten Gerade. Der Schnittpunkt von OC mit der fixierten Gerade sei E, der Mittelpunkt der Strecke CE sei D. Dann ist auch $EC = 2OA$ und

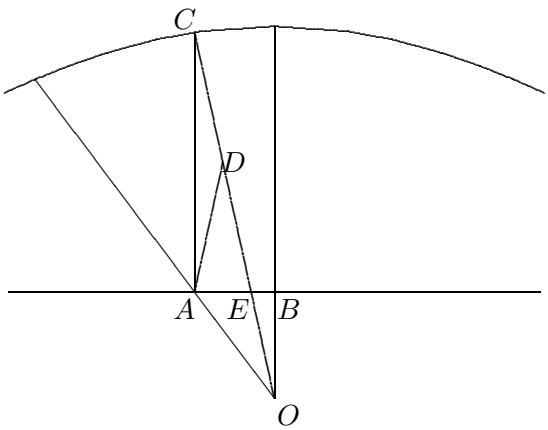
$$DE = k/2 = OA.$$

Außerdem ist auch $DE = DA$ und das Dreieck OAD ist gleichschenklig. Deswegen ist

$$\angle DOA = \angle ODA = \angle EDA = 2\angle BOE.$$

Wegen $\alpha = \angle DOA + \angle BOE$ folgt daraus

$$\frac{\alpha}{3} = \angle BOE.$$



Die Spiren des Perseus ($\sim$ 150 v. Chr)

Ein (Kreis-) Kegel entsteht, indem man eine schräge Gerade um eine Achse rotieren lässt. Die nächst-komplizierte Figur, welche man rotieren lassen kann ist der Kreis. Lässt man einen Kreis um eine Gerade in der Kreisebene, welche den Kreis nicht schneiden soll, rotieren, so entsteht eine Fläche, die wir heute *Torus* nennen. Zuerst wollen wir dessen Gleichung herleiten:

Wir rotieren um die z-Achse und den Kreis fassen wir auf als den Graphen der (mehrwertigen) Funktion

$$x = R + \sqrt{r^2 - z^2}$$

in der x, z-Ebene. Dann hat die Rotationsfläche eine Gleichung

$$\sqrt{x^2 + y^2} = R + \sqrt{r^2 - z^2}.$$

Um daraus eine Polynom-Gleichung zu machen, müssen wir zweimal geschickt quadrieren:

$$\begin{aligned}
x^2 + y^2 &= R^2 + 2R\sqrt{r^2 - z^2} + r^2 - z^2 \\
x^2 + y^2 + z^2 - R^2 - r^2 &= 2R\sqrt{r^2 - z^2} \\
(x^2 + y^2 - R^2 + z^2 - r^2)^2 &= 4R^2(r^2 - z^2) \\
(x^2 + y^2 - R^2)^2 + 2(x^2 + y^2 - R^2)(z^2 - r^2) + (z^2 - r^2)^2 &= 4R^2(r^2 - z^2) \\
(x^2 + y^2 - R^2)^2 + 2(x^2 + y^2 + R^2)(z^2 - r^2) + (z^2 - r^2)^2 &= 0 \\
(x^2 + y^2 + R^2)^2 + 2(x^2 + y^2 + R^2)(z^2 - R^2) + (z^2 - r^2)^2 &= 4R^2(x^2 + y^2) \\
(x^2 + y^2 + z^2 + R^2 - r^2)^2 &= 4R^2(x^2 + y^2)
\end{aligned}$$

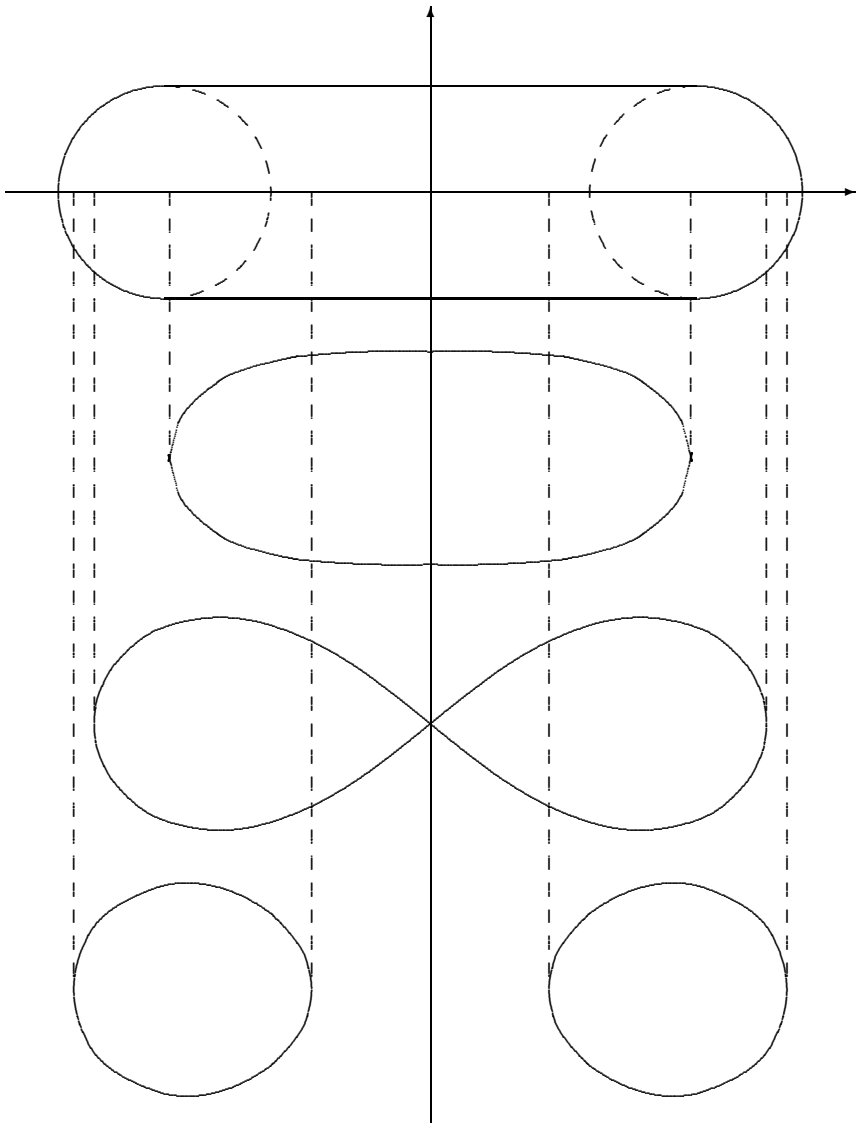
Nachdem die Griechen die Kegelschnitte als ebene Schnitte eines Rotationskegels erfunden hatten, kamen sie auch auf die Idee, diese Torus-Fläche mit Ebenen zu schneiden. Wählt man dafür die Ebenen $y = c$ parallel zur Rotationsachse, so haben die Schnittkurven die Gleichungen

$$(x^2 + z^2 + c^2 + R^2 - r^2)^2 = 4R^2(x^2 + c^2),$$

oder, wenn wir z durch y ersetzen:

$$(x^2 + y^2 + c^2 + R^2 - r^2)^2 = 4R^2(x^2 + c^2).$$

Wozu die Griechen diese Kurven erfunden haben, weiß ich nicht. Aber sie sehen ungefähr so aus (für $c = R$, $R - r$, r):



Die Epizykloiden des Hipparchos ($\sim$ 150 n. Chr.)

Die Astronomen der Antike nahmen zunächst an, dass die Erde ein Zentrum ist, um das sich die Sonne und die Planeten herumbewegen. Merkwürdig dabei war allerdings, dass die Planeten sich meistens in die gleiche Richtung bewegen, aber gelegentlich auch gegenläufig. Soetwas passiert bei manchen Zykloiden. Das sind Rollkurven, die entstehen, wenn ein Kreis auf einem anderen abrollt. Deswegen haben die Griechen solche Zykloiden zur Beschreibung der Planetenbewegungen herangezogen. Ganz schief sind sie damit nicht gelegen. Denn, wenn man annimmt, dass alle Planeten auf einem echten Kreis um die Sonne herumfliegen, dann bewegt sich die Sonne auf einem Kreis um das Zentrum Erde, und die Planeten tatsächlich auf Zykloidenbahnen um die Erde.

Epizykloiden, die allerdings nicht ganz optimal zur Erklärung der Planetenbahnen sind, entstehen wenn ein Kreis vom Radius r außen auf einem Kreis vom Radius R abrollt, ohne zu rutschen. Ein Punkt auf dem abrollenden Kreis bewegt sich auf einer Epizykloide. Diese Kurve ist einfach zu parametrisieren: Sei etwa Φ der Winkel zum Berührpunkt auf dem festen Kreis, φ der Winkel um den sich der rollende Kreis gedreht hat und

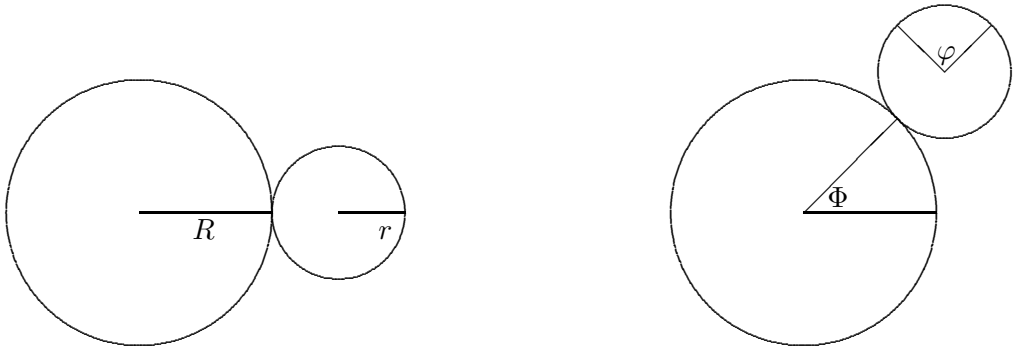
$$l = R \cdot \Phi = r \cdot \varphi$$

die abgerollte Strecke. Dann ist

$$\Phi = \frac{l}{R}, \quad \varphi = \frac{l}{r} = \frac{R}{r}\Phi.$$

Ein Punkt auf der Bahn hat die Koordinaten

$$(x, y) = (R + r)(cos(\Phi), sin(\Phi)) + r(cos(\Phi + \varphi), sin(\Phi + \varphi)).$$



Nehmen wir $t := \Phi$ als Parameter, so wird

$$x = (R + r)cos(t) + rcos((1 + \frac{R}{r})t), \quad y = (R + r)sin(t) + rsin((1 + \frac{R}{r})t).$$

Falls R/r irrational ist, bekommt man keine algebraische Kurve. Aber für rationale Werte R/r ist das schon der Fall. Zumindest glaube ich das, ohne es allerdings allgemein beweisen zu können. Ausgangspunkt ist die Gleichung

$$\begin{aligned} x^2 + y^2 &= (R + r)^2 + r^2 + 2r(R + r) \cdot [cos(t)cos((1 + \frac{R}{r})t) + sin(t)sin((1 + \frac{R}{r})t)] \\ &= (R + r)^2 + r^2 + 2r(R + r)cos(t - (1 + \frac{R}{r})t) \\ &= (R + r)^2 + r^2 + 2r(R + r)cos\left(\frac{R}{r}t\right). \end{aligned}$$

bzw.

$$cos(\frac{R}{r}t) = \frac{1}{2r(R + r)}(x^2 + y^2 - (R + r)^2 - r^2).$$

Diese Gleichung kann man benutzen, um aus

$$x = (R+r)cos(t) + rcos((1+\frac{R}{r})t)$$

die Cosinus-Werte zu eliminieren.

Wir wollen einige Spezialfälle diskutieren, wobei vereinfachend $R = 1$ gesetzt werde. Wir benutzen die mit den Additionstheoremen der Winkelfunktionen leicht zu verifizierenden Formeln

$$cos(2u) = 2cos^2(u) - 1, \quad cos(3u) = 4cos^3(u) - 3cos(u).$$

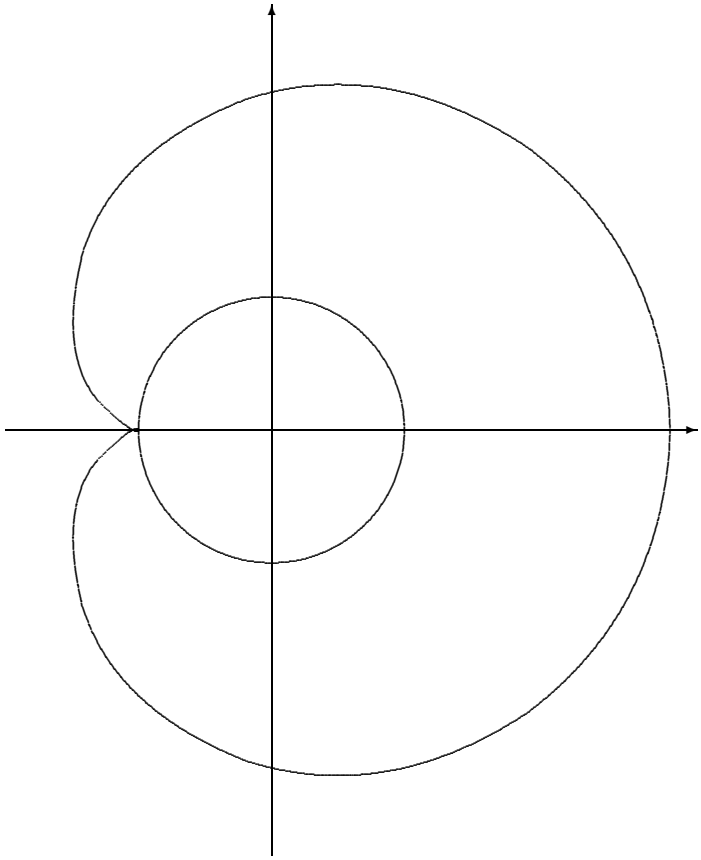
$r = 1$: Hier ist

$$x = 2cos(t) + cos(2t) = 2cos(t) + 2cos^2(t) - 1, \quad cos(t) = \frac{x^2+y^2-5}{4}.$$

Nach etwas Rechnung findet man

$$(x^2+y^2)^2 - 6(x^2+y^2) - 8x - 3 = 0.$$

Dies ist das sogenannte Cardioid (Koersma 1689), die Herzkurve.



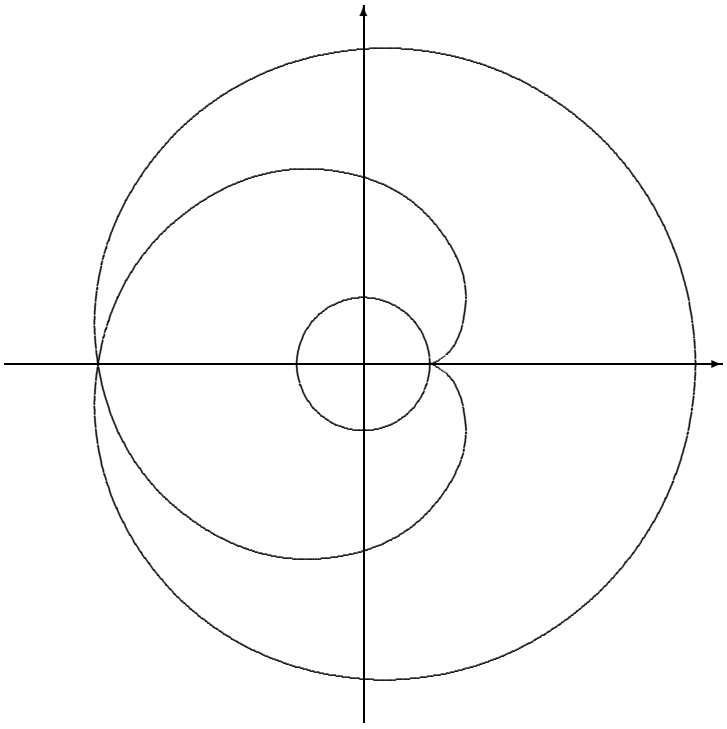
$r = 2$: Wir haben

$$x = 3cos(t) + 2cos(\frac{3}{2}t), \quad cos(u) = \frac{1}{12}(x^2+y^2-13)$$

mit $u = t/2$. Dann ist also $cos(t) = cos(2u)$ und $cos(3t/2) = cos(3u)$. Nach etwas Rechnung findet man, dass die Punkte der Kurve der Gleichung

$$2(x^2+y^2)^3 - 69(x^2+y^2)^2 + 564(x^2+y^2) - 432x - 1361 = 0$$

genügen. Komisch ist hier die Primzahl 1361.



$r = 1/2$: Jetzt ist

$$x = \frac{3}{2}cos(t) + \frac{1}{2}cos(3t), \quad cos(2t) = \frac{2}{3}(x^2+y^2-\frac{5}{2}).$$

Damit finden wir

$$cos(t) = \sqrt{\frac{1}{2}(1+cos(2t))} = \sqrt{\frac{1}{3}(x^2+y^2-1)},$$

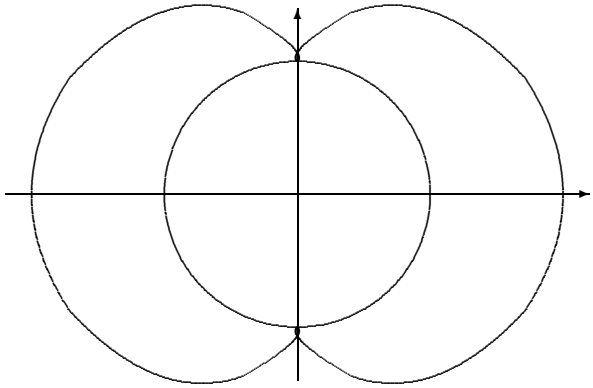
$$cos(3t) = cos(t)\cdot(4cos^2(t)-3) = cos(t)\cdot(2cos(2t)-1) = cos(t)\cdot\left(\frac{4}{3}(x^2+y^2)-\frac{13}{3}\right).$$

Die Punkte der Kurve genügen also der Gleichung

$$x = \sqrt{\frac{1}{3}(x^2+y^2-1)}\cdot\left(\frac{3}{2}+\frac{1}{2}(\frac{4}{3}(x^2+y^2)-\frac{13}{3})\right).$$

Quadriert man hier, ordnet etwas um und bereinigt die Nenner, so wird daraus

$$64(x^2+y^2)^3 - 336(x^2+y^2)^2 + 453x^2 + 561y^2 - 17^2 = 0.$$



Dürers Konchoide (1525)

Aus reinem Lokal-Patriotismus möchte ich hier noch eine Kurve vorstellen, die Dürer in seiner *Underweysung der messung mit den zirkel un richtscheyt* angibt, *die in mancherley sachen zu gebrauchen ist*. Auf welche Sachen er sich dabei bezieht weiß ich leider nicht. Weil er noch keine Koordinaten kannte, hat Dürer eine mechanische Konstruktion seiner Kurve angegeben:

Auf zwei orthogonalen Geraden mögen sich zwei Punkte P und Q bewegen. Der Einfachheit halber nehme ich als Geraden die Koordinatenachsen und setze

$$P = (p, 0), \quad Q = (0, q).$$

Bei der Bewegung der Punkte möge stets $p+q = const$, etwa $= 1$ sein (eine ziemlich merkwürdige und ungeometrische Bedingung). Die Punkte auf der Geraden PQ, welche von P einen festen Abstand a haben, überstreichen die Kurve.

Um die Gleichung der Kurve herzuleiten, verwenden wir

$$p + q = 1, \quad (x-p)^2 + y^2 = a^2, \quad y = -\frac{q}{p}x + q.$$

Die zweite Gleichung ist die Abstandsbedingung des Kurvenpunktes von P, die dritte Gleichung die Bedingung dafür, dass der Kurvenpunkt auf der Geraden PQ liegt. Die Kurvengleichung erhält man, indem man aus diesen drei Gleichungen die Konstanten p und q eliminiert. Das ist allerdings leichter gesagt als getan. Wir verfahren folgendermaßen:

Wenn wir $q = 1 - p$ in die umgeformte dritte Gleichung

$$py + q(x-p) = 0$$

einsetzen, erhalten wir

$$py + (1-p)(x-p) = 0, \quad \text{bzw.} \quad p^2 + p(y-x-1) + x = 0.$$

Diese quadratische Gleichung für p brauchen wir jetzt nur noch nach p aufzulösen

$$p = \frac{1}{2}(x + 1 - y \pm w)$$

mit

$$w = \sqrt{(x+1-y)^2 - 4x} = \sqrt{x^2+y^2+1-2xy-2x-2y},$$

und in die zweite Gleichung von oben einzusetzen. Das Problem besteht natürlich darin, die Wurzel wieder los zu werden. Ich möchte deshalb erst mal die zweite Gleichung von oben umformen

$$x^2 + y^2 - 2px + p^2 - a^2 = 0$$

und $p^2 = p(x+1-y) - x$ rausschmeißen:

$$x^2 + y^2 - 2px + p(x+1-y) - x - a^2 = x^2 + y^2 + p(1-x-y) - x - a^2 = 0.$$

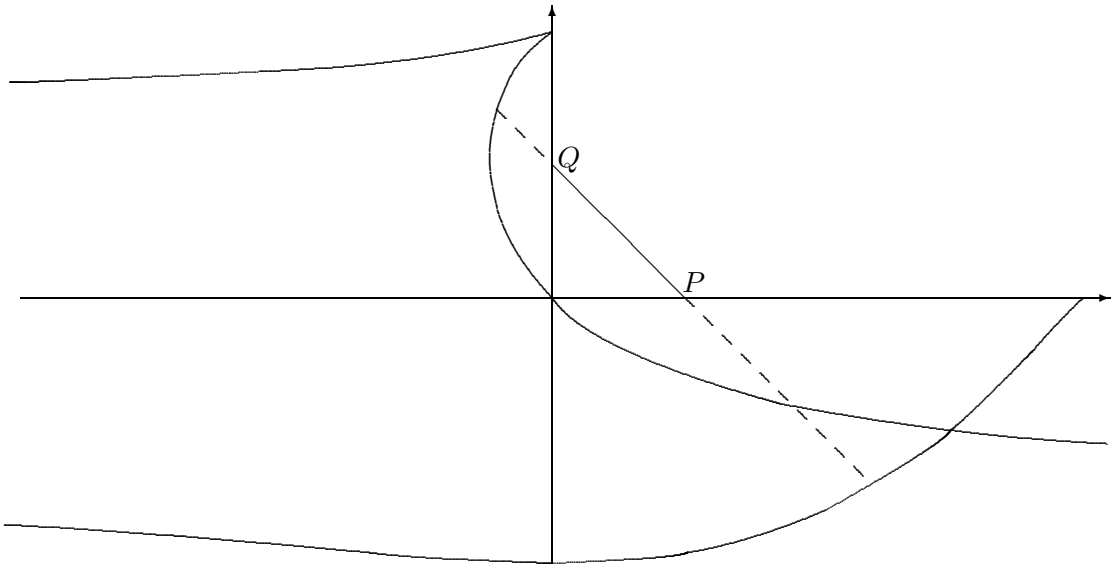
Jetzt können wir die Wurzel isolieren:

$$\begin{aligned} x^2+y^2-x-a^2 &= p(x+y-1) \\ x^2+y^2-x-a^2 &= \frac{1}{2}(x+1-y)(x+y-1) \pm \frac{1}{2}w(x+y-1) \\ x^2+3y^2-2x-2y+1-2a^2 &= w(x+y-1) \end{aligned}$$

Jetzt müssen wir quadrieren und das Ergebnis geschickt zusammenfassen. Das habe ich lieber MAPLE überlassen und das folgende Ergebnis erhalten:

$$2y^2(x^2+y^2) - 2y^2(x+y) + (1-3a^2)y^2 - a^2x^2 + 2a^2(x+y) + a^2(a^2-1) = 0.$$

So steht das auch in dem von mir benutzten Buch 'J.D.Lawrence, p.159'. Für $a = 1$ sieht die Kurve ungefähr so aus:



0.3 Referenzen

Hier möchte ich alle Lehrbücher zur systematischen Theorie der ebenen algebraischen Kurven angeben, die ich kenne. Natürlich sind sie nicht alle zu empfehlen. Aber sie zeigen doch, wie das Thema in den letzten drei Jahrhunderten, unter wechselnden Gesichtspunkten behandelt wurde.

Die ältesten Bücher hierzu, die ich kenne, sind

- C. MacLaurin: De linearum geometricarum proprietatibus tractatus (1720)
- G. Cramer: Introduction a l'Analyse des lignes courbes (1750)

Beide Bücher habe ich noch nie in der Hand gehabt und kann dazu nicht mehr sagen. Aus dem Netz habe ich allerdings gelernt, dass Cramer (einer) der Erfinder der Cramerschen Regel ist, und dass diese Regel deswegen mit 'C' geschrieben werden muss. Und wie es so geht, braucht er diese Regel genau im eben zitierten Buch, wo er folgende Aussage beweist: Durch fünf Punkte in der Ebene geht immer ein Kegelschnitt. Er setzt den Kegelschnitt mit sechs unbestimmten Koeffizienten an, etwa

$$c_1 \cdot x^2 + c_2 \cdot xy + c_3 \cdot y^2 + c_4 \cdot x + c_5 \cdot y + c_6 = 0.$$

Wenn (p_ν, q_ν), $\nu = 1, ..., 5$, die Koordinaten der fünf Punkte sind, so geht der Kegelschnitt durch den ν-ten dieser Punkte, wenn die Kegelschnittgleichung mit $x = p_\nu$, $y = q_\nu$ erfüllt ist. Das ist eine homogene lineare Gleichung für die sechs unbekannten Koeffizienten $c_1, ..., c_6$. Und wenn der Kegelschnitt durch alle fünf Punkte gehen soll, hat man fünf homogene lineare Gleichungen für sechs Unbekannte. Man kann hier $c_6 = 1$ probieren, es in allen fünf Gleichungen auf die rechte Seite bringen, und hat fünf inhomogene Gleichungen für fünf Unbekannte. Das ist ein klarer Fall für die Cramersche Regel.

Die Autoren der folgenden Bücher sahen ihre Aufgabe vor allem darin, konkrete Typen von Kurven anzugeben und zu analysieren. Dabei ist 'analysieren' ganz analytisch gemeint: Die Bogenlänge gewisser Kurvenabschnitte oder die Fläche von Gebieten, welche die Kurve umschließt, werden mit den Mitteln der Infinitesimalrechnung berechnet. So ist die Entwicklung der Theorie (algebraischer und transzendenter) Kurven im 18. und 19. Jahrhundert eng mit der Entwicklung der Analysis verbunden.

- G. Salmon: Higher Plane Curves (1879), deutsche Bearbeitung: G. Salmon, O.W. Fiedler: Analytische Geometrie der höheren ebenen Kurven (1882)
- H. Schroeter: Theorie der ebenen Kurven (1888)
- W.H. Besant: Roulettes and Glissettes (1890)
- P. Frost: Curve Tracing (1892)
- A.B. Basset: Elementary treatise on Cubic and Quartic Curves (1901)
- G. Loria: Spezielle algebraische und transcendente ebene Kurven - Theorie und Geschichte (1902)

- F. Ebner: Leitfaden der technisch wichtigen Kurven (1906)
- H. Wieleitner: Spezielle ebene Kurven (1908)
- E. Beutel: Algebraische Kurven, Kurvendiskussion (1914)
- F. Gomes Texeira: Traite des courbes speciales remarquables planes et gauches I, II ,II (1908-15)
- S. Ganguli: The Theory of Plane Curves I, II (1919)
- H. Schmidt: Ausgewählte höhere Kurven (1949)
- E.H. Lockwood: A Book of Curves (1961)
- H. Brocard, T. Lemoyne: Courbes Geometriques Remarquables I, II, III (1967-1970)
- L.D. Lawrence: A Catalog of Special Plane Curves (1972)

Eine Online-Version dieser mehr katalogisierenden als theoretischen Art, Kurven zu untersuchen finden Sie unter der Adresse

- www-groups.dcs.st-and.ac.uk

In den 20-er Jahren des 20-ten Jahrhunderts kam es zu einem totalen Zusammenbruch der Algebraischen Geometrie, und damit auch der Theorie der ebenen algebraischen Kurven: Das angesammelte Material an Beispielen und Techniken war unübersichtlich vielfältig geworden, während gleichzeitig tragfähige Grundlagen fehlten. Man fing an, sich fast ausschließlich auf die topologischen, komplex-analytischen oder algebraischen Grundlagen zu konzentrieren. Diese Entwicklung, die erst um 1970 abebbte, hatte auch Auswirkungen auf die Lehrbücher. Die folgenden Bücher sind in diesem neuen Stil geschrieben:

- J.L. Coolidge: Treatise on Algebraic Plane Curves (1931)
- R.J. Walker: Algebraic Curves (1950)
- W. Hauser, W. Burau: Integrale algebraischer Funktionen und ebene algebraische Kurven (1958)
- H.F. Baker: Principles of Geometry, Vol. 5: Analytic Principles of the Theory of Curves (1960)
- W. Burau: Algebraische Kurven in der Ebene (1962)
- E. Brieskorn, H. Knörrer: Ebene algebraische Kurven (1981)
- M. Namba: Geometry of Projective Algebraic Curves (1984)
- G. Fischer: Ebene algebraische Kurven (1994)

1 Grundlagen

1.1 Affine und projektive Kurven

In 0.1 haben wir ebene Kurven als Teilmengen des $\mathbb{K}^2$ definiert. Im Folgenden wollen wir die präziser 'ebene *affin*-algebraische Kurven' nennen. Bei der Gestalt von Kurven in der reellen affinen Ebene macht es einen großen Unterschied, ob eine Kurve ganz in einem beschränkten Gebiet liegt (wie z.B. die Ellipse), oder sich bis ins Unendliche erstreckt (wie z.B. die Hyperbel). Ist letzteres der Fall, so ist es auch wichtig, in welcher Richtung die Kurve nach Unendlich geht, und was dann ihre Asymptoten sind, falls sie existieren. Zunächst hat man das mit den Mitteln der affinen Geometrie untersucht. Aber als die Technik der projektiven Ebene zur Verfügung stand, hat man das Verhalten der Kurve im Unendlichen beschrieben, indem man sie in die projektive Ebene fortsetzte.

Formal geht das so: Die affine Kurve werde duch das Polynom $p(x, y)$ definiert. Wir setzen $x = x_1/x_0$, $y = x_2/x_0$ und betrachten

$$p(x, y) = p\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right).$$

Das ist jetzt natürlich kein Polynom mehr. Es gibt ja Nenner, die alle Potenzen von x_0 sind. Sei x_0^d die höchste dieser Potenzen. (Dieses d ist der höchste Grad $d = m + n$ eines Monoms $x^m y^n$, das in p vorkommt.) Wir setzen

$$P(x_0, x_1, x_2) := x_0^d \cdot p\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right).$$

Das ist jetzt ein Polynom, ohne Nenner, allerdings leider in drei Variablen. Aber P ist homogen, und zwar vom Grad d. Das bedutet

$$P(tx_0, tx_1, tx_2) = t^d P(x_0, x_1, x_2).$$

Wegen $tx_i/tx_0 = x_i/x_0$ für $i = 1, 2$ folgt das sofort aus

$$P(tx_0, tx_1, tx_2) = (tx_0)^d \cdot p\left(\frac{tx_1}{tx_0}, \frac{tx_2}{tx_0}\right).$$

Äquivalent dazu ist, dass P eine Darstellung

$$P(x_0, x_1, x_2) = \sum_{\lambda+\mu+\nu=d} a_{\lambda,\mu,\nu} x_0^\lambda x_1^\mu x_2^\nu$$

besitzt.

Definition 1.1 *Das Polynom $P(x_0, x_1, x_2)$ heißt die* Homogenisierung *von $p(x, y)$. Das Polynom $p(x, y) = P(1, x, y)$ heißt das* affine *Polynom zu P.*

Satz 1.1 *a) Das Polynom p ist durch seine Homogenisierung P eindeutig bestimmt.*

b) Falls P nicht zufällig den Faktor x_0 abspaltet, ist auch umgekehrt P durch p eindeutig bestimmt.

Beweis. a) Es ist ja

$$p(x,y) = P(1,x,y).$$

b) Es sei $P(x_0,x_1,x_2)$ ein homogenes Polynom vom Grad d, das den Faktor x_0 nicht abspaltet. Das bedeutet

$$P(x_0,x_1,x_2) = \sum_{\lambda+\mu+\nu=d} a_{\lambda,\mu,\nu} x_0^\lambda x_1^\mu x_2^\nu,$$

wo mindestens einmal $\lambda = 0$ ist. Dann hat das affine Polynom zu P

$$p(x,y) = P(1,x,y)$$

auch den Grad d. Seine Homogenisierung ist

$$x_0^d \cdot P(1, \frac{x_1}{x_0}, \frac{x_2}{x_0}) = P(x_0, x_0\frac{x_1}{x_0}, x_0\frac{x_2}{x_0}) = P(x_0,x_1,x_2),$$

weil P homogen vom Grad d ist. □

Wenn P homogen ist, dann ist die Teilmenge

$$\bar{C} := \{(x_0 : x_1 : x_2) \in \mathbb{P}_2(\mathbb{K}) : \ P(x_0,x_1,x_2) = 0\}$$

wohldefiniert. Aus $P(x_0,x_1,x_2) = 0$ folgt ja für alle $t \in \mathbb{K}$

$$P(tx_0,tx_1,tx_2) = t^d P(x_0,x_1,x_2) = 0,$$

wo d der Grad von P ist.

Definition 1.2 *Eine projektive ebene algebraische Kurve ist die Nullstellenmenge $\bar{C}$ eines homogenen Polynoms $P \in \mathbb{K}[x_0,x_1,x_2]$. Der* Grad *dieser Kurve ist der Grad des Polynoms P.*

Lemma 1.1 *Es sei $C \subset \mathbb{K}^2$ eine ebene algebraische Kurve, etwa die Nullstellenmenge des Polynoms p. Weiter sei P die Homogenisierung von p und $\bar{C}$ die durch P definierte projektive ebene algebraische Kurve. Dann ist*

$$C = \mathbb{K}^2 \cap \bar{C}.$$

Dabei ist $\mathbb{K}^2 = \{(1 : x : y),\ x,y \in \mathbb{K}\}$ wie üblich der affine Teil der projektiven Ebene.

Beweis. Der Durchschnitt $\bar{C} \cap \mathbb{K}^2$ ist

$$\{(1 : x : y) : \ P(1,x,y) = 0\} = \{(x,y) \in K^2 : \ p(x,y) = 0\}.$$

□

Beispiel: Das *Folium* (= Blatt) von Descartes hat die affine Gleichung

$$x^3 + y^3 - xy = 0.$$

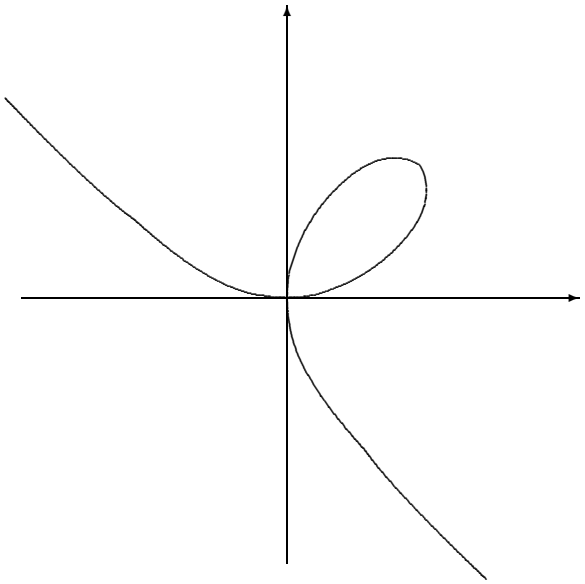
Die zugehörige projektive Kurve hat die Gleichung

$$x_1^3 + x_2^3 - x_0x_1x_2 = 0.$$

Deren Durchschnitt mit der unendlich fernen Geraden ist die Menge

$$\{(0 : x_1 : x_2) : \, x_1^3 + x_2^3 = 0\}.$$

Im Reellen gibt es nur den Punkt $(0 : 1 : -1)$, im Komplexen dazu noch die beiden Punkte $(0 : 1 : -\omega), (0 : 1 : -\omega^2)$ mit $\omega = e^{2\pi i/3}$.



1.2 Singularitäten

In der Analysis beweist man den Satz über implizite Funktionen etwa in der folgenden Form:

Es sei $f(x, y)$ eine unendlich oft differenzierbare Funktion der beiden reellen Variablen x und y, definiert auf einer offenen Menge. Ist (x_0, y_0) ein Punkt der Definitionsmenge von F mit

$$f(x_0, y_0) = 0 \quad \text{und} \quad \frac{\partial f}{\partial y}(x_0, y_0) \neq 0.$$

Dann ist die Gleichung $f(x, y) = 0$ bei diesem Punkt lokal nach y auflösbar. D.h., es gibt eine (unendlich oft) differenzierbare Funktion $g(x)$ so, dass lokal bei (x_0, y_0) gilt:

$$f(x, y) = 0 \quad \Leftrightarrow \quad y = g(x).$$

Natürlich gilt diese Aussage auch, wenn man x und y vertauscht: Ist $\partial f/\partial x \neq 0$ in (x_0, y_0) so ist die Gleichung $f(x, y) = 0$ lokal nach x auflösbar.

Zusammen erhält man: Sei (x_0, y_0) ein Punkt mit $f(x_0, y_0) = 0$, wo nicht die beiden partiellen Ableitungen verschwinden, also

$$\left(\frac{\partial f}{\partial x}(x_0, y_0), \frac{\partial f}{\partial y}(x_0, y_0)\right) \neq (0, 0),$$

so sieht dort die Nullstellenmenge von f lokal aus wie ein Funktionsgraph ($y = g(x)$ oder $x = g(y)$). Das gilt natürlich auch für Polynome:

Es sei $C \subset \mathbb{R}^2$ eine algebraische Kurve, definiert durch die Polynomgleichung $g(x,y) = 0$ und $(x_0, y_0) \in C$. Gilt in diesem Punkt

$$(\partial_x f, \partial_y f) \neq (0,0),$$

so sieht die Kurve C in der Nähe dieses Punktes aus wie ein Funktionsgraph. Derartige Punkte nennt man glatt.

Über einem beliebigen Körper ist es etwas schwierig, die Sache mit der lokalen Auflösung exakt zu machen. Aber man definiert ganz allgemein:

Definition 1.3 *Es sei $C \subset \mathbb{K}^2$ eine algebraische Kurve, definiert durch $p(x,y) = 0$ und $(x_0, y_0) \in C$. Dieser Punkt heißt*

- glatter *(oder gewöhnlicher, oder regulärer) Punkt von C, wenn dort $(p_x, p_y) \neq (0,0)$, und*
- singulärer *Punkt von C, wenn hier $p_x = p_y = 0$.*

Singuläre Punkte von C heißen auch Singularitäten.

Beispiel: Die Neilsche Parabel mit der Gleichung

$$p(x,y) = y^2 - x^3 = 0.$$

Es ist

$$p_x = -3x^2, \quad p_y = 2y.$$

Und $p_x = p_y = 0$ gilt nur, wenn $x = y = 0$. Der Nullpunkt ist die einzige Singularität.

Beispiel: Das Folium von Descartes mit der Gleichung $p(x,y) = x^3 + y^3 - xy = 0$. Nun ist

$$p_x = 3x^2 - y, \quad p_y = 3y^2 - x.$$

Aus $p_x = 0$ kann man $y = 3x^2$ eliminieren und in $p_y = 0$ einsetzen. Man erhält die Bedingung

$$3(3x^2)^2 - x = x \cdot ((3x)^3 - 1) = 0$$

mit den Lösungen $x = 0$ und $x = 1/3,\ \omega/3,\ \omega^2/3$. Symmetrisch dazu findet man für eine Singularität die Bedingungen $y = 0$ oder $y = \omega^k/3$, $k = 0,1,2$. Es ist klar, dass $(0,0)$ ein Punkt der Kurve und damit eine Singularität ist. (Vgl. dazu auch die Skizze der Kurve.) Aber kein Punkt $(0, \omega^k/3)$ oder $(\omega^k/3, 0)$ liegt auf der Kurve und kann eine Singularität sein. Als weitere mögliche Singularitäten bleiben die Punkte $(\omega^k/3, \omega^l/3)$ mit $k,l = 0,1,2$. Setzen wir sie in die Kurvengleichung ein, so erhalten wir

$$\frac{\omega^{3k}}{3^3} + \frac{\omega^{3l}}{3^3} - \frac{\omega^{k+l}}{3^2} = \frac{1}{27}(2 - 3\omega^{k+l}) = 0.$$

Man erhielte hieraus $\omega^{k+l} = 2/3$, und das ist weder für $\mathbb{K} = \mathbb{R}$ noch für $\mathbb{K} = \mathbb{C}$ möglich. In diesen Fällen ist die einzige Singularität der Nullpunkt.

In der Definition der Singularitäten haben wir Koordinaten x und y benutzt. Im Prizip könnte es vom Koordinatensystem abhängen, ob ein Kurvenpunkt singulär ist. Aber nehmen wir mal eine Koordinatentransformation

$$x = x(\xi, \eta), \quad y = y(\xi, \eta)$$

vor. Sei $q(\xi, \eta) = p(x(\xi, \eta), y(\xi, \eta))$ die transformierte Funktion. Dann ist nach der Kettenregel

$$(q_\xi, q_\eta) = (p_x, p_y) \cdot \begin{pmatrix} x_\xi & x_\eta \\ y_\xi & y_\eta \end{pmatrix}.$$

Hier wird (p_x, p_y) mit der Funktionalmatrix der Transformation multipliziert. Diese Matrix ist invertierbar. Deswegen gilt $(q_\xi, q_\eta) = (0, 0)$ genau dann, wenn $(p_x, p_y) = (0, 0)$. Die Frage, ob ein Kurvenpunkt singulär ist, ist unabhängig vom gewählten Koordinatensystem.

Das eben Gesagte gilt für affine (invertierbare) Koordinatentransformationen, aber auch für Transformationen, die man aus einer projektiven Transformation $T : \mathbb{P}_2 \to \mathbb{P}_2$ durch

$$\mathbb{K}_2 \subset \mathbb{P}_2 \xrightarrow{T} \mathbb{P}_2 \supset \mathbb{K}^2$$

erhält. Das macht die Definition der Singularitäten auch für projektive Kurven koordinatenunabhängig:

Definition 1.4 *Es sei $\mathbf{x} \in \mathbb{P}_2$ ein Punkt der projektiven algebraischen Kurve C und $\mathbb{K}^2$ ein affiner Teil der projektiven Ebene, der $\mathbf{x}$ enthält. Der Punkt $\mathbf{x} \in C$ heißt singulär, wenn der entsprechende Punkt der affinen Kurve $\mathbb{K}^2 \cap C$ singulär ist.*

Man kann also die Singularitäten einer projektiven Kurve ausrechnen, indem man (lokal) affine Koordinaten benützt. Aber es geht auch anders. Dazu brauchen wir

Satz 1.2 (Formel von Euler) *Es sei $P(x_0, x_1, x_2)$ ein homogenes Polynom vom Grad d. Dann ist*

$$x_0 \cdot \frac{\partial P}{\partial x_0} + x_1 \cdot \frac{\partial P}{\partial x_1} + x_2 \cdot \frac{\partial P}{\partial x_2} = d \cdot P.$$

Beweis. Für alle $t \in \mathbb{K}$ ist $P(tx_0, tx_1, tx_2) = t^d \cdot P(x_0, x_1, x_2)$. Daraus folgt

$$\frac{\partial}{\partial t} P(tx_0, tx_1, tx_2) = dt^{d-1} \cdot P(x_0, x_1, x_2).$$

Andererseits ergibt eine elementare Anwendung der Kettenregel in mehrereren Variablen

$$\frac{\partial}{\partial t} P(tx_0, tx_1, tx_2) = P_{x_0}(tx_0, tx_1, tx_2) \cdot x_0 + P_{x_1}(tx_0, tx_1, tx_2) \cdot x_1 + P_{x_2}(tx_0, tx_1, tx_2) \cdot x_2.$$

Setzt man nun $t = 1$ in diesen Formeln, so ergibt sich die Behauptung. □

Eine Folgerung aus der Eulerschen Formel ist

Satz 1.3 *a) Es sei $P(x_0, x_1, x_2)$ ein homogenes Polynom und $\mathbf{x} \in \mathbb{P}_2$ ein Punkt mit*

$$P_{x_0}(\mathbf{x}) = P_{x_1}(\mathbf{x}) = P_{x_2}(\mathbf{x}) = 0.$$

Dann ist auch $P(\mathbf{x}) = 0$.

b) Ein Punkt $\mathbf{x}$ der projektiven algebraischen Kurve $P(x_0, x_1, x_2) = 0$ ist genau dann eine Singularität, wenn in diesem Punkt $P_{x_0} = P_{x_1} = P_{x_2} = 0$.

Beweis. a) ist eine direkte Anwendung der Eulerschen Formel.

b) Sei $\mathbf{x}$ singulär. Wir wählen die Koordinaten so, dass in $\mathbf{x}$ die Koordinate $x_0 \neq 0$ ist. Für $p = P(1, x, y)$ gilt in dem entsprechenden Punkt des $\mathbb{K}^2$, dass $p_x = p_y = p = 0$ ist. Daraus folgt $P_{x_1}(\mathbf{x}) = P_{x_2}(\mathbf{x}) = P(\mathbf{x}) = 0$. Mit der Eulerschen Formel finden wir in diesem Punkt $\mathbf{x}$, dass $x_0 \cdot P_{x_0} = 0$ ist, wegen $x_0 \neq 0$ also $P_{x_0} = 0$.

Sei umgekehrt $P_{x_0} = P_{x_1} = P_{x_2} = 0$ in $\mathbf{x}$ vorausgesetzt. Aus der Eulerschen Formel folgt jetzt $P(\mathbf{x}) = 0$. Der Punkt $\mathbf{x}$ liegt also auf der Kurve $P = 0$. Nicht alle drei Koordinaten x_i können in $\mathbf{x}$ verschwinden. O.B.d.A. sei $x_0 \neq 0$. Wir gehen über in die affinen Koordinaten $x = x_1$, $y = x_2$ und finden in dem entsprechenden Punkt des $\mathbb{K}^2$

$$p_x = p_y = p = 0.$$

□

Die projektive Version der Bedingung für singuläre Punkte hat manchmal rechentechnische Vorteile: Um Singularitäten in affinen Koordinaten zu finden, muss man die drei Gleichungen

$$p_x = p_y = p = 0$$

lösen, zwei Gleichungen vom Grad $d-1$ und eine vom Grad d. In der projektiven Version muss man die drei Gleichungen

$$P_{x_0} = P_{x_1} = P_{x_2} = 0$$

vom Grad $d-1$ lösen.

Beispiel: Eine homogene Gleichung für das Folium von Descartes ist

$$P := x_1^3 + x_2^3 - x_0 x_1 x_2 = 0.$$

Die Bedingungen für eine Singularität sind

$$P_{x_1} = 3x_1^2 - x_0 x_2 = 0, \quad P_{x_2} = 3x_2^2 - x_0 x_1 = 0, \quad P_{x_0} = x_1 x_2 = 0.$$

Also ist entweder $x_1 = 0$ oder $x_2 = 0$. Wenn $x_1 = 0$ ist, so folgt aus $P_{x_2} = 0$ auch $x_2 = 0$. Und wenn $x_2 = 0$ sein sollte, erhält man mit $P_{x_1} = 0$ denselben Punkt $(1 : 0 : 0)$.

Beispiel: Die Kurve mit der Gleichung

$$f(x_0, x_1, x_2) := x_0^n + x_1^n + x_2^n = 0$$

heißt *Fermat*-Kurve vom Grad n. Diese Kurven sind zahlen-theoretisch sehr interessant, optisch aber sehr langweilig. Deswegen zeichne ich sie auch nicht. (Für gerades n haben sie nicht einmal reelle Punkte.) Aber man kann besonders leicht nachrechnen, dass sie glatt sind: Die partiellen Ableitungen

$$\frac{\partial f}{\partial x_i} = n x_i^{n-1}$$

verschwinden nur, wenn $x_0 = x_1 = x_2 = 0$. Den Punkt gibt es nicht.

1.3 Lineare Schnitte, Tangenten

Es sei $C \subset \mathbb{P}_2$ eine algebraische Kurve und $L \subset \mathbb{P}_2$ eine Gerade. Welche Möglichkeiten gibt es für den Durchschnitt $C \cap L$? Natürlich muss man das Polynom P, welches die Kurve definiert, auf die Gerade L einschränken, und die Nullstellen des eingeschränkten Polynoms suchen. Wir können die Koordinaten so anpasssen, dass L die Gleichung $x_0 = 0$ hat. Die Punkte auf L sind dann von der Form $(0 : x_1 : x_2)$ und das eingeschränkte Polynom ist $P(0, x_1, x_2)$. Da gibt es zwei prinzipiell verschiedene Möglichkeiten:

1) Das Polynom $P(0, x_1, x_2)$ kann identisch verschwinden. Das ist äquivalent mit $L \subset C$. Entwickeln wir

$$P(x_0, x_1, x_2) = \sum_{\lambda+\mu+\nu=d} a_{\lambda,\mu,\nu} x_0^\lambda x_1^\mu x_2^\nu,$$

so ist $P(0, x_1, x_2)$ identisch $= 0$, genau dann, wenn alle Koeffizienten $a_{0,\mu,\nu} = 0$ sind. Aber Vorsicht: Das gilt nur, wenn der Grundkörper $\mathbb{K}$ unendlich viele Elemente enthält! Ist dies der Fall, so kommt die Koordinate x_0 in jedem Summanden vor, der einen Koeffizienten $a_{\lambda,\mu,\nu} \neq 0$ besitzt. Jeder Summand ist durch x_0 teilbar, und dann spaltet auch $P(x_0, x_1, x_2)$ den Faktor x_0 ab. Natürlich ist es unwesentlich, dass wir die Gerade $L : x_0 = 0$ genommen haben. Wenn wir eine andere Gerade haben, sie auf $x_0 = 0$ transformieren, und wieder zurück-transformieren, so sehen wir: Eine Gerade $L : l(x_0, x_1, x_2) = 0$ gehört genau dann zu der algebraischen Kurve $C : P(x_0, x_1, x_2) = 0$, wenn P den Linearfaktor l abspaltet.

2) Im Allgemeinen wird das Polynom $P(0, x_1, x_2)$ nicht identisch verschwinden. Dann ist das Polynom $P(0, x_1, x_2)$ wieder homogen vom Grad $d = deg(P)$, nicht das Null-Polynom. Das ist ein fundamentaler Unterschied zum affinen Fall: Sei etwa C die Hyperbel $p(x, y) := xy - 1 = 0$ und L die Gerade $y = c$. Das auf die Gerade L eingeschränkte Polynom $p(c, x) = cx - 1$ hat immer den Grad 1, außer für $c = 0$, wo es sogar den Grad 0 hat. Im Projektiven hat also das eingeschränkte Polynom $P(0, x_1, x_2)$ immer den gleichen Grad d wie P. Nach der homogenen Version des Fundamentalsatzes der Algebra zerfällt $P(0, x_1, x_2)$ in d Linearfaktoren, die zu d Schnittpunkten in $L \cap C$ gehören. Allerdings kann es mehrfache Faktoren, also Schnittpunkte die mehrfach zählen, geben. Hier müssen wir als Grundkörper natürlich $\mathbb{K} = \mathbb{C}$ voraussetzen.

Wir fassen zusammen:

Satz 1.4 *Es sei $C : P = 0$ in $\mathbb{P}_2(\mathbb{K})$ eine algebraische Kurve und $L : l = 0$ in $\mathbb{P}_2(\mathbb{K})$ eine Gerade.*

a) Der Körper $\mathbb{K}$ enthalte unendlich viele Elemente. Dann ist $L \subset C$ äquivalent dazu, dass P den Faktor l abspaltet.

b) Es sei $\mathbb{K} = \mathbb{C}$ und d der Grad von P. Weiter sei $L \not\subset C$. Dann ist $L \cap C$ nicht leer. Jeder Schnittpunkt zählt mit einer Vielfachheit, und die Summe dieser Vielfachheiten ist $= d$.

Definition 1.5 *Es sei C eine algebraische Kurve, $\mathbf{a} \in C$, und L eine Gerade durch $\mathbf{a}$. Die Vielfachheit von $\mathbf{a}$ als Schnittpunkt von C und L bezeichnet man mit $i_{\mathbf{a}}(C, L)$.*

Was bedeutet $i_{\mathbf{a}}(C, L) > 1$? Es genügt, dies für eine affine Kurve $C : p(x, y) = 0$ zu untersuchen. Dazu parametrisieren wir die Gerade als $L : \mathbf{x} = \mathbf{a} + t \cdot \mathbf{v}$, $t \in \mathbb{K}$, mit einem Richtungsvektor $\mathbf{v} \neq \mathbf{0}$. Wegen $\mathbf{a} \in C$ ist

$$p(\mathbf{a}) = p(\mathbf{a} + t\mathbf{v})|_{t=0} = 0$$

und die Bedingung wird

$$\frac{\partial}{\partial t} p(\mathbf{a} + t\mathbf{v})|_{t=0} = 0.$$

Sei etwa $\mathbf{v} = (v_1, v_2)$. Dann folgt aus der Kettenregel

$$\frac{\partial}{\partial t} p(\mathbf{a} + t\mathbf{v}) = p_x v_1 + p_y v_2.$$

Dafür, dass diese Ableitung verschwindet, gibt es zwei Möglichkeiten:

- Entweder ist $p_x(\mathbf{a}) = p_y(\mathbf{a}) = 0$ und $\mathbf{a}$ ist eine Singularität der Kurve C.
- Oder es gilt $(p_x(\mathbf{a}), p_y(\mathbf{a})) \neq (0, 0)$ und $\mathbf{v}$ steht senkrecht auf dem Gradienten $(p_x(\mathbf{a}), p_y(\mathbf{a}))$ von p in $\mathbf{a}$. Die Gleichung der Geraden L ist dann

$$p_x(\mathbf{a})(x - a_1) + p_y(\mathbf{a})(y - a_2) = 0.$$

Diese Geradengleichung wollen wir jetzt homogen schreiben. Wie üblich setzen wir $\mathbf{x} = (1 : x : y)$ und $\mathbf{a} = (1 : a_1 : a_2)$. Aus $P(\mathbf{a}) = 0$ folgt mit der Eulerschen Formel

$$1 \cdot P_0(\mathbf{a}) + a_1 \cdot P_1(\mathbf{a}) + a_2 \cdot P_2(\mathbf{a}) = 0,$$

bzw.

$$-(p_x(\mathbf{a}) \cdot a_1 + p_y(\mathbf{a}) \cdot a_2) = P_0(\mathbf{a}).$$

Dann wird die Geradengleichung

$$P_0(\mathbf{a}) \cdot x_0 + P_1(\mathbf{a}) \cdot x_1 + P_2(\mathbf{a}) \cdot x_2 = 0.$$

Definition 1.6 *Es sei* $\mathbf{a}$ *ein regulärer Punkt der algebraischen Kurve* $C : P = 0$. *Dann heißt die Gerade mit der Gleichung*

$$P_0(\mathbf{a}) \cdot x_0 + P_1(\mathbf{a}) \cdot x_1 + P_2(\mathbf{a}) \cdot x_2 = 0$$

die Tangente $T_{\mathbf{a}}(C)$ *im Punkt* $\mathbf{a}$.

Die Tangente $T_{\mathbf{a}}(C)$ ist die einzige Gerade durch den regulären Punkt $\mathbf{a}$, welche C in $\mathbf{a}$ mit einer Vielfachheit $i > 1$ schneidet. Daraus folgt, dass die Tangente projektiv invariant definiert ist. Wir hätten ihre Gleichung auch ohne den Umweg über die affinen Koordinaten finden können, wenn wir die Kettenregel in den drei Veränderlichen x_0, x_1, x_2 benutzt hätten. Wir halten fest:

Satz 1.5 *Es sei* $\mathbf{a}$ *ein Punkt der algebraischen Kurve* $C \subset \mathbb{P}_2$ *und* L *eine Gerade durch diesen Punkt. Dann ist* $i_{\mathbf{a}}(C, L) > 1$ *genau dann, wenn entweder*

- $\mathbf{a} \in C$ *singulär ist,*
- *oder* $\mathbf{a} \in C$ *regulär ist und* L *die Tangente* $T_{\mathbf{a}}(C)$.

Für jede Gerade $L \neq T_{\mathbf{a}}(C)$ durch den regulären Punkt $\mathbf{a} \in C$ ist also $i_{\mathbf{a}}(C, L) = 1$. Man sagt, solche Geraden schneiden die Kurve *transversal*.

Beispiel: Sei C die Hyperbel mit der affinen Gleichung

$$x^2 - y^2 = 1$$

und der homogenen Gleichung $x_1^2 - x_2^2 - x_0^2 = 0$. Ihre Punkte im Unendlichen sind $(0 : 1 : \pm 1)$. Die Tangenten in diesen beiden Punkten haben die Gleichungen

$$2 \cdot 1 \cdot x_1 - 2 \cdot (\pm 1) \cdot x_2 = 0, \quad \text{bzw.} \quad x_1 = \pm x_2.$$

Affin geschrieben sind dies die beiden Asymptoten der Hyperbel.

Beispiel: Wir betrachten das Folium von Descartes mit der homogenen Gleichung $P := x_1^3 + x_2^3 - x_0 x_1 x_2 = 0$ und darauf den unendlich fernen Punkt $(0 : 1 : -1)$. Die Tangente an diesen Punkt hat die Gleichung

$$P_0 x_0 + P_1 x_1 + P_2 x_2 = x_0 + 3x_1 + 3x_2 = 0.$$

Affin ist dies die Gerade $x + y = -1/3$. Wenn die Schnittvielfachheit der Tangente $= 2$ ist, muss es noch einen weiteren Schnittpunkt geben. Weil die Tangente die unendlich ferne Gerade nur in einem Punkt schneidet, müsste es ein affiner Punkt sein. Wir könnten ihn ausrechnen indem wir $y := -x - 1/3$ in die Kurvengleichung einsetzen:

$$x^3 - (x + 1/3)^3 + x(x + 1/3) = -1/27 = 0.$$

Das geht nicht. Also gibt es keinen weiteren solchen Punkt, und die Schnittvielfachheit war $= 3$.

1.4 Zerlegung in irreduzible Komponenten

Es seien $C_1, C_2 \subset \mathbb{P}_2$ zwei algebraische Kurven. Dann ist auch ihre Vereinigungsmenge $C_1 \cup C_2$ eine algebraische Kurve. Denn seien etwa $P_i = 0$, $i = 1, 2$, die Gleichungen der beiden Kurven. Dann gilt

$$P_1(\mathbf{x}) = 0 \text{ oder } P_2(\mathbf{x}) = 0 \quad \Leftrightarrow \quad P_1(\mathbf{x}) \cdot P_2(\mathbf{x}) = 0.$$

$C_1 \cup C_2$ ist also die algebraische Kurve mit der Gleichung $P_1 \cdot P_2 = 0$.

Definition 1.7 *Das homogene Polynom $P \in \mathbb{K}[x_0, x_1, x_2]$ heißt* irreduzibel*, wenn es nicht ein Produkt zweier Polynome kleineren Grades ist. Anders ausgedrückt: Wenn $P = P_1 \cdot P_2$ ist mit $P_1, P_2 \in \mathbb{K}[x_0, x_1, x_2]$, so ist entweder $P_1 \in \mathbb{K}$ eine Konstante, oder $P_2 \in \mathbb{K}$.*

Die algebraische Kurve C mit der Gleichung $P = 0$ heißt irreduzibel*, wenn P irreduzibel ist.*

Da stellen sich sofort einige Fragen: Ist P die Homogenisierung von $p \in \mathbb{K}[x, y]$, so führt jede Faktorisierung $p = p_1 \cdot p_2$ zu einer Faktorisierung von P. Gilt das auch umgekehrt? Natürlich kann P den Faktor $P_1 = x_0$ abspalten, ohne dass man das dem Polynom p ansieht. Aber, wenn man davon absieht, läuft das auf folgende Tatsache hinaus:

Satz 1.6 *Sei $P \in \mathbb{K}[x_0, x_1, x_2]$ homogen. Wenn $P = P_1 \cdot P_2$ ein Produkt ist mit $P_1, P_2 \in \mathbb{K}[x_0, x_1, x_2]$, dann sind die beiden Polynome P_1 und P_2 wieder homogen.*

Beweis. Jedes Polynom in $\mathbb{K}[x_0, x_1, x_2]$ ist Summe homogener Bestandteile, etwa

$$P_1 = \sum_{\mu=a_1}^{b_1} P_{1,\mu}, \quad P_2 = \sum_{\nu=a_2}^{b_2} P_{2,\nu},$$

mit homogenen Polynomen $P_{1,\mu}$ vom Grad μ und $P_{2,\nu}$ vom Grad ν. In diesen Summen können wir Nullpolynome weglassen, und annehmen, dass die Polynome $P_{1,a_1}, P_{1,b_1}, P_{2,a_2}, P_{2,b_2}$ keine Nullpolynome sind. Dann enthält P als homogene Summanden $\neq 0$ die Polynome

$$P_{1,a_1} \cdot P_{2,a_2} \text{ vom Grad } a_1 + a_2 \text{ und } P_{1,b_1} \cdot P_{2,b_2} \text{ vom Grad } b_1 + b_2.$$

Weil P homogen ist, muss $a_1 + a_2 = b_1 + b_2$ gelten. Aus $a_i \leq b_i$ folgt $a_1 = b_1$, $a_2 = b_2$, und beide Faktoren P_1, P_2 müssen homogen sein. □

Weil Faktorisierungen von p und P (bis auf Potenzen von x_0) übereinstimmen, betrachten wir jetzt nur noch affine Kurven $C : p(x, y) = 0$. Entweder ist p irreduzibel, oder $p = p_1 \cdot p_2$ mit Faktoren p_1, p_2 kleineren Grades. Diese Zerlegung können wir iterieren und beweisen:

Satz 1.7 *Jedes Polynom $p \in \mathbb{K}[x, y]$ ist ein Produkt $p = p_1 \cdot ... \cdot p_k$ irreduzibler Polynome $p_1, ..., p_k \in \mathbb{K}[x, y]$. Jede (affine oder projektive) ebene algebraische Kurve C ist Vereingung $C = C_1 \cup ... \cup C_k$ irreduzibler Kurven.*

Definition 1.8 *Die irreduziblen Kurven $C_1, ..., C_k$ aus Satz 1.7 heißen die* irreduziblen Komponenten *von C.*

Die Zerlegung einer Kurve in irreduzible Komponenten vereinfacht das Leben etwas, weil man viele Probleme auf die Behandlung irreduzibler Kurven zurückführen kann. Allerdings muss man folgenden Effekt berücksichtigen:

Satz 1.8 *Ist $C = C_1 \cup C_2$, so ist jeder Punkt $\mathbf{x} \in C_1 \cap C_2$ ein singulärer Punkt von C.*

Beweis. Es sei $P_i = 0$ die Gleichung von C_i. Dann ist $P = P_1 \cdot P_2$ ein Polynom, das C definiert. Und wegen $\mathbf{x} \in C_i$, $i = 1, 2$, gilt in $\mathbf{x}$

$$\partial_\nu P = (\partial_\nu P_1) \cdot P_2 + P_1 \cdot (\partial_\nu P_2) = 0 \quad \text{für} \quad \nu = 0, 1, 2.$$

□

Wenn hier $C_1 = C_2$ ist, dann führt das auf eine merkwürdige Komplikation:

$$C = C_1 = C_2 = C_1 \cup C_2$$

Sei $P = 0$ eine Gleichung für C und dann auch für C_1 und C_2. Es erscheint zunächst töricht, formal für $C_1 \cup C_2$ die Gleichung $P^2 = 0$ zu nehmen. Es ist ja $P^2(\mathbf{x}) = 0$ genau dann, wenn $P(\mathbf{x}) = 0$. Beide Polynome P und P^2 beschreiben dieselbe Kurve C. Die Kurve ist gleich, die

Gleichungen sind verschieden. Daraus lernen wir: Eine Kurve ist nicht nur eine Menge, sondern es muss immer eine Gleichung für diese Menge festgelegt sein.

Diesen Effekt kennt man schon von den Kegelschnitten her: Sei $L \subset \mathbb{P}_2$ eine Gerade mit der Gleichung $l(x_0, x_1, x_2) = 0$, wo l homogen vom Grad 1 ist. Dann ist L eine glatte Kurve. Dieselbe Punktmenge hat aber auch die Gleichung $l^2 = 0$. Jetzt ist die ein Kegelschnitt, dessen Punkte alle singulär sind. Dieser Effekt ist nicht weiter schlimm, sondern nur gewöhnungsbedürftig. Eine Kurve ist nicht nur eine Punktmenge, sondern (wichtiger noch), dazu gehört immer auch ein definierendes Polynom.

Das führt jetzt weiter auf zwei höchst nicht-triviale Fragen. Die erste möchte ich hier noch nicht problematisieren und vorläufig geheimhalten. Auf die zweite kann nur ein Mathematiker kommen, der eine moderne Ausbildung genossen hat, in der klassischen Geometrie wurde sie als selbstverständlich erfüllt angenommen:

Es sei $C = C_1 \cup ... \cup C_k$ die Zerlegung einer Kurve in irreduzible Komponenten. Sind die Komponenten C_i durch C eindeutig bestimmt?

Das (bis auf den eben vorgestellten Effekt mehrfacher Komponenten) dazu äquivalente algebraische Problem ist:

Es sei $p \in \mathbb{K}[x, y]$ und $p = p_1 \cdot ... \cdot p_k$ mit irreduziblen Polynomen $p_1, ..., p_k \in \mathbb{K}[x, y]$. Sind die irreduziblen Faktoren p_i (bis auf ihre Reihenfolge) durch p eindeutig bestimmt?

Äquivalent zu dieser Frage ist offensichtlich: Es sei $q \in \mathbb{K}[x, y]$ ein irreduzibles Polynom. Teilt q ein Produkt $p_1 \cdot p_2$, so teilt q einen Faktor p_i. Wir wollen uns dieser Frage vorsichtig nähern, und erst einmal Polynome in einer Veränderlichen untersuchen.

Wir betrachten also jetzt Polynome $p, q \in \mathbb{K}[x]$. Das ebenso simple (weil aus dem Gymnasium bekannte) wie durchschlagskräftige Werkzeug ist die Division mit Rest: Zu p und q gibt es Polynome $p_1, r_1 \in \mathbb{K}[x]$ derart, dass

$$p = p_1 \cdot q + r_1, \quad deg(r_1) < deg(q).$$

Der für uns wichtige Punkt ist: Jeder gemeinsame Teiler von p und q teilt auch r_1. Und jeder gemeinsame Teiler von q und r_1 teilt auch p. Die gemeinsamen Teiler von p und q, bzw. q und r_1 stimmen überein. Und diese Division kann man iterieren:

$$\begin{aligned}
q &= p_2 \cdot r_1 + r_2, \quad deg(r_2) < deg(r_1) \\
r_1 &= p_3 \cdot r_2 + r_3, \quad deg(r_3) < deg(r_2) \\
&\vdots \\
r_{k-2} &= p_k \cdot r_{k-1} + r_k, \quad deg(r_k) < deg(r_{k-1}) \\
r_{k-1} &= p_{k+1} \cdot r_k
\end{aligned}$$

Weil die Reste immer (echt) kleineren Grad haben, ist irgendwann Schluss: r_{k-1} ist durch r_k teilbar. Dann ist auch r_{k-2} und r_{k-1} durch r_k teilbar, ... , p und q durch r_k teilbar. Der letzte Rest r_k ist also ein gemeinsamer Teiler von p und q. Andererseits ist

$$\begin{aligned}
r_k &= r_{k-2} - p_k r_{k-1} \\
&= r_{k-2} - p_k(r_{k-3} - p_{k-1} r_{k-2})
\end{aligned}$$

$$
\begin{aligned}
&= (1 + p_k p_{k-1}) r_{k-2} - p_k r_{k-3} \\
&\vdots \\
&= f \cdot p + g \cdot q
\end{aligned}
$$

mit irgendwelchen Polynomen $f, g \in \mathbb{K}[x]$. Daraus folgt, dass jeder gemeinsame Teiler von p und q auch umgekehrt ein Teiler von r_k ist. Das bedeutet: r_k ist der *größte gemeinsame Teiler* $ggT(p, q)$ von p und q. Dieses Verfahren, die Division mit Rest zu iterieren heißt *euklidischer Algorithmus*. Wir fassen zusammen:

Satz 1.9 *Zu zwei Polynomen $p, q \in \mathbb{K}[x]$ gibt es einen größten gemeinsamen Teiler $r = ggT(p, q)$. Er lässt sich als $r = f \cdot p + g \cdot q$ mit $f, g \in \mathbb{K}[x]$ schreiben.*

Es kann natürlich passieren, dass r kein echtes Polynom (von einem Grad > 0) ist. Dann kann man $r = 1$ wählen. Man sagt, p und q sind *teilerfremd*.

Mit diesem ggT löst sich unser p, q-Problem von oben wie folgt: Das irreduzible Polynom q teile ein Produkt $p_1 \cdot p_2$. Wenn q weder p_1 noch p_2 teilt, dann ist

$$ggT(q, p_1) = ggT(q, p_2) = 1$$

und

$$1 = f_1 \cdot q + g_1 \cdot p_1 = f_2 \cdot q + g_2 \cdot p_2.$$

Daraus folgt

$$
\begin{aligned}
1 &= (f_1 \cdot q + g_1 \cdot p_1) \cdot (f_2 \cdot q + g_2 \cdot p_2) \\
&= (f_1 f_2 + f_1 g_2 p_2 + f_2 g_1 p_1) \cdot q + g_1 g_2 \cdot p_1 p_2
\end{aligned}
$$

Der ggT von q und $p_1 p_2$ ist $= 1$ und kann kein echtes Polynom sein. Also hat q das Produkt $p_1 p_2$ gar nicht geteilt. Damit haben wir bewiesen:

Satz 1.10 *Die Zerlegung eines Polynoms $p \in \mathbb{K}[x]$ in irreduzible Faktoren ist eindeutig (bis auf die Reihenfolge der Faktoren, oder Multiplikation mit Konstanten $\in \mathbb{K}$).*

Das ist sehr lehrreich. Aber was bringt es uns für Polynome $p \in \mathbb{K}[x, y]$, an denen wir ja eigentlich interessiert sind? Die geniale Idee ist, den Ring $\mathbb{K}[x, y]$ als Unterring des Polynomrings $\mathbb{K}(x)[y]$ in einer Veränderlichen y aufzufassen. Dabei ist

$$\mathbb{K}(x) = \{\frac{z(x)}{n(x)},\ z(x), n(x) \in \mathbb{K}[x],\ n(x) \neq 0\}$$

der Körper der rationalen Funktionen in x. Wie immer in kritischen Situationen, kann man sich auch hier auf Gauß verlassen.

Satz 1.11 (Lemma von Gauß) *Das Polynom $p(x, y)$ sei irreduzibel im Ring $\mathbb{K}[x, y]$. Dann ist es auch irreduzibel im Ring $\mathbb{K}(x)[y]$.*

Beweis. Wir schreiben

$$p(x,y) = \sum_{\lambda=0}^{l} p_\lambda(x) y^\lambda, \quad p_\lambda \in \mathbb{K}[x].$$

Wenn $p(x,y) \in \mathbb{K}[x,y]$ irreduzibel ist, kann man es auch durch kein Polynom teilen, das nur von x abhängt. Es ist

$$ggT(p_0(x), ..., p_l(x)) = 1.$$

Lemma 1.2 (Hilfs-Lemma) *Es seien*

$$p(x,y) = \sum_{0}^{l} p_{\lambda(x)} y^\lambda, \quad q(x,y) = \sum_{0}^{m} q_\mu(x) y^\mu \quad \in \mathbb{K}[x,y]$$

Polynome mit

$$ggT(p_0(x), ..., p_l(x)) = ggT(q_0(x), ..., q_m(x)) = 1.$$

Dann ist

$$p(x,y) \cdot q(x,y) = \sum_{0}^{l+m} a_\nu(x) y^\nu$$

auch ein Polynom mit

$$ggT(a_0(x), ..., a_{l+m}(x)) = 1.$$

Beweis. Es sei $a(x) \in \mathbb{K}[x]$ ein Polynom, das alle Koeffizienten $a_0 x, ..., a_{l+m}(x)$ des Produkts $p \cdot q$ teilt. Weil die Koeffizienten $p_0(x), ..., p_l(x)$ teilerfremd sind, gibt es einen ersten Koeffizienten $p_{\lambda_1}(x)$, den $a(x)$ nicht teilt. Ebenso gibt es einen ersten Koeffizienten $q_{\mu_1}(x)$, den $a(x)$ nicht teilt. Für $\nu := \lambda_1 + \mu_1$ ist der ν-te Koeffizient von $p \cdot q$

$$a_\nu(x) = \sum_{\lambda+\mu=\nu} p_\lambda(x) q_\mu(x) = \sum_{\lambda<\lambda_1} p_\lambda(x) q_{\nu-\lambda}(x) + p_{\lambda_1}(x) q_{\mu_1}(x) + \sum_{\mu<\mu_1} p_{\nu-\mu}(x) q_\mu(x).$$

Hier teilt $a(x)$ alle Koeffizienten $p_\lambda(x) q_\mu(x)$ mit $\lambda < \lambda_1$ oder $\mu < \mu_1$. Weil $a(x)$ weder $p_{\lambda_1}(x)$ noch $q_{\mu_1}(x)$ teilt, folgt aus Satz 1.10, dass $a(x)$ auch deren Produkt $p_{\lambda_1}(x) q_{\mu_1}(x)$ nicht teilt. Somit ist $a_\nu(x)$ nicht durch $a(x)$ teilbar. □

Jetzt machen wir weiter mit dem Beweis des Lemmas von Gauß. Angenommen, wir hätten eine Zerlegung

$$p(x,y) = q_1(x,y) \cdot q_2(x,y), \quad q_1, q_2 \in \mathbb{K}(x)[y].$$

Wir bilden den Hauptnenner $n_i(x)$ aller Koeffizienten von q_i und klammern $z_i(x)$, den ggT aller Koeffizienten von $n_i \cdot q_i$ aus:

$$q_1(x,y) = \frac{z_1(x)}{n_1(x)} \cdot p_1(x,y), \quad q_2(x,y) = \frac{z_2(x)}{n_2(x)} \cdot p_2(x,y).$$

Dann sind p_1 und p_2 Polynome in x, y, deren Koeffizienten (Polynome in x) keinen nichtkonstanten gemeinsamen Teiler haben. Nach dem Hilfs-Lemma haben auch die Koeffizienten

des Produkts $p_1(x,y) \cdot p_2(x,y)$ keinen nicht-konstanten gemeinsamen Teiler. Wir betrachten die Gleichung

$$n_1(x)n_2(x) \cdot p(x,y) = z_1(x)z_2(x) \cdot p_1(x,y)p_2(x,y).$$

Hier ist (bis auf konstante Faktoren aus $\mathbb{K}$) der ggT aller Koeffizienten der linken Seite $= n_1(x)n_2(x)$ und auf der rechten Seite $= z_1(x)z_2(x)$. Es folgt (wieder bis auf konstante Faktoren aus $\mathbb{K}$)

$$n_1(x)n_2(x) = z_1(x)z_2(x)$$

und

$$p(x,y) = p_1(x,y) \cdot p_2(x,y).$$

Das ist eine Zerlegung von $p(x,y)$ in $\mathbb{K}[x,y]$, Widerspruch! □

So, jetzt können wir beginnen, die Eindeutigkeit einer Zerlegung

$$p(x,y) = p_1(x,y) \cdot ... \cdot p_k(x,y)$$

in irreduzible Faktoren $p_\kappa \in \mathbb{K}[x,y]$ zu beweisen. Eine solche Zerlegung ist ja auch eine Faktorisierung im Polynomring $\mathbb{K}(x)[y]$ einer Veränderlichen y. Als solche ist sie eindeutig. Eindeutig heißt aber leider: bis auf Faktoren aus $\mathbb{K}(x)$, und der Teufel steckt im Detail. Seien wir vorsichtig: Schreiben wir

$$p(x,y) = n(x) \cdot p'(x,y),$$

wo $n(x)$ der ggT aller Koeffizienten von $p(x,y)$ ist. Die Zerlegung von $n(x)$ im Ring $\mathbb{K}[x]$ ist eindeutig. Wir können deswegen o.B.d.A. voraussetzen: Die Koeffizienten von $p(x,y) \in \mathbb{K}[x][y]$ haben keinen nicht-konstanten gemeinsamen Teiler. Das gilt dann auch für die Faktoren $p_1, ..., p_k$. Seien etwa zwei Zerlegungen

$$p = p_1 \cdot ... \cdot p_k = q_1 \cdot ... \cdot q_l$$

gegeben. Wegen der Eindeutigkeit der Zerlegung über $\mathbb{K}(x)$ folgt $k = l$, und nach Umordnung

$$p_i(x,y) = \frac{z_i(x)}{n_i(x)} \cdot q_i(x,y), \quad i = 1, ..., l.$$

Wieder betrachten wir die Polynomgleichung

$$n_i(x) \cdot p_i(x,y) = z_i(x) \cdot q_i(x,y).$$

Hier ist $n_i(x)$ der ggT aller Koeffizienten auf der linken Seite und $z_i(x)$ der ggT der Koeffizienten auf der rechten Seite. Bis auf konstante Faktoren aus $\mathbb{K}$ folgt $n_i(x) = z_i(x)$ und damit $p_i(x,y) = q_i(x,y)$. Wir haben fertig:

Satz 1.12 *Die Zerlegung eines Polynoms $p(x,y) \in \mathbb{K}[x,y]$ in irreduzible Faktoren ist eindeutig, bis auf die Reihenfolge der Faktoren und eventuelle Faktoren $\in \mathbb{K}$.*

2 Resultante, Schnittzahlen

Jetzt wollen wir uns mit dem Fundamentalproblem der Vorlesung beschäftigen, das ich bisher (aus didaktischen Gründen) nicht erwähnt habe. Inwieweit ist die Gleichung $p(x,y) = 0$ einer Kurve $C \subset \mathbb{K}^2$ durch die Kurve eindeutig bestimmt? Da gibt es die offensichtliche Antwort: Aus einem trivialen Grund überhaupt nicht. Sei etwa $p = p_1 \cdot ... \cdot p_m$ die Zerlegung in irreduzible Faktoren. Wir wählen beliebige Potenzen $k_1, ..., k_m \geq 1$. Dann definiert das Polynom $p_1^{k_1} \cdot ... \cdot p_m^{k_m}$ die gleiche Kurve wie p. Diesen Effekt kennen wir schon. Wir schließen ihn wie folgt aus:

Es sei $p(x,y) \in \mathbb{K}[x,y]$ irreduzibel. Inwieweit ist p durch die Punktmenge $C := \{(x,y) \in \mathbb{K}^2 : p(x,y) = 0\}$ eindeutig bestimmt? Auch da gibt es wieder die offensichtliche Antwort: Aus einem trivialen Grund überhaupt nicht. Sei etwa $\mathbb{K} = \mathbb{R}$. Dann haben die irreduziblen Polynome x^2+1 und y^2+1 dieselbe Nullstellenmenge, nämlich die leere Menge, obwohl sich beide Polynome nicht um einen konstanten Faktor unterscheiden. Das liegt aber am Grundkörper. Die Nullstellenmengen in $\mathbb{C}^2$ sind $x = \pm i$, bzw. $y = \pm i$. Die sind nicht identisch.

Wir müssen also $\mathbb{K} = \mathbb{C}$ voraussetzen. Und dann gilt:

Satz 2.1 *Es sei $p(x,y) \in \mathbb{C}[x,y]$ ein irreduzibles Polynom mit der Nullstellenmenge $C \subset \mathbb{C}^2$. Ist $f(x,y) \in \mathbb{C}[x,y]$ ein weiteres Polynom, das in allen Punkten von $\mathbb{C}$ verschwindet, so ist $f = p \cdot g$ mit $g \in \mathbb{C}[x,y]$.*

Dies ist ein elementarer Spezialfall des sogenannten *hilbertschen Nullstellensatzes*. Ich kenne die Aussage auch noch unter dem Namen 'Lemma von Study', bzw. 'Lemma von van der Woude'. Ich möchte diese Aussage so elementar wie möglich beweisen und dabei die Resultante benutzen.

2.1 Definition und Eigenschaften der Resultante

Sei zunächst $\mathbb{K}$ ein beliebiger Körper. Wir betrachten in $\mathbb{K}[x]$ zwei Polynome

$$f = a_0 x^m + ... + a_{m-1}x + a_m, \quad g = b_0 x^n + ... + b_{n-1}x + b_n.$$

Für $\varphi := g$, $\psi := -f$ gilt offensichtlich

$$\varphi \cdot f + \psi \cdot g = 0.$$

Satz 2.2 *Es gibt Polynome $\varphi, \psi \in \mathbb{K}[x]$, $\varphi \neq 0 \neq \psi$, mit*

$$\varphi \cdot f + \psi \cdot g = 0 \in \mathbb{K}[x], \quad deg(\varphi) < deg(g),\ deg(\psi) < deg(f),$$

genau dann, wenn

$$R_{f,g} := det \begin{pmatrix} a_m & a_{m-1} & ... & a_0 & & \\ & a_m & a_{m-1} & ... & a_0 & \\ & & \ddots & \ddots & & \ddots \\ b_n & b_{n-1} & ... & b_0 & & \\ & b_n & b_{n-1} & ... & b_0 & \\ & & \ddots & \ddots & & \ddots \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} m \end{matrix} = 0.$$

Beweis. Sei V der $\mathbb{K}$-Vektorraum der Polynome in x vom Grad $< m+n$. Er hat die Basis

$$1,\ x,\ ...,\ x^{m+n-1}.$$

Die Zeilen der obigen Matrix sind die Koeffizienten der Polynome

$$f,\ x\cdot f, ..., x^{n-1}\cdot f, \quad g,\ x\cdot g, ..., , x^{m-1}\cdot g$$

in dieser Basis. Die Determinente $R_{f,g}$ verschwindet genau dann, wenn es Koeffizienten

$$(c_0, c_1, ..., c_{n-1}, d_0, d_1, ..., d_{m-1}) \neq (0, ..., 0) \in \mathbb{K}^{n+m}$$

gibt mit

$$c_0 f + c_1 x f + ... + c_{n-1} x^{n-1} f + d_0 g + d_1 x g + ... + d_{m-1} x^{m-1} g = 0.$$

Wir setzen

$$\varphi := c_0 + c_1 x + ... + c_{n-1} x^{n-1}, \quad \psi := d_0 + d_1 x + ... + d_{m-1} x^{m-1}$$

und finden

$$\varphi \cdot f + \psi \cdot g = 0.$$

Nach Konstruktion können nicht beide Polynome φ und ψ das Nullpolynom sein. Aber wenn eines der Polynome das Nullpolynom ist, dann auch das andere. Also sind beide Polynome $\neq 0$. □

Beispiel: Es seien

$$f := x + a, \quad g := x + b.$$

Dann ist

$$R_{f,g} = det \begin{pmatrix} 1 & a \\ 1 & b \end{pmatrix} = b - a$$

die Differenz der Nullstellen.

Definition 2.1 *Das Element $R_{f,g} \in \mathbb{K}$ heißt die* Resultante *der beiden Polynome $f, g \in \mathbb{K}[x]$.*

Die Bedeutung der Resultante liegt an folgender Eigenschaft:

Satz 2.3 *Für $f, g \in \mathbb{K}[x]$ ist $R_{f,g} = 0$ genau dann, wenn f und g einen gemeinsamen Faktor aus $\mathbb{K}[x]$ vom Grad > 0 besitzen.*

Beweis $\Leftarrow$: Sei $f = h \cdot f_1$ und $g = h \cdot g_1$ mit einem Polynom $h \in \mathbb{K}[x]$ vom Grad > 0. Dann ist $deg(f_1) < deg(f)$ und $deg(g_1) < deg(g)$ mit

$$g_1 \cdot f - f_1 \cdot g = 0.$$

Die Behauptung folgt aus Satz 2.2.

$\Rightarrow$: Es sei $R_{f,g} = 0$, also

$$\varphi \cdot f + \psi \cdot g = 0, \quad deg(\psi) < deg(f), deg(\varphi) < deg(g).$$

Weil ψ einen kleineren Grad als f hat, können nicht alle irreduziblen Faktoren von f mit ihren Vielfachheiten in ψ auftreten. Mindestens einer muss Faktor von g sein. □

Lemma 2.1 *Es sei $c \in \mathbb{K}$.*

a) $R_{f,g}$ ändert sich nicht, wenn wir $f(x)$ durch $f(x+c)$ und $g(x)$ durch $g(x+c)$ ersetzen.

b) Es gilt

$$R_{f,\,(x-c)g} = f(c) \cdot R_{f,g}.$$

Beweis. a) Die Resultante ist die Koeffizientenmatrix der Polynome

$$f,\, xf, ..., x^{n-1}f,\, g,\, xg, ..., x^{m-1}g$$

in der Basis $1, x, ..., x^{m+n-1} \in V$. Wir setzen $y := x - c$ und gehen über zu der Basis

$$\begin{aligned} 1 &= 1 \\ y &= -c + x \\ y^2 &= c^2 + -2cx + x^2 \\ &\vdots \end{aligned}$$

Die Übergangsmatrix hat Dreiecksform mit Einträgen $= 1$ auf der Diagonale. Deswegen können wir die Resultante auch in dieser Basis ausrechnen. Dabei müssen wir $f(x) = f(y+c)$ und $g(x) = g(y+c)$ setzen. Die Resultante ist deswegen die Koeffizientendeterminante der Polynome

$$\begin{aligned} f(y+c) &= f(y+c) \\ (y+c)f(y+c) &= c \cdot f(y+c) + c \cdot f(y+c) \\ (y+c)^2 \cdot f(y+c) &= c^2 \cdot f(y+c) + 2cy \cdot f(y+c) + y^2 \cdot f(y+c) \\ &\vdots \end{aligned}$$

Nach elementaren Zeilenumformungen wird dies die Resultante der Polynome $f(y+c)$ und $g(y+c)$ in $\mathbb{K}(y)$.

b) Wir berechnen zunächst

$$R_{f,xg} = det \begin{pmatrix} a_m & a_{m-1} & ... & a_0 & & & \\ & a_m & a_{m-1} & ... & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & b_n & b_{n-1} & ... & b_0 & & \\ & & b_n & b_{n-1} & ... & b_0 & \\ & & & \ddots & \ddots & & \ddots \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} n+1 \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} m \end{matrix} = a_m \cdot R_{f,g} = f(0) \cdot R_{f,g}.$$

Mit a) finden wir

$$R_{f(x),(x-c)g(x)} = R_{f(x+c),xg(x+c)} = f(c) R_{f(x+c),g(x+c)} = f(c) \cdot R_{f,g}.$$ □

Satz 2.4 (Korollar) *Es sei $\mathbb{K} = \mathbb{C}$.*

a) Ist

$$f = (x - a_1) \cdot ... \cdot (x - a_m), \quad g = (x - b_1) \cdot ... \cdot (x - b_n),$$

dann ist

$$R_{f,g} = \prod_{\mu,\nu}(b_\mu - a_\nu).$$

b) $R_{f,g_1 \cdot g_2} = R_{f,g_1} \cdot R_{f,g_2}$.

Beweis. a) Wir schreiben

$$g = (x - b_1) \cdot g_1 = (x - b_1)(x - b_2) \cdot g_2 = ...$$

Durch widerholte Anwendung von Satz 2.1 b) sehen wir

$$R_{f,g} = f(b_1) \cdot R_{f,g_1} = f(b_1)f(b_2) \cdot R_{f,g_2} = ... = f(b_1) \cdot ... \cdot f(b_n).$$

Dies ist die Behauptung.

b) Wir schreiben $g = c_1 \cdot (x - b_1) \cdot ... \cdot (x - b_r)$ und $g_2 = c_2 \cdot (x - b_{r+1}) \cdot ... \cdot (x - b_n)$. Aus der Determinantendarstellung folgt $R_{f,cg} = c^m \cdot R_{f,g}$. Damit wird

$$R_{f,g} = (c_1c_2)^m R_{f,(x-b_1)\cdot....\cdot(x-b_n)} = (c_1c_2)^m \prod f(b_\nu) = c_1^m \prod_{\nu=1}^{r} f(b_\nu) \cdot c_2^m \prod_{\nu=r+1}^{n} f(b_\nu) = R_{f,g_1} \cdot R_{f,g_2}.$$

□

2.2 Der Nullstellensatz

Wir wenden die Resultante auf Polynome $f, g \in \mathbb{C}[x, y]$ in zwei Veränderlichen an. Wie früher verwenden wir $\mathbb{K} = \mathbb{C}(x)$ und fassen

$$f = \sum_\mu f_\mu(x) \cdot y^\mu, \quad g = \sum_\nu g_\nu(x) \cdot y^\nu$$

als Elemente in

$$\mathbb{K}[y] = \mathbb{C}(x)[y]$$

auf. Dann wird $R_{f,g} \in \mathbb{K}$ ein Körperelement, d.h., eine rationale Funktion in x. Aus der Determinantenform sehen wir aber, dass in Wirklichkeit $R_{f,g} \in \mathbb{C}[x]$ ein Polynom in x ist. Satz 2.3 bedeutet nun: $R_{f,g}$ ist das Nullpolynom genau dann, wenn f und g einen gemeinsamen Teiler $p \in \mathbb{K}[y]$ haben. Hier ist $p(x, y)$ ein Polynom in y von einem Grad > 0. Die Koeffizienten sind allerdings rationale Funktionen in x. Wir bilden den Hauptnenner $n(x)$ aller dieser Funktionen und schreiben

$$p(x, y) = \frac{1}{n(x)} \cdot q(x, y),$$

wo $q(x, y) \in \mathbb{C}[x, y]$ ein Polynom ist, das in y denselben Grad wie p hat.

Aus $R_{f,g} = 0$ folgt also, dass $n(x) \cdot f$ und $n(x) \cdot g$ den gemeinsamen Teiler $q(x, y)$ besitzen. O.B.d.A. können wir hier $q \in \mathbb{C}[x, y]$ irreduzibel annehmen. Weil q echt von y abhängt, kann $q(x, y)$ das Polynom $n(x)$ nicht teilen. Aus Satz 1.12 folgt somit, dass q ein gemeinsamer Teiler von f und g in $\mathbb{C}[x, y]$ ist. Dieses Ergebnis halten wir fest:

Satz 2.5 *Für $f, g \in \mathbb{C}[x,y]$ werde $R_{f,g} \in \mathbb{C}(x)$ vermöge $\mathbb{C}[x,y] \subset \mathbb{K}[y]$ mit $\mathbb{K} = \mathbb{C}[x]$ berechnet. Dann gilt: $R_{f,g} = 0$ genau dann, wenn f und g als Elemente in $\mathbb{C}[x,y]$ einen gemeinsamen Teiler besitzen.*

Damit beweisen wir jetzt den Nullstellensatz.

Sei also $C \subset \mathbb{C}^2$ eine Kurve, Nullstellenmenge des irreduziblen Polynoms $p[x,y] \in \mathbb{C}[x,y]$. Wir betrachten ein Polynom $f(x,y) \in \mathbb{C}[x,y]$ mit $f(\mathbf{x}) = 0$ für alle $\mathbf{x} \in C$. Wenn p von y unabhängig ist, also ein Polynom in x, dann muss es linear sein und C eine Gerade. Dafür wurde in Satz 1.4 a) gezeigt, dass f durch p teilbar ist. Wir können also o.B.d.A. annehmen

$$p(x,y) = \sum_{\nu=0}^{n} p_\nu(x) y^\nu$$

mit $n > 0$ und p_n nicht das Null-Polynom. Dieses Polynom $p_n(x)$ hat nur endlich viele Nullstellen $x_1, ..., x_k$. Für jedes $x_0 \neq x_1, ..., x_k$ ist $p(x_0, y)$ ein Polynom in y vom Grad n.

Insbesondere hat $p(x_0, y)$ Nullstellen. Wir fixieren y_0, eine dieser Nullstellen. Dann ist $\mathbf{x} := (x_0, y_0)$ ein Punkt aus C. Nach Voraussetzung gilt also $f(x_0, y_0) = 0$. Somit haben die Polynome $p(x_0, y)$ und $f(x_0, y)$ die gemeinsame Nullstelle y_0. Beide Polynome haben einen Linearfaktor gemeinsam, deswegen ist

$$R_{f(x_0,y),p(x_0,y)} = 0.$$

Setzt man x_0 in die Determinantendarstellung für $R_{f,p}$ ein, so findet man

$$R_{f,p}(x_0) = R_{f(x_0,y),p(x_0,y)} = 0.$$

Das Polynom $R_{f,p} \in \mathbb{C}[x]$ verschwindet in allen Punkten $x \neq x_1, ..., x_k$. Dann muss es identisch $= 0$ sein. Nach der obigen Diskussion müssen also f und p einen gemeinsamen Faktor besitzen. Weil p irreduzibel ist, kann dies nur p selbst sein. Damit ist der Nullstellensatz bewiesen.

Nach Definition einer affinen algebraischen Kurve ist jedem Polynom $p(x,y)$ eindeutig die Kurve $C = \{(x,y) : p(x,y) = 0\}$ zugeordnet. A priori ist nicht klar, dass jede Kurve von einem eindeutig bestimmten Polynom p herkommt. Weil p und p^2 dieselbe Kurve (als Punktmenge) bestimmen, ist dies sogar falsch. Aber mit dem Nullstellensatz und etwas Vorsicht können wir schon soetwas wie ein durch die Kurve eindeutig bestimmtes Polynom definieren.

Satz 2.6 *Es sei $C \subset \mathbb{C}^2$ eine algebraische Kurve. Dann ist das Polynom $p \neq 0$ kleinsten Grades, welches in allen Punkten von C verschwindet (bis auf konstante Faktoren) eindeutig bestimmt.*

Beweis. Es werde zunächst der Spezialfall betrachtet, dass C irreduzible ist. Sei p ein irreduzibles Polynom, welches die Kurve C definiert. Ist f irgend ein Polynom, das auf C verschwindet, so ist nach dem Nullstellensatz $f = p \cdot q$ mit einem weiteren Polynom q. Deswegen ist $deg(f) = deg(p) + deg(q) > deg(p)$, außer, wenn $deg(q) = 0$ und $q = c$ eine Konstante ist. Ist $f \neq 0$, so muss c eine Konstante $\neq 0$ sein, und $f = c \cdot p$.

Sei nun allgemein $C = \cup C_i$ mit irreduziblen Kurven C_i, die durch irreduzible Polynome p_i definiert sind. Jedes Polynom $f \neq 0$, das auf C verschwindet, muss durch alle p_i teilbar sein. Wegen der Eindeutigkeit der Zerlegung von f in irreduzible Faktoren ist dann f durch $\prod p_i$ teilbar. Hat f minimalen Grad, so stimmt es bis auf konstante Faktoren mit $\prod p_i$ überein. □

Bemerkung 1: Passt man etwas auf und berücksichtigt die Sonderrolle der unendlich-fernen Gerade $x_0 = 0$, so gilt Satz 2.6 wörtlich genauso für projektive Kurven und homogene Polynome in x_0, x_1, x_2.

Bemerkung 2: In Satz 2.6 wird C als reine Punktmenge aufgefasst. Manchmal muss man aber auch Vielfachheiten k_i der Faktoren p_i und der irreduziblen Komponenten C_i berücksichtigen. Man schreibt dann

$$C = \sum_i k_i C_i$$

und nennt soetwas einen *Divisor* oder *Zyklus*. Das Polynom kleinsten Grades, welches diesen Divisor definiert ist dann bis auf konstante Faktoren das Produkt $\prod p_i^{k_i}$.

Definition 2.2 *Der Grad $deg(C)$ einer algebraischen Kurve ist der kleinste Grad eines Polynoms, das C definiert. Da dieses Polynom bis auf konstante Faktoren eindeutig festgelegt ist, ist diese Definition sinnvoll.*

Kurven kleinen Grades haben besondere Namen:

Grad	Name	Grad	Name
1	Gerade	5	Quintik
2	Kegelschnitt	6	Sextik
3	Kubik	7	Septik
4	Quadrik	8	Oktik

2.3 Der Satz von Bezout

Jetzt müssen wir die Resultante $R_{f,g}$ auch für homogene Polynome $f, g \in \mathbb{C}[x_0, x_1, x_2]$ definieren. Dazu schreiben wir

$$f = \sum_{\mu=0}^{m} f_\mu(x_0, x_1) x_2^{m-\mu}$$

mit Koeffizienten $f_\mu \in \mathbb{C}[x_0, x_1]$ homogen vom Grad μ (und analog für g). Den Ring $\mathbb{C}[x_0, x_1]$ fassen wir auf als Unterring des Körpers $\mathbb{C}(x_0, x_1)^h$ der rationalen Funktionen z/n, wo Zähler und Nenner homogen in x_0, x_1 sind. Dann ist also

$$R_{f,g} \in \mathbb{C}(x_0, x_1)^h$$

eine solche rationale Funktion. Aber aus der Determinentendarstellung folgt, dass $R_{f,g}$ sogar ein Polynom ist. Aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren im Ring $\mathbb{C}[x_0, x_1, x_2]^h$ der homogenen Polynome folgt genau wie in Satz 2.5: $R_{f,g} = 0$ genau dann, wenn f und g ein homogenes Polynom als gemeinsamen Faktor haben.

Satz 2.7 *Es seien $f, g \in \mathbb{C}[x_0, x_1, x_2]$ homogen vom Grad m bzw. n. Dann ist entweder $R_{f,g} = 0$, d.h., f und g haben einen gemeinsamen homogenen Faktor, oder $R_{f,g}$ ist eine homogenes Polynom in x_0, x_1 vom Grad $m \cdot n$.*

Beweis. Für die Koeffizienten f_μ von F gilt

$$f_\mu(tx_0, tx_1) = t^\mu f(x_0, x_1), \quad t \in \mathbb{C}.$$

In die Determinante, welche $R_{f,g}$ definiert, schreiben wir statt der Koeffizienten von f und g nur die Potenz von t, welche man aus $f(tx_0, tx_1)$ rausziehen kann, und versuchen zu verfolgen, welche Potenz von t man aus $R_{f,g}$ rausziehen kann. In der Matrix sind dies die Potenzen

$$\begin{pmatrix} t^m & t^{m-1} & & & t & 1 & & \\ & t^m & t^{m-1} & & & t & 1 & \\ & & \ddots & \ddots & & & \ddots & \ddots \\ t^n & t^{n-1} & & & t & 1 & & \\ & t^n & t^{n-1} & & & t & 1 & \\ & & \ddots & \ddots & & & \ddots & \ddots \end{pmatrix}.$$

Der resultierenden Determinante sieht man nichts an. Aber jetzt multiplizieren wir die erste Zeile mit t^n, die zweite mit $^{n-1}$,..., die n-te mit t, sowie die $m+1$-ste mit t^m, die $m+2$-te mit t^{m-1}, die letzte mit t. Auf geradezu wunderbare Weise enthält die neue erste Spalte nur die Potenz t^{m+n}, die zweite Spalte nur die Potenz t^{m+n-1}, ..., die letzte ($= m+n$-te) Spalte nur die Potenz t. Die neue Determinante ist also homogen in t vom Grad

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

Durch die Zeilenmultiplikationen hat sich allerdings der Homogenitätsgrad der ursprünglichen Determinante um

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

erhöht. Deswegen war die ursprüngliche Determinante homogen vom Grad

$$\frac{1}{2}((m+n)^2 + (m+n) - (m^2 + m + n^2 + n)) = m \cdot n.$$

□

Satz 2.8 (von Bezout) *Es seien $C, D \subset \mathbb{P}_2(\mathbb{C})$ zwei algebraische Kurven vom Grad c, bzw. d. Wir setzen voraus, dass C und D keine gemeinsame Komponente haben. Dann gilt:*

- *$C \cap D$ ist nicht leer;*
- *$C \cap D$ enthält höchstens $c \cdot d$ Punkte;*
- *jedem Punkt $\mathbf{x} \in C \cap D$ kann man eine Schnitt-Vielfachheit $i_\mathbf{x}(C, D)$ zuordnen derart, dass*

$$\sum_{\mathbf{x} \in C \cap D} i_\mathbf{x}(C, D) = c \cdot d.$$

Beweis. $C \cup D$ ist eine algebraische Kurve, definiert durch ein Polynom p, das nicht das Nullpolynom ist. Daraus folgt $C \cup D \neq \mathbb{P}_2$. Es gibt also Punkte in $\mathbb{P}_2$, die nicht auf $C \cup D$ liegen. Wir wählen das Koordinatensystem so, dass $(0:0:1) \notin C \cup D$ einer dieser Punkte ist.

Es seien $f = 0$ bzw. $g = 0$ Gleichungen für C bzw. D mit homogenen Polynomen $f, g \in \mathbb{C}[x_0, x_1, x_2]$. Vermöge

$$\mathbb{C}[x_0, x_1, x_2] \subset \mathbb{C}(x_0, x_1)[x_2]$$

berechnen wir $R_{f,g} \in \mathbb{C}[x_0, x_1]$. Da C und D keine gemeinsame Komponente haben, ist $R_{f,g}$ nicht das Null-Polynom. Nach Satz 2.7 ist diese Resultante homogen vom Grad $c \cdot d > 0$. Insbesondere besitzt $R_{f,g}$ Nullstellen. Für jeden Punkt $(a_0 : a_1) \in \mathbb{P}_1$ betrachten wir die Gerade $(x_0 : x_1) = (a_0 : a_1)$ durch $(a_0 : a_1 : 0)$ und $(0 : 0 : 1)$. Die Resultante $R_{f,g}$ hat die Nullstelle $(a_0 : a_1)$ genau dann, wenn C und D einen Schnittpunkt auf dieser Gerade haben. Daraus folgt schon einmal, dass $C \cap D$ nicht leer ist.

Wenn unendlich viele Schnittpunkte auf der Geraden liegen würden, dann müssten f und g auf der Geraden identisch verschwinden. Weil sie aber beide in dem Punkt $(0 : 0 : 1)$ auf dieser Geraden nicht verschwinden, kann das nicht der Fall sein. Jeder Schnittpunkt von C und D liegt also auf einer Geraden durch $(0 : 0 : 1)$, die zu einer (der endlich vielen) Nullstellen von $R_{f,g}$ gehört. Und auf jeder dieser Geraden gibt es nur endlich viele Schnittpunkte. Dann gibt es auch insgesamt nur endlich viele Schnittpunkte von C und D.

Jetzt fangen wir den Beweis nochmal von vorne an. Und zwar wählen wir $(0 : 0 : 1)$ zusätzlich so, dass dieser Punkt auf keiner der endlich vielen Geraden liegt, welche zwei verschiedene Schnittpunkte aus $C \cap D$ verbinden. Auf jeder Geraden durch $(0 : 0 : 1)$ liegt also höchstens ein einziger Schnittpunkt. Zu jeder Nullstelle $(a_0 : a_1)$ von $R_{f,g}$ gehört dann genau ein Schnittpunkt $\mathbf{x}$ von C und D. Nach Satz 2.7 ist $R_{f,g}$ homogen vom Grad $c \cdot d$. Es gibt also - mit Vielfachheit gerechnet - genau $m \cdot n$ Nullstellen $(a_0 : a_1)$. Wir definieren die Schnitt-Vielfachheit $i_{\mathbf{x}}(C, D)$ als die Vielfachheit der entsprechenden Nullstelle von $R_{f,g}$. Damit haben wir dann

$$\sum_{\mathbf{x} \in C \cap D} i_{\mathbf{x}}(C, D) = deg(R_{f,g}) = m \cdot n.$$

□

Dieser Satz von Bezout von Bezout ist wunderschön. Er verallgemeinert die bekannten Tatsachen, dass sich zwei Geraden in einem Punkt schneiden, eine Gerade und ein Kegelschnitt - mit Vielfachheit gerechnet - in zwei Punkten, zwei Kegelschnitte - mit Vielfachheit gerechnet - in vier Punkten. Aber der Satz ist nicht nur schön. Er ist das ganz zentrale Werkzeug in der Theorie der ebenen Kurven. Am häufigsten wird er in der folgenden Form angewendet:

Satz 2.9 *Es seien C und D Kurven vom Grad c und d. Wenn C und D mehr als $c \cdot d$ Schnittpunkte haben, dann haben sie eine gemeinsame Komponente.*

Das Unschöne an der hier gegebenen Formulierung des Satzes von Bezout ist allerdings die Definition der Schnitt-Vielfachheit $i_{\mathbf{x}}(C, D)$. Sie ist nicht unabhängig vom gewählten Koordinatensystem. Außerdem ist sie für praktische Berechnungen sehr unhandlich. Wir wollen erst einmal einige formale Eigenschaften festhalten:

Satz 2.10 *a) Die Schnittvielfachheit $i_{\mathbf{x}}(C, d)$ ist symmetrisch in C und D.*

b) Ist $D = D_1 \cup D_2$ Vereinigung zweier Kurven und $\mathbf{x} \in C \cap D_1 \cap D_2$, dann gilt

$$i_{\mathbf{x}}(C, D_1 \cup D_2) = i_{\mathbf{x}}(C, D_1) + i_{\mathbf{x}}(C, D_2).$$

c) Ist $D = L$ eine Gerade, so ist $i_{\mathbf{x}}(C, L)$ die Schnittvielfachheit aus Definition 1.5, nämlich die Verschwingungsordnung des Polynoms $f|L$ in $\mathbf{x}$.

d) Ist $\mathbf{x}$ singulär auf einer der beiden Kurven C, D, so ist

$$i_{\mathbf{x}}(C, D) > 1.$$

e) Genau dann ist $i_{\mathbf{x}}(C, D) = 1$, wenn beide Kurven in $\mathbf{x}$ glatt sind und dort verschiedene Tangenten haben.

Beweis. a) Die Determinanten-Darstellung zeigt, dass sich die Resultanten $R_{f,g}$ und $R_{g,f}$ höchstens um das Vorzeichen unterscheiden. Beide Resultanten haben deswegen identische Nullstellenordnungen.

b) Es seien $g_1 = 0$ und $g_2 = 0$ Gleichungen für D_1 und D_2. Die Behauptung folgt, wenn wir

$$R_f, g_1 \cdot g_2 = F_{f,g_1} \cdot F_{f,g_2}$$

zeigen können. Aber für alle $(a_0 : a_1)$ folgt aus Satz 2.4 b)

$$R_{f,g_1 \cdot g_2}(a_0, a_1) = R_{f,g_1}(a_0, a_1) \cdot R_{f,g_1}(a_0, a_1).$$

Das ist genau das, was wir brauchen.

c) Wir wählen die Koordinaten so, dass $L : x_2 = 0$. (Hier stört natürlich, dass die Schnitt-Vielfachheit möglicherweise vom Koordinatensystem abhängt.) Wir schreiben das Polynom f, welches C definiert als

$$f(x_0, x_1, x_2) = a_c(x_0, x_1) + a_{c-1}(x_0, x_1)x_2 + ... + a_0 x_2^c$$

mit $a_i(x_0, x_1)$ homogen vom Grad i. Nach Definition ist

$$R_{f,g} = det \begin{pmatrix} a_c & a_{c-1} & ... & a_1 & a_0 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix} = a_c(x_0, x_1) = f|L.$$

Die Nullstellenordnung der Resultante ist genau die Nullstellenordnung von $f|L$.

d) Wir wählen die Koordinaten so, dass $\mathbf{x} = (1 : 0 : 0)$ und nehmen an, dass $\mathbf{x} \in C$ singulär ist. Wir schreiben wieder

$$\begin{aligned} f(x_0, x_1, x_2) &= a_c(x_0, x_1) + a_{c-1}(x_0, x_1) \cdot x_2 + ... + a_0 \cdot x_2^c, \\ g(x_0, x_1, x_2) &= b_d(x_0, x_1) + b_{d-1}(x_0, x_1) \cdot x_2 + ... + b_0 \cdot x_2^d. \end{aligned}$$

Wir haben die Bedingungen

$$\begin{aligned} f(1,0,0) = a_c(1,0) = 0 \quad &\Rightarrow \quad a_c(x_0,x_1) = x_1 \cdot a_c'(x_0,x_1), \\ \frac{\partial f}{\partial x_1}(1,0,0) = a_c'(1,0) + x_1 \frac{\partial a_c'}{\partial x_1}\Big|_{x_1=0} = 0 \quad &\Rightarrow \quad a_c(x_0,x_1) = x_1^2 \cdot a_c''(x_0,x_1), \\ \frac{\partial f}{\partial x_2}(1,0,0) = a_{c-1}(1,0) = 0 \quad &\Rightarrow \quad a_{c-1}(x_0,x_1) = x_1 \cdot a_{c-1}'(x_0,x_1), \\ g(1,0,0) = b_d(1,0) = 0 \quad &\Rightarrow \quad b_d(x_0,x_1) = x_1 \cdot b_d'(x_0,x_1). \end{aligned}$$

Die Determinante für die Resultante $R_{f,g}$ hat die beiden ersten Spalten

$$\begin{pmatrix} x_1^2 a_c'' & x_1 a_{c-1}' & \dots \\ & x_1^2 a_c'' & \\ & & \ddots \\ x_1 b_d' & b_{d-1} & \dots \\ & x_1 b_d' & \\ & & \ddots \end{pmatrix}.$$

Entwickelt man die Determinante nach der ersten Zeile, so ist das Ergebnis durch x_1^2 teilbar.

e) Wenn $i_{\mathbf{x}}(C,D) = 1$ ist, so folgt aus d) dass beide Kurven in $\mathbf{x}$ glatt sind. Wir wählen wieder $\mathbf{x} = (1:0:0)$ und nehmen an, dass beide Kurven hier glatt sind. Zusätzlich zu allen anderen Voraussetzungen an den Punkt $(0:0:1)$ wählen wir ihn so, dass er auf keiner der beiden Tangenten $T_{\mathbf{x}}(C), T_{\mathbf{x}}(D)$ liegt. Dann ist keine der beiden Tangenten die Gerade $x_1 = 0$ durch $\mathbf{x}$. Das impliziert

$$\frac{\partial f}{\partial x_2}(1,0,0) \neq 0, \quad \frac{\partial g}{\partial x_2}(1,0,0) \neq 0.$$

Jetzt brauchen wir den Satz über implizite Funktionen um lokal bei $\mathbf{x}$ aufzulösen

$$f(1,x_1,x_2) = 0 \Leftrightarrow x_2 = u(x_1), \quad g(1,x_1,x_2) = 0 \Leftrightarrow x_2 = v(x_1).$$

Das ist nicht ganz unproblematisch, weil man es hier mit komplexen Funktionen zu tun hat. Aber wenn man den normalen reellen Satz über implizite Funktionen in vier reellen Veränderlichen und die Cauchy-Riemann-Differentialgleichungen aus der Funktionentheorie benutzt, sieht man, dass es tatsächlich solche holomorphen Funktionen u und v gibt. Wir schreiben die Resultante in der Produktform (Satz 2.4)

$$R_{f,g}(x_1) = \prod (u_\mu(x_1) - v_\nu(x_1)).$$

Dabei sind Zahlen $u_\mu(x_1)$ die x_2-Koordinaten der Punkte in $C \cap \{x_1 = const\}$ und v_ν die x_2-Koordinaten der Punkte in $D \cap \{x_1 = const\}$. Wie man die präzise zu wählen hat, das ist auch wieder so eine Sache. Aber wir wissen, dass $u_1(x_1) = u(x_1)$ und $v_1(x_1) = v(x_1)$ genommen werden können. Deswegen ist

$$R_{f,g}(x_1) = (u(x_1) - v(x_1)) \cdot r(x_1)$$

mit einem Rest $r(x_1)$, der in $x_1 = 0$ nicht verschwindet. Also ist die Verschwindungsordnung von $R_{f,g}(x_1)$ gerade die Verschwindungsordnung der Funktion $u(x_1) - v(x_1)$.

Nun ist

$$f(x_1, u(x_1)) \equiv 0,$$

und deswegen

$$\partial_1 f + \partial_2 f \cdot \frac{du}{dx_1} = 0.$$

Das bedeutet, der Vektor $(1, du/dx_1)(0)$ steht senkrecht auf dem Gradienten $(\partial_1 f, \partial_2 f)(0,0)$, der Vektor ist also ein Richtungsvektor für die Tangente $T_{\mathbf{x}}(C)$. Genauso ist $(1, dv/dx_1)(0)$ ein Richtungsvektor für $T_{\mathbf{x}}(D)$. Beide Tangenten sind genau dann voneinander verschieden, wenn

$$\frac{du}{dx_1}(0) \neq \frac{dv}{dx_1}(0), \quad \text{bzw.} \quad \frac{d}{dx_1}(u - v)(0) \neq 0.$$

Das bedeutet aber, dass $u - v$ und damit $R_{f,g}$ in $x_1 = 0$ nur von erster Ordnung verschwindet. □

Als erste, und zugleich typische Anwendung des Satzes von Bezout beweisen wir:

Satz 2.11 *Eine irreduzible Kurve $D \subset \mathbb{P}_2$ vom Grad d hat höchstens*

$$\frac{1}{2}(d-1)(d-2)$$

Singularitäten.

Für niedrigen Grad ist z.B.

d	1	2	3	4	5	6
$(d-1)(d-2)/2$	0	0	1	3	6	10

Beweis des Satzes. Für $d = 1$ (Geraden) oder $d = 2$ (Kegelschnitte) kennen wir die Aussage aus der elementaren Geometrie. Sei also $d \geq 3$. Wir nehmen an, die Kurve D habe mindestens

$$\frac{1}{2}(d-1)(d-2) + 1$$

Singularitäten. Auf D wählen wir noch $d-3$ voneinander verschiedene weitere Punkte beliebig. Insgesamt sind dies

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

Punkte auf D.

Jetzt benutzen wir, dass die homogenen Polynome in x_0, x_1, x_2 vom Grad m einen $\mathbb{C}$-Vektorraum der Dimension

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

bilden. Insbesondere für $m = d - 2$ ist diese Dimension $= d(d-1)/2$. Wegen

$$d(d-1) = d^2 - d > d^2 - d - 2 = (d+1)(d-2)$$

ist die Dimension größer als die Anzahl unserer Punkte.

Dass ein homogenes Polynom in einem Punkt verschwindet, ist eine lineare Gleichung an die Koeffizienten von f. Dass f in allen unseren Punkten verschwindet, sind $(d+1)(d-2)$ lineare Gleichungen für die Koeffizienten von f. Wegen der Dimensionsformel für den Lösungsraum eines linearen Gleichungssystems gibt es ein nicht-triviales Polynom f vom Grad $d-2$, welches in allen unseren Punkten verschwindet. Sei C die Kurve mit der Gleichung $f = 0$. Weil die Schnittzahlen von C und D in den singulären Punkten von D mindestens $= 2$ sind (Satz 2.10 d), ist die Summe aller Schnittzahlen

$$\begin{aligned}
\sum_{\mathbf{x} \in C \cap D} i_{\mathbf{x}}(C, D) &\geq 2 \cdot (\frac{1}{2}(d-1)(d-2) + 1) + d - 3 \\
&= (d-1)(d-2) + (d-1) \\
&= (d-1)^2 \\
&= d^2 - 2d + 1 \\
&> d(d-2).
\end{aligned}$$

Dies widerspräche dem Satz von Besout, wenn nicht C und D eine gemeinsame Komponente besitzen. Weil D irreduzibel vorausgesetzt ist, könnte diese Komponente nur D sein. Weil aber C einen kleineren Grad als D hat, kann C die Kurve D nicht als Komponente enthalten. □

2.4 Polare und Hessesche

Sei $C \subset \mathbb{P}_2$ die algebraische Kurve mit der Gleichung $f = 0$. Die Tangente von C in einem glatten Punkt $\mathbf{p} \in C$ hat die Gleichung

$$\frac{\partial f}{\partial x_0}(\mathbf{p}) \cdot x_0 + \frac{\partial f}{\partial x_1}(\mathbf{p}) \cdot x_1 + \frac{\partial f}{\partial x_2}(\mathbf{p}) \cdot x_2 = 0.$$

Ein Punkt $\mathbf{q} \in \mathbb{P}_2$ liegt also auf der Tangente in $\mathbf{p}$ genau dann, wenn

$$\frac{\partial f}{\partial x_0}(\mathbf{p}) \cdot q_0 + \frac{\partial f}{\partial x_1}(\mathbf{p}) \cdot q_1 + \frac{\partial f}{\partial x_2}(\mathbf{p}) \cdot q_2 = 0.$$

Hier können wir $\mathbf{q}$ fixieren, und die Gleichung auffassen als Gleichung in $\mathbf{p}$. Sie hat dann den Grad $deg(C) - 1$. Und ein glatter Punkt $\mathbf{p} \in C$ ist genau dann Berührpunkt einer Tangente durch $\mathbf{q}$, wenn die Gleichung erfüllt ist.

Definition 2.3 *Die Kurve $P_{\mathbf{q}}(C)$ mit der Gleichung*

$$\frac{\partial f}{\partial x_0}(\mathbf{x}) \cdot q_0 + \frac{\partial f}{\partial x_1}(\mathbf{x}) \cdot q_1 + \frac{\partial f}{\partial x_2}(\mathbf{x}) \cdot q_2 = 0$$

vom Grad $deg(C) - 1$ heißt die Polare *von C bezüglich $\mathbf{q}$.*

Beispiel: Sei C der Kegelschnitt mit der Gleichung $f(\mathbf{x}) := \mathbf{x}^t \cdot A \cdot \mathbf{x} = 0$ in Matrixform. Dann ist

$$\frac{\partial f}{\partial x_i} = 2\sum_{j=0}^{2} a_{i,j}x_j.$$

Die Polare hat die Gleichung

$$\sum_{i,j=0}^{2} a_{i,j}x_j q_i = 0$$

und ist genau die Polare aus der projektiven Geometrie.

Beispiel: Die Neilsche Parabel mit der homogenen Gleichung

$$x_0x_2^2 - x_1^3 = 0$$

hat die Polare

$$P_{\mathbf{q}}(C):\ q_0 \cdot x_2^2 - q_1 \cdot 3x_1^2 + q_2 \cdot 2x_0x_2 = 0.$$

Satz 2.12 (Eigenschaften der Polare) *a) Die Polare $P_{\mathbf{q}}(C)$ ist eine projektive Kovariante, d.h., für jede projektive Transformation $\Phi : \mathbb{P}_2 \to \mathbb{P}_2$ gilt*

$$P_{\Phi(\mathbf{q})}\Phi(C) = \Phi(P_{\mathbf{q}}(C)).$$

b) Die Polare ist immer wohldefiniert (d.h., ihr definierendes Polynom ist nicht das Null-Polynom), außer wenn C Vereinigung von Geraden durch $\mathbf{q}$ ist.

c) Wenn C keine mehrfachen Komponenten besitzt, dann kann eine gemeinsame Komponente von C und $P_{\mathbf{q}}(C)$ nur eine Gerade durch $\mathbf{q}$ sein.

d) Die Polare $P_{\mathbf{q}}(C)$ geht durch alle Singularitäten von C.

Beweis. a) Die Kurven, mit denen wir es zu tun haben, werden durch die folgenden Gleichungen beschrieben:

$$\begin{aligned}
P_{\mathbf{q}}(C): &\quad \sum_i q_i \frac{\partial f}{\partial x_i}(\mathbf{x}) = 0,\\
\Phi(C): &\quad f(\Phi^{-1}(\mathbf{x})) = 0,\\
P_{\Phi(\mathbf{q})}(\Phi(C)): &\quad \sum_i \Phi(\mathbf{q})_i \frac{\partial (f\circ\Phi^{-1})}{\partial x_i}(\mathbf{x}) =\\
&\quad \sum_{i,j,k} \frac{\partial f}{\partial x_k}(\Phi^{-1}(\mathbf{x}))\cdot(\Phi^{-1})_{k,i}\cdot(\Phi)_{i,j}q_j =\\
&\quad \sum_k \frac{\partial f}{\partial x_k}(\Phi^{-1}(\mathbf{x}))\cdot q_j = 0,\\
\Phi(P_{\mathbf{q}}(C)): &\quad \sum_i q_i \frac{\partial f}{\partial x_i}(\Phi^{-1}(\mathbf{x})) = 0.
\end{aligned}$$

b) O.B.d.A. betrachten wir $\mathbf{q} = (1:0:0)$. Die Ableitung

$$\frac{\partial f}{\partial x_0}(\mathbf{x})$$

verschwindet identisch genau dann, wenn $f = f(x_1, x_2)$ nicht von x_0 abhängt. Dann beschreibt $f = 0$ aber eine Menge von Geraden durch $\mathbf{q}$.

c) Es sei $f = g \cdot h$ und $\{g = 0\}$ eine irreduzible Komponente von $P_{\mathbf{q}}(C)$. Nach dem Nullstellensatz dividiert g das Polynom

$$\sum_i q_i \frac{\partial f}{\partial x_i} = \left(\sum_i q_i \frac{\partial g}{\partial x_i} \right) \cdot h + g \cdot \left(\sum_i q_i \frac{\partial h}{\partial x_i} \right).$$

Weil C keine mehrfache Komponente besitzen soll, ist g kein Teiler von h. Das Polynom g muss das Polynom $\sum q_i \partial g / \partial x_i$ von einem Grad $< deg(g)$ teilen. Dann muss

$$\sum q_i \frac{\partial g}{\partial x_i} \equiv 0$$

das Nullpolynom sein. Wie eben sehen wir, dass $\{g = 0\}$ nur aus Geraden durch $\mathbf{q}$ besteht. Weil g irreduzibel war, ist die Kurve $\{g = 0\}$ eine Gerade durch $\mathbf{q}$.

d) Wenn $\mathbf{x} \in C$ singulär ist, dann gilt $(\partial f / \partial x_i)(\mathbf{x}) = 0$ für $i = 0, 1, 2$, und $\mathbf{x}$ gehört zur Polaren $P_{\mathbf{q}}(C)$ für alle Punkte $\mathbf{q}$. □

Definition 2.4 *Sei $\mathbf{p} \in C$ ein glatter Punkt. Die Tangente $T = T_{\mathbf{p}}(C)$ heißt* gewöhnliche *Tangente, wenn $i_{\mathbf{p}}(T, C) = 2$ ist. Der Punkt $\mathbf{p}$ heißt gewöhnlicher Berührpunkt seiner Tangente.*

Satz 2.13 (Polare) *Die Kurve $C \subset \mathbb{P}_2$ habe keine linearen oder mehrfachen Komponenten. Dann ist $P_{\mathbf{q}}(C)$ eine Kurve vom Grad $deg(C) - 1$, welche aus C genau die folgenden Punkte ausschneidet:*

- *die Singularitäten von D,*
- *die Berührpunkte von C mit den Tangenten an C aus $\mathbf{q}$.*

Ist $\mathbf{p} \in C$ ein ein gewöhnlicher Berührpunkt seiner Tangente, so gilt

$$i_{\mathbf{p}}(C, P_{\mathbf{q}}(C)) = 1.$$

Beweis. Nur die allerletzte Behauptung ist noch unbewiesen. Um sie zu beweisen, betrachten wir $C: f = 0$. Die Taylor-Entwicklung von $f|T$ in $\mathbf{p}$ ist

$$f(\mathbf{p} + t \cdot \mathbf{q}) = f(\mathbf{p}) + \sum_i \frac{\partial f}{\partial x_i}(\mathbf{p}) \cdot q_i \cdot t + \frac{1}{2} \sum_{i,j} \frac{\partial^2 f}{\partial x_i \partial x_j}(\mathbf{p}) \cdot q_i q_j \cdot t^2 + ...$$

Wegen $\mathbf{p} \in C$ ist hier $f(\mathbf{p}) = 0$. Weil $\mathbf{pq}$ die Tangente $T_{\mathbf{p}}(C)$ ist, verschwindet auch $\sum (\partial f / \partial x_i)(\mathbf{p}) \cdot q_i$. Wenn T eine gewöhnliche Tangente ist, muss also

$$\sum_{i,j} \frac{\partial^2 f}{\partial x_i \partial x_j}(\mathbf{p}) \cdot q_i q_j \neq 0$$

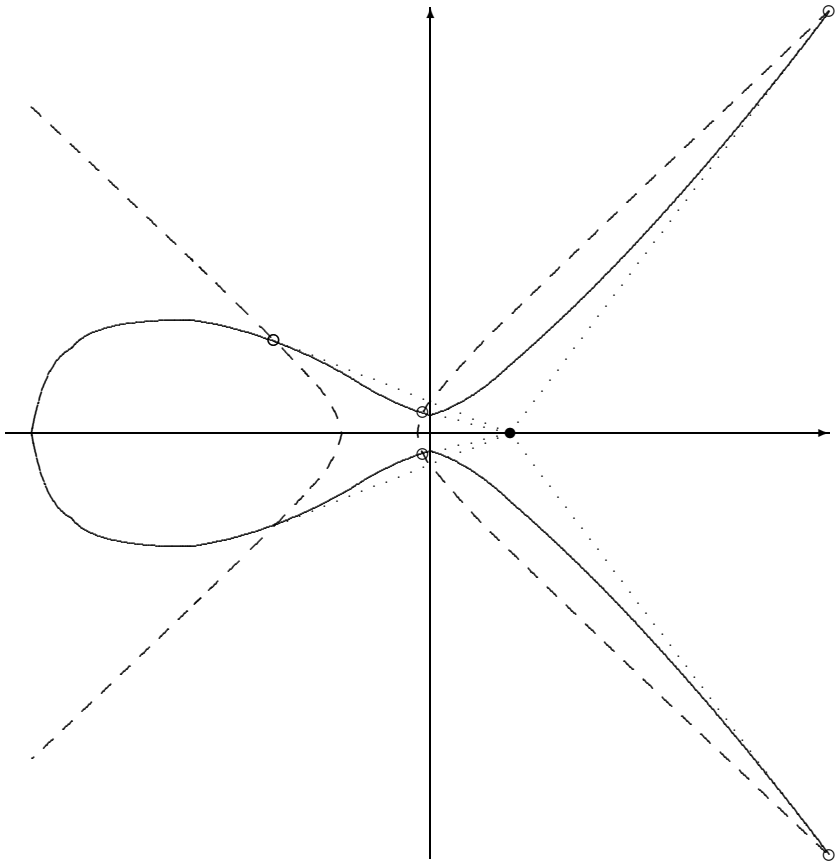
gelten. Die Polare

$$P_{\mathbf{q}}(C) : \sum_i \frac{\partial f}{\partial x_i}(\mathbf{x}) \cdot q_i = 0$$

hat in $\mathbf{p}$ die Tangente mit der Gleichung

$$\sum_{i,j} \frac{\partial^2 f}{\partial x_i \partial x_j}(\mathbf{p}) \cdot q_i \cdot x_j = 0.$$

Deswegen kann diese Tangente nicht durch $\mathbf{q}$ gehen. Die Kurve C und die Polare haben in $\mathbf{p}$ verschiedene Tangenten, und mit Satz 2.10 e) folgt die Behauptung. □



Definition 2.5 *Es sei $C \subset \mathbb{P}_2$ eine Kurve mit der Gleichung $f = 0$. Die Kurve H_C mit der Gleichung*

$$det\left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right) = 0$$

heißt die Hessekurve *oder einfach die* Hessesche *von C.*

Kurven von Grad ≤ 2 haben keine Hessesche. Die Hessesche einer Kurve C vom Grad ≥ 3 hat selbst den Grad $3 \cdot (deg(C) - 2)$, außer wenn die Determinante identisch verschwindet.

Beispiel: Wir betrachten eine Kubik in sogenannter *Hesse-Normalform*

$$f := x_0^3 + x_1^3 + x_2^3 + 6mx_0x_1x_2 = 0.$$

Man berechnet

$$\partial_{i,i} f = 6x_i, \quad \partial_{0,1} f = 6mx_2 \text{ usw.}$$

Damit wird die Hessesche

$$6^3 det \begin{pmatrix} x_0 & mx_2 & mx_1 \\ mx_2 & x_1 & mx_0 \\ mx_1 & mx_0 & x_2 \end{pmatrix} \sim (1+2m^2) \cdot x_0x_1x_2 - m^2 \cdot (x_0^3 + x_1^3 + x_2^3) \sim$$

$$\sim x_0^3 + x_1^3 + x_2^3 - \frac{1+2m^3}{m^2} \cdot x_0x_1x_2 = 0.$$

Falls $1 + 2m^3 \neq 0$, sind die Punkte in $C \cap H_C$ die Lösungen der Gleichungen

$$x_0^3 + x_1^3 + x_2^3 = x_0x_1x_2 = 0.$$

Es sind die neun Punkte $(0 : -1 : \omega^k), ...$ von denen nur drei reell sind.

Satz 2.14 (Eigenschaften der Hesseschen) *a) H_C ist eine projektive Kovariante, d.h., für jede Projektivität $\Phi : \mathbb{P}_2 \to \mathbb{P}_2$ gilt*

$$H_{\Phi(C)} = \Phi(H_C).$$

b) Wenn die Determinante nicht identisch verschwindet ist

$$deg(H_C) = 3 \cdot (deg(H) - 2).$$

c) H_C geht durch alle Singularitäten von C.

Beweis a) Wie üblich sei $f = 0$ die Gleichung von C. Die Gleichung von $\Phi(C)$ ist dann $f \circ \Phi^{-1} = 0$. Und

$$\begin{aligned} \partial_{i,j}(f \circ T^{-1})(\mathbf{x}) &= \partial_i \left(\sum_k (\partial_k f)(\Phi^{-1}(\mathbf{x}))\Phi^{-1}_{k,j} \right) \\ &= \sum_{k,l} (\partial_{k,l} f)(\Phi^{-1}(\mathbf{x}))(\Phi^{-1})_{k,j}(\Phi^{-1})_{l,i} \\ &= (\Phi^{-1})^t \cdot (\partial_{k,l} f)(\Phi^{-1}(\mathbf{x})) \cdot \Phi^{-1}. \end{aligned}$$

Deswegen hat $H_{\Phi(C)}$ die Gleichung

$$det(\Phi^{-1})^2 \cdot det((\partial_{k,l} f)(\Phi^{-1}(\mathbf{x})) = 0.$$

Bis auf eine Konstante ist das die Gleichung für $\Phi(H_C)$.

b) wurde gereits bewiesen.

c) Sei $\mathbf{a} = (a_0 : a_1 : a_2) \in C$ singulär. Mit der Eulerschen Formel sehen wir

$$((\partial_{i,j} f)(\mathbf{a})) \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = (deg(f) - 1) \cdot \begin{pmatrix} (\partial_0 f)(\mathbf{a}) \\ (\partial_1 f)(\mathbf{a}) \\ (\partial_2 f)(\mathbf{a}) \end{pmatrix} = 0.$$

Deswegen hat die Matrix $((\partial_{i,j} f)(\mathbf{a}))$ einen Rang ≤ 2 und ihre Determinante verschwindet. □

Definition 2.6 *Der glatte Punkt* $\mathbf{p} \in C$ *heißt* Wendepunkt*, wenn*

$$i_{\mathbf{p}}(C, T_{\mathbf{p}}(C)) \geq 3.$$

Der Punkt heißt gewöhnlicher *Wendepunkt, wenn diese Schnittzahl genau* $= 3$ *ist.*

Beispiel: Sei etwa $\mathbf{p} = \mathbf{0}$ der Ursprung auf der Kurve mit der affinen Gleichung $y = x^3$. Die Tangente T in diesem Punkt ist die x-Achse mit der Gleichung $y = 0$. Die Schnittzahl ist

$$i_{\mathbf{0}}(C, T) = \text{Nullstellenordnung}(x^3) = 3.$$

Der Nullpunkt ist ein gewöhnlicher Wendepunkt der Kurve. Auf der Kurve $y = x^4$ hat der Nullpunkt ebenfalls die Tangente $T : y = 0$. Aber jetzt ist

$$i_{\mathbf{0}}(C, T) = \text{Nullstellenordnung}(x^4) = 4.$$

Für diese Kurve ist der Nullpunkt kein gewöhnlicher Wendepunkt. Man nennt einen solchen Punkt einen *Flachpunkt* und die Tangente eine *Flachtangente*.

Satz 2.15 *Es sei* $\mathbf{p} \in C$ *ein glatter Punkt.*
a) $\mathbf{p}$ *ist genau dann Wendepunkt von* C*, wenn* $\mathbf{p} \in H_C$*.*
b) Wenn $\mathbf{p}$ *ein gewöhnlicher Wendepunkt ist, dann gilt*

$$i_{\mathbf{p}}(C, H_C) = 1.$$

Beweis. Es sei $d \geq 3$ der Grad von f. Wie früher schon kürze ich ab

$$f_i := \frac{\partial f}{\partial x_i}, \quad f_{i,j} := \frac{\partial^2 f}{\partial x_i \partial x_j}, \quad f_{i,j,k} := \frac{\partial^3 f}{\partial x_i \partial x_j \partial x_k}.$$

Für $\mathbf{q} \neq \mathbf{p}$ hat man die Taylorentwicklung bis zur dritten Ordnung

$$f(\mathbf{p} + t\mathbf{q}) = f(\mathbf{p}) + t \cdot \sum_i f_i(\mathbf{p}) q_i + \frac{t^2}{2} \cdot \sum_{i,j} f_{i,j}(\mathbf{p}) q_i q_j + \frac{t^3}{6} \cdot \sum_{i,j,k} f_{i,j,k}(\mathbf{p}) q_i q_j q_k.$$

Mit der Eulerschen Formel haben wir für $\mathbf{p} \in C$

$$d(d-1) \cdot f(\mathbf{p}) = (d-1) \cdot \sum_i f_i(\mathbf{p}) p_i = \sum_{i,j} f_{i,j}(\mathbf{p}) p_i p_j = 0.$$

Und $\mathbf{q}$ liegt genau dann auf der Tangente $T_{\mathbf{p}}(C)$, wenn

$$(d-1)\cdot\sum_j f_j(\mathbf{p})q_j = \sum_{i,j} f_{i,j}(\mathbf{p})p_iq_j = 0.$$

a) $\Rightarrow$: Die Tangente $Y_{\mathbf{p}}(C)$ werde aufgespannt von $\mathbf{p}$ und $\mathbf{q}$. Wenn $\mathbf{p}$ ein Wendepunkt ist, dann berührt die Tangente mit einer Ordnung ≥ 3 und aus der Taylor-Entwicklung folgt

$$\sum_{i,j} f_{i,j}(\mathbf{p})q_iq_j = 0.$$

Zusammen mit

$$\sum_{i,j} f_{i,j}(\mathbf{p})p_ip_j = \sum_{i,j} f_{i,j}(\mathbf{p})p_1q_j = 0$$

zeigt dies, dass die quadratische Form mit der Matrix $(f_{i,j}(\mathbf{p}))$ auf dem 2-dimensionalen Unterraum des $\mathbb{C}^3$ verschwindet, der durch $\mathbf{p}$ und $\mathbf{q}$ aufgespannt wird. Deswegen ist diese Form entartet, und ihre Determinante $det(f_{i,j}(\mathbf{p})) = 0$.

$\Leftarrow$: Jetzt ist die Form mit der Matrix $f_{i,j}(\mathbf{p})$ entartet. Deswegen gibt es ein $\mathbf{q} \neq \mathbf{0}$ mit

$$\sum_j f_{i,j}(\mathbf{p})q_j = 0 \quad \text{für} \quad i = 0,1,2.$$

Wäre $\mathbf{q} = \mathbf{p}$, so hätten wir für $i = 0,1,2$

$$(d-1)f_i(\mathbf{p}) = \sum_j f_{i,j}(\mathbf{p})p_j = 0.$$

Weil $\mathbf{p} \in C$ glatt ist, geht das nicht. Deswegen spannen $\mathbf{p}$ und $\mathbf{q}$ eine Gerade auf. Wegen

$$\sum_{i,j} f_{i,j}(\mathbf{p})q_j \cdot p_i = \sum_i 0 \cdot p_i$$

ist diese Gerade die Tangente $T_{\mathbf{p}}(C)$. Und wegen

$$\sum_{i,j} f_{i,j}(\mathbf{p})q_iq_j = 0$$

ist die Schnittzahl $i(C, T_{\mathbf{p}}(C)) \geq 3$.

b) Wie eben werde die Tangente $T_{\mathbf{p}}(C)$ aufgespannt von $\mathbf{p}$ und $\mathbf{q}$. Der Einfachheit halber wählen wir die Koordinaten so, dass

$$\mathbf{p} = (1:0:0), \quad \mathbf{q} = (0:1:0).$$

Mit den Rechnungen am Beginn des Beweises, und weil $\mathbf{p}$ ein Wendepunkt ist, folgt

$$f_{0,0}(\mathbf{p}) = f_{0,1}(\mathbf{p}) = f_{1,1}(\mathbf{p}) = 0.$$

Mit der Eulerschen Formel finden wir

$$f_{0,0,1}(\mathbf{p}) = \sum_{i,j,k} f_{i,j,k}(\mathbf{p})p_ip_jq_k = (d-2)\sum_{j,k} f_{j,k}(\mathbf{p})p_jq_k = (d-1)(d-2)\sum_k f_k(\mathbf{p})q_k = 0,$$

$$f_{0,1,1}(\mathbf{p}) \sum_{i,j,k} f_{i,j,k}(\mathbf{p}) p_i q_j q_k = (d-2) \sum_{j,k} f_{j,k}(\mathbf{p}) q_j q_k = 0.$$

Aber

$$f_{0,2}(\mathbf{p}) = \sum_i f_{i,2}(\mathbf{p}) p_i = (d-1) f_2(\mathbf{p}) \neq 0,$$

wei $f_2(\mathbf{p})$ der einzige Koeffizient $\neq 0$ in der Tangentengleichung ist, und

$$f_{1,1,1}(\mathbf{p}) = \sum_{i,j,k} f_{i,j,k}(\mathbf{p}) q_i q_j q_k \neq 0,$$

weil $\mathbf{p} \in C$ ein gewöhnlicher Wendepunkt ist. Jetzt entwickeln wir die Einschränkung $det(f_{i,j}(\mathbf{p}+ t \cdot \mathbf{q}))$ der Hesse-Determinante auf die Tangente bis zur ersten Ordnung

$$\begin{aligned}
det(f_{i,j}(\mathbf{p}+t\cdot\mathbf{q})) &= det\left((f_{i,j}(\mathbf{p})) + t\cdot(\sum_k f_{i,j,k}(\mathbf{p})q_k)\right) \\
&= det\left((f_{i,j}(\mathbf{p})) + t\cdot(f_{i,j,1}(\mathbf{p}))\right) \\
&= det\left(\begin{pmatrix} 0 & 0 & f_{0,2}(\mathbf{p}) \\ 0 & 0 & f_{1,2}(\mathbf{p}) \\ f_{0,2}(\mathbf{p}) & f_{1,2}(\mathbf{p}) & f_{2,2}(\mathbf{p}) \end{pmatrix} + t\cdot \begin{pmatrix} 0 & 0 & f_{0,2,1}(\mathbf{p}) \\ 0 & f_{1,1,1}(\mathbf{p}) & f_{1,2,1}(\mathbf{p}) \\ f_{0,2,1}(\mathbf{p}) & f_{1,2,1}(\mathbf{p}) & f_{2,2,1}(\mathbf{p}) \end{pmatrix}\right) \\
&= det\begin{pmatrix} 0 & 0 & f_{0,2}(\mathbf{p})+t\cdot f_{0,2,1}(\mathbf{p}) \\ 0 & t\cdot f_{1,1,1}(\mathbf{p}) & f_{1,2}(\mathbf{p})+t\cdot f_{1,2,1}(\mathbf{p}) \\ f_{0,2}(\mathbf{p})+t\cdot f_{0,2,1}(\mathbf{p}) & f_{1,2}(\mathbf{p})+t\cdot f_{1,2,1}(\mathbf{p}) & f_{2,2}(\mathbf{p})+t\cdot f_{2,2,1}(\mathbf{p}) \end{pmatrix} \\
&= t\cdot f_{0,2}(\mathbf{p})^2 \cdot f_{1,1,1}(\mathbf{p}) + ...
\end{aligned}$$

Also verschwindet die eingeschränkte hessesche Determinante auf $T_{\mathbf{p}}(C)$ nur von der ersten Ordnung und es ist tatsächlich $i_{\mathbf{p}}(C, H_C) = 1$. □

Beispiel: Die zweiten Ableitungen von

$$f := x_0^n + x_1^n + x_2^n$$

sind

$$f_{i,i} = n(n-1)x_i^{n-2}, \quad f_{i,j} = 0 \text{ für } i \neq j.$$

Die Hesse-Kurve der Fermat-Kurve hat deswegen die Gleichung

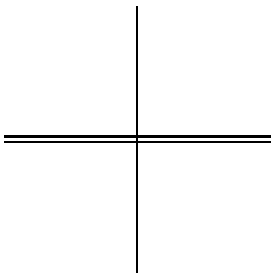
$$(x_0 x_1 x_2)^{n-2} = 0.$$

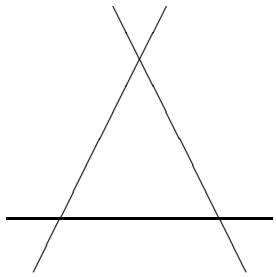
Die Schnittpunkte der Fermat-Kurve kann man leicht ausrechnen. Es sind $3n$ Punkte, aber für $n \geq 4$ sind dies keine transversalen Schnittpunkte und die Wendepunkte sind keine gewöhnlichen Wendepunkte.

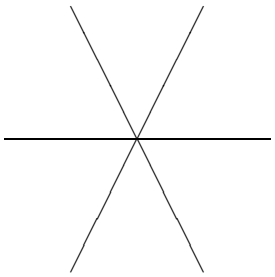
3 Kubiken

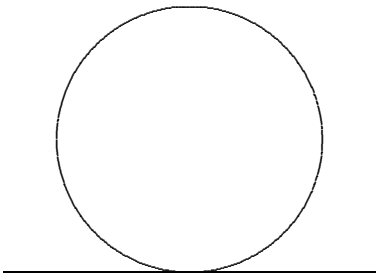
Kubiken sind Kurven vom Grad drei. Nach den Kegelschnitten sind dies die nächst-komplizierten Kurven. Um Symmetrien auszunützen möchte ich das Polynom vom Grad drei, welches eine Kubik beschreibt, wie folgt schreiben:

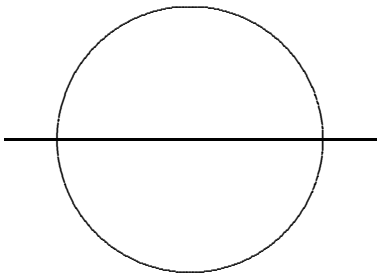
$$
\begin{array}{ccccccccccc}
 & & & & & & a_{300}x_0^3 & & & & \\
 & & + & & a_{210}x_0^2x_1 & + & & a_{201}x_0^2x_2 & & & \\
 & + & & a_{120}x_0x_1^2 & & + & a_{111}x_0x_1x_2 & & + & & a_{102}x_0x_2^2 \\
+ & & a_{030}x_1^3 & & + & & a_{021}x_1^2x_2 & & + & & a_{012}x_1x_2^2 & + & & a_{003}x_2^3
\end{array}
$$











3.1 Klassifikation

Reduzible Kubikem können als irreduzible Komponenten nur Geraden oder Kegelschnitte aufweisen. Deswegen kann man alle Möglichkeiten sehr schnell angeben. Bis auf projektive Äquivalenz sind es die folgenden sechs Fälle:

- drei zusammenfallende Geraden;
- zwei zusammenfallende Geraden und eine weitere Gerade;
- drei Geraden in allgemeiner Lage (Seiten eines Dreiecks);
- drei Geraden durch einen Punkt;
- ein Kegelschnitt mit Tangente;
- ein Kegelschnitt mit Transversale.

Die Klassifikation der Kubiken läuft also im Wesentlichen darauf hinaus, irreduzible Kubiken zu klassifizieren. Davon gibt es singuläre und nicht-singuläre. Weil das einfacher ist, konzentrieren wir uns zuerst auf die singulären Kurven.

Lemma 3.1 *Eine irreduzible Kubik C hat höchstens einen einzigen singulären Punkt.*

Beweis. Seien $\mathbf{p} \neq \mathbf{q} \in C$ zwei singuläre Punkte. Für die Gerade $L = \mathbf{pq}$ gilt nach Satz 2.10 d)

$$i_{\mathbf{p}}(C, L) \geq 2, \quad i_{\mathbf{q}}(C, L) \geq 2.$$

Also wäre

$$\sum_{\mathbf{p} \in C \cap L} i_{\mathbf{p}}(C, L) \geq 4.$$

Nach dem Satz von Bezout müssten C und L eine gemeinsame Komponente haben. Dies könnte nur die Gerade L sein, und C wäre nicht irreduzibel. □

Wir wählen die Koordinaten so, dass die (einzige) Singularität der Punkt $\mathbf{p} = (1 : 0 : 0)$ ist. Dann ist also

$$a_{300} = f(\mathbf{p}) = 0, \quad a_{210} = f_1(\mathbf{p}) = 0, \quad a_{201} = f_2(\mathbf{p}) = 0.$$

Wir ändern die Bezeichnung der Koeffizienten und schreiben das Polynom, welches die Kurve definiert, als

$$f(x_0, x_1, x_2) = x_0(b_{11}x_1^2 + 2b_{12}x_1x_2 + b_{22}x_2^2) + c_0x_1^3 + c_1x_1^2x_2 + c_2x_1x_2^2 + c_3x_2^3.$$

Hier kann nicht $b_{11} = b_{12} = b_{22} = 0$ gelten. Denn dann wäre für jede Gerade L durch $\mathbf{p}$

$$i_{\mathbf{p}}(C, L) = 3.$$

Wäre $\mathbf{q}$ ein weiterer, beliebiger Punkt aus C, so würde aus dem Satz von Bezout wieder folgen, dass $L := \mathbf{pq}$ eine Komponente von C ist. Das ist aber jetzt ausgeschlossen.

Die quadratische Form

$$(x_1, x_2) \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

ist nicht die Nullform. Es gibt zwei Möglichkeiten:

Fall 1: $Rang(b_{ij}) = 2$

Durch eine Koordinatentransformation in x_1, x_2 könnten wir die quadratische Form diagonalisieren. Aber wir wollen sie so transformieren, dass sie die Matrix

$$\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$$

hat. Dann wird das Polynom

$$f(x_0, x_1, x_2) = x_0x_1x_2 + c_0x_1^3 + c_1x_1^2x_2 + c_2x_1x_2^2 + c_3x_2^3.$$

Wir transformieren weiter

$$x_0' = x_0 + c_1x_1 + c_2x_2$$

und bringen das Polynom auf die Form

$$f(x_0', x_1, x_2) = x_0'x_1x_2 + c_0x_1^3 + c_3x_2^3.$$

Hier kann nicht $c_0 = 0$ oder $c_3 = 0$ sein, denn dann würde C die Gerade $x_1 = 0$ oder $x_2 = 0$ abspalten. Also können wir weiter transformieren

$$x_0'' := -\frac{x_0'}{\sqrt[3]{c_0c_1}}, \quad x_1' := \sqrt[3]{c_0}x_1, \quad x_2' := \sqrt[3]{x_2}$$

und das Polynom in die Form

$$(x_1')^3 + (x_2')^3 - x_0''x_1'x_2'$$

bringen. Die Kurve ist das Folium von Descartes geworden.

Fall 2: $Rang(b_{ij}) = 1$

Wir können die Koordinaten so wählen, dass die quadratische Form

$$\sum_{i,j=1}^{2} b_{i,j}x_ix_j = x_2^2$$

wird. Dann wird das Polynom

$$f(x_0, x_1, x_2) = x_0x_2^2 + c_0x_1^3 + c_1x_1^2x_2 + c_2x_1x_2^2 + c_3x_2^3.$$

Hier ist $c_0 \neq 0$, denn sonst würde C die Gerade $x_2 = 0$ abspalten. Wir können also transformieren

$$x_1' = \sqrt[3]{c_0}(x_1 + \frac{c_1}{3c_0}x_2), \quad (x_1')^3 = c_0x_1^3 + c_1x_1^2x_2 + \frac{c_1^2}{3c_0}x_1x_2^2 + \frac{c_1^3}{27c_0^2}x_2^3$$

und das Polynom in eine Form

$$f(x_0, x_1', x_2) = x_0 x_2^2 + (x_1')^3 + c_2' x_1' x_2^2 + c_3' x_2^3$$

bringen. Schließlich ersetzen wir x_0 durch $x_0' := -(x_0 + c_1' x_1' + c_2' x_2)$ und erhalten

$$f(x_0', x_1', x_2) = -x_0' x_2^2 + (x_1')^3.$$

Die Kurve C ist in die Neilsche Parabel transformiert worden.

Wir haben bewiesen:

Satz 3.1 *Die Kubik C sei irreduzibel und singulär. Dann kann man sie durch eine projektive Koordinatentransformation entweder auf die Form*

$$x_1^3 + x_2^3 - x_0 x_1 x_2 = 0 \quad \textit{(Folium von Descartes)}$$

oder

$$x_0 x_2^2 - x_1^3 = 0 \quad \textit{(Neilsche Parabel)}$$

bringen.

So, jetzt wenden wir uns dem interessantesten Fall zu, dass nämlich C glatt ist. Der Anfangspunkt der Diskussion ist ein Wendepunkt von C. Nach Bezout ist ja

$$C \cap H_C \neq \emptyset,$$

und C besitzt mindestens einen Wendepunkt. Den transformieren wir auf $(0:0:1)$. Und die Wendetangente in diesem Punkt transformieren wir auf die Gerade $x_0 = 0$. Die Einschränkung von f auf die Wendetangente ist

$$f(0, x_1, x_2) = a_{030} x_1^3 + a_{021} x_1^2 x_2 + a_{012} x_1 x_2^2 + a_{003} x_2^3.$$

Weil der Schnittpunkt $(0:0:1)$ von C mit der Wendetangente mindestens die Vielfachheit $= 3$ hat, ist $x_1 = 0$ eine dreifache Nullstelle dieses eingeschränkten Polynoms. Anders ausgedrückt:

$$a_{021} = a_{012} = a_{003} = 0.$$

Nach Umbenennung der Koefizienten wird das Polynom

$$f(x_0, x_1, x_2) = x_0 \cdot (a x_0^2 + b x_0 x_1 + c x_0 x_2 + d x_1^2 + e x_1 x_2 + f x_2^2) + g x_1^3.$$

(Ich gebe zu, der Koeffizient f ist nur schwer vom Polynom f zu unterscheiden, aber wir werden ihn sofort wieder los.) Es ist nämlich

$$f_0(0:0:1) = f, \quad f_1(0,0,1) = f_2(0,0,1) = 0.$$

Weil der Wendepunkt nicht singulär sein darf, folgt $f \neq 0$, und wir können transformieren

$$x_2' := \sqrt{2f}\, x_2, \quad (x_2')^2 = 2f x_2^2.$$

Damit wird

$$f(x_0, x_1, x_2') = x_0 \cdot (ax_0^2 + bx_0x_1 + c'x_0x_2 + dx_1^2 + e'x_1x_2 + \frac{1}{2}(x_2')^2) + gx_1^3.$$

Jetzt transformieren wir

$$x_2'' = x_2' + c'x_0 + e'x_1$$

um

$$\begin{aligned} c'x_0x_2' + e'x_1x_2' + \frac{1}{2}(x_2')^2 &= x_2' \cdot (c'x_0 + e'x_1 + \frac{1}{2}x_2') \\ &= (x_2'' - c'x_0 - e'x_1) \cdot \frac{1}{2}(x_2'' + c'x_0 + e'x_1) \\ &= \frac{1}{2} \cdot \left((x_2'')^2 - (c'x_0 + e'x_1)^2\right) \end{aligned}$$

zu erhalten. Damit haben wir das Polynom auf die Form

$$f(x_0, x_1, x_2'') = x_0 \cdot \left(a'x_0^2 + b'x_0x_1 + d'x_1^2 + \frac{1}{2}(x_2'')^2)\right) + gx_1^3$$

gebracht. Um die Übersicht zu behalten, lassen wir jetzt alle Striche weg:

$$f(x_0, x_1, x_2) = x_0 \cdot \left(ax_0^2 + bx_0x_1 + dx_1^2 + \frac{1}{2}x_2^2)\right) + gx_1^3$$

Hier ist $g \neq 0$, weil f irreduzibel ist. Deswegen dürfen wir

$$x_1' = \sqrt[3]{g}x_1$$

transformieren, und das Polynom auf eine Form

$$f(x_0, x_1', x_2) = x_0 \cdot \left(ax_0^2 + b'x_0x_1' + d'(x_1')^2 + \frac{1}{2}x_2^2\right) + (x_1')^3$$

zu bringen. Hier setzen wir

$$x_1'' := x_1' + \frac{d}{3}x_0$$

und haben

$$f(x_0, x_1'', x_2) = x_0 \cdot \left(a'x_0^2 + b'x_0x_1'' + \frac{1}{2}x_2^2\right) + (x_1'')^3.$$

Jetzt lassen wir wieder erst mal alle Striche weg:

$$f(x_0, x_1, x_2) = x_0 \cdot \left(ax_0^2 + bx_0x_1 + \frac{1}{2}x_2^2\right) + x_1^3.$$

Dann transfomieren wir

$$x_0 = -2x_0'$$

und

$$\begin{aligned} f(x_0', x_1, x_2) &= x_1^3 - 2x_0' \cdot \left(4a(x_0')^2 - 2bx_0'x_1 + \frac{1}{2}x_2^2\right) \\ &= x_1^3 - x_0'x_2^2 + 4b(x_0')^2x_1 - 8a(x_0')^3. \end{aligned}$$

Schließlich ersetzen wir x_1 durch $x_1'/\sqrt[3]{4}$, lassen wieder alle Striche weg, und erhalten mit neuen Konstanten g_2, g_3

$$f(x_0, x_1, x_2) = 4x_1^3 - x_0x_2^2 - g_2x_0^2x_1 - g_3x_0^3.$$

In affinen Koordinaten hat dann C die Gleichung

$$y^2 = 4x^3 - g_2x - g_3.$$

Definition 3.1 (WNF) *Eine Gleichung dritten Grades in der homogenen Form*

$$x_0x_2^2 = 4x_1^3 - g_2x_0^2x_1 - g_3x_0^2,$$

bzw. der affinen Form

$$y^2 = 4x^3 - g_2x - g_3$$

heißt Gleichung in Weierstraß Normalform.

Wir haben Teil a) des folgenden Satzes bewiesen:

Satz 3.2 *a) Die Gleichung einer glatten Kubik kann durch projektive Koordinatentransformation immer in Weierstraß Normalform gebracht werden.*

b) Eine Kubik mit Gleichung in Weierstraß Normalform ist genau dann glatt, wenn

$$g_2^3 \neq 27g_3^2.$$

Beweis b): Das Polynom f in Weierstraß Normalform hat die Ableitungen

$$\begin{aligned} \partial_0 f &= -x_2^2 - 2g_2x_0x_1 - 3g_3x_0^2, \\ \partial_1 f &= 12x_1^2 - g_2x_0^2 \\ \partial_2 f &= 2x_0x_2. \end{aligned}$$

In einer Singularität von C ist also entweder $x_0 = 0$ oder $x_2 = 0$. Wenn $x_0 = 0$ ist, dann folgt aus den beiden ersten Gleichungen $x_1 = x_2 = 0$. Das geht nicht. Und wenn $x_2 = 0$ ist, dann muss das Polynom

$$p(x_0, x_1) := f(x_0, x_1, 0) = 4x_1^3 - g_2x_0^2x_1 - g_3x_0^3$$

eine mehrfache Nullstelle besitzen. Wegen $x_0 \neq 0$ genügt es, das entsprechende inhomogene Polynom

$$p(x) = 4x^3 - g_2x - g_3$$

zu diskutieren.

Eine mehrfache Nullstelle von p ist eine Nullstelle von p und von seiner Ableitung

$$p' = 12x^2 - g_2.$$

Sowas gibt es genau dann, wenn die Resultante

$$R_{p,p'} = \det \begin{pmatrix} 4 & & -g_2 & -g_3 & \\ & 4 & & -g_2 & -g_3 \\ 12 & & -g_2 & & \\ & 12 & & -g_2 & \\ & & 12 & & -g_2 \end{pmatrix}$$

verschwindet. Die Berechnung dieser Determinante ist eigentlich ein Fall für den Computer. Aber es geht auch ganz einfach mit der Hand. Zunächst formen wir die Matrix etwas um. Dazu ziehen wir die dritte von der ersten und die vierte von der zweiten Zeile ab. Dann entsteht die Matrix

$$\begin{pmatrix} -8 & & & -g_3 & \\ & -8 & & & -g_3 \\ 12 & & -g_2 & & \\ & 12 & & -g_2 & \\ & & 12 & & -g_2 \end{pmatrix}$$

Jetzt multiplizieren wir die erste Zeile mit $3/2$ und addieren sie zur dritten Zeile. Ebenso multiplixieren wir die zweite Zeile mit $3/2$ und addieren sie zur vierten:

$$\begin{pmatrix} -8 & & & -g_3 & \\ & -8 & & & -g_3 \\ & & -g_2 & -3g_3/2 & \\ & & & -g_2 & -3g_3/2 \\ & & 12 & & -g_2 \end{pmatrix}$$

Diese Determinante verschwindet genau dann, wenn die rechte untere 3×3-Determinante

$$det \begin{pmatrix} -g_2 & -3g_3/2 & \\ & -g_2 & -3g_3/2 \\ 12 & & -g_2 \end{pmatrix} = -g_2^3 + 27g_3^2$$

verschwindet. Und das ist genau die Behauptung. □

Damit haben wir die glatten Kubiken noch nicht ganz klassifiziert. Wir wissen, dass man jede davon in eine WNF mit $g_2^3 \neq 27g_3^2$ bringen kann. Aber wann sind zwei Kubiken in dieser WNF projektiv äquivalent? Dieses Problem zerfällt in zwei Teile:

- Welche Rolle spielt die Auswahl des Wendepunktes?
- Wann sind zwei Kubiken mit festem Wendepunkt $(0 : 0 : 1)$ projektiv äquivalent?

Das erste dieser Probleme klären wir im nächsten Abschnitt.

3.2 Die Wendepunktskonfiguration

In diesem Abschnitt sei C eine irreduzible, glatte Kubik.

Wenn eine Wendetangente mit Vielfachheit > 3 im Wendepunkt schneidet, dann spaltet die Wendetangente als Komponente ab nach Bezout. Weil C irreduzibel ist, geht das nicht. Alle Wendepunkte von C sind gewöhnliche Wendepunkte. Aus Satz 4.15 b) folgt $i_{\mathbf{p}}(C, H_C) = 1$. Und aus dem Satz von Bezout folgt:

Satz 3.3 *C hat neun verschiedene Wendepunkte.*

Jetzt schauen wir uns die Gleichung von C in WNF nochmal an. Auf der Wendetangente $x_0 = 0$ von $(0 : 0 : 1)$ liegt kein weiterer Punkt von C. Wir schreiben die WNF deswegen affin

$$y^2 - 4x^3 - g_2x - g_3 = 0.$$

Diese Gleichung ist invariant unter der Involution

$$y \mapsto -y.$$

Unter dieser Involution werden die acht Wendepunkte $\neq (0 : 0 : 1)$ permutiert. Wenn ein Wendepunkt dabei fest bleibt, muss er auf der Geraden $y = 0$ liegen und von der Form $(x_0, 0)$ sein, wo x_0 eine Wurzel des Polynoms

$$p(x) = 4x^3 - g_2x - g_3$$

ist. Schränkt man die Gleichung von C auf die Gerade $x = x_0$ ein, so wird daraus $y^2 = 0$ mit der doppelten Nullstelle $y = 0$. Deswegen ist die Gerade $x = x_0$ eine Tangente, aber keine Wendetangente. Der Punkt $(x_0, 0)$ ist also kein Wendepunkt. Die Involution vertauscht also die acht Wendepunkte $\neq (0 : 0 : 1)$ paarweise. Je zwei davon liegen auf einer Geraden $x = const$ durch $(0 : 0 : 1)$. Weil der erste Wendepunkt, der auf $(0 : 0 : 1)$ transformiert wurde, beliebig gewählt war, finden wir:

Satz 3.4 *a) Durch jeden Wendepunkt gibt es vier Geraden derart, dass die anderen acht Wendepunkte paarweise auf diesen Geraden liegen.*

b) Die Verbindungsgerade je zwei verschiedener Wendepunkte schneidet C in einem dritten Wendepunkt.

c) Zu jedem Wendepunkt $\mathbf{p} \in C$ gibt es eine projektive Involution $I : \mathbb{P}_2 \to \mathbb{P}_2$, welche $\mathbf{p}$ fest lässt und C in sich transformiert. Sie vertauscht je zwei Wendepunkte, welche mit $\mathbf{p}$ auf einer Geraden liegen.

Jetzt zählen wir die Verbindungsgeraden von Wendepunkten ab: Auf jeder dieser Geraden liegen genau drei Wendepunkte. Durch jeden Wndepunkt gehen genau vier dieser Geraden. Die Anzahl möglicher Inzidenzen

$$\text{Wendepunkt} \ \in \ \text{Verbindungsgerade}$$

ist deshalb

$$9 \cdot 4 = 36.$$

Andererseits ist diese Zahl auch gleich

$$3 \times \text{Anzahl der Verbindungsgeraden.}$$

Deswegen gibt es genau 12 Verbindungsgeraden. Wir haben gezeigt:

Satz 3.5 *Die neun Wendepunkte und ihre zwölf Verbindungsgeraden bilden ein System von Punkten und Geraden, derart, dass durch jeden Punkt gleich viele (nämlich vier) Geraden gehen, und auf jeder Gerade gleich viel (nämlich drei) Punkte liegen.*

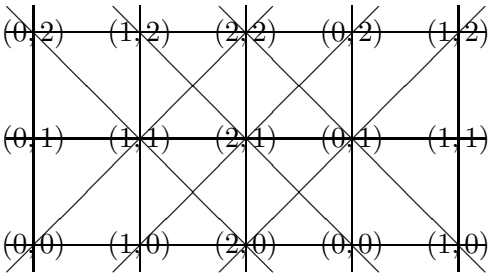
Ein solches System von Geraden nennt man eine *Konfiguration*. Wir haben es hier genauer mit einer

$$(12_3, 9_4) - \text{Konfiguration}$$

zu tun. Es gibt, bis auf projektive Äquivalenz, nur eine einzige derartige Konfiguration. Das zeigen wir in zwei Schritten:

Satz 3.6 *Jede $(12_3, 9_4)$-Konfiguration ist kombinatorisch äquivalent zur affinen Ebene $\mathbb{F}_3^2$ über dem Primkörper $\mathbb{F}_3$. Das heißt, man kann die neun Punkte bijektiv auf die neuun Punkte in $\mathbb{F}_3^2$ abbilden, so, dass die 12 Geraden, aufgefasst als Tripel kollinearer Konfigurationspunkte, auf die 12 Geraden in der affinen Ebene abgebildet werden.*

Die affine Ebene $\mathbb{F}_3^2$ kann man folgendermaßen visualisieren:



Das ist das bekannte 3×3-Determinanten-Schema.

Beweis des Satzes. Wir fixieren eine Konfigurations-Gerade L_0. Durch jeden der drei Konfigurations Punkte auf L_0 gehen, außer L_0 selbst, noch drei andere Geraden. Damit schneiden neun andere Geraden die Gerade L_0 in einem Konfigurationspunkt. Es muss dann

$$2 = 12 - 1 - 9$$

Geraden L_1, L_2 geben, die L_0 nicht in einem Konfigurationspunkt schneiden.

Wenn sich L_1 und L_2 in einem Konfigurationspunkt schneiden würden, so gingen durch diesen Schnittpunkt noch die drei Verbindungsgeraden mit den Konfigurationspunkten auf L_0. Das ist eine Gerade zuviel. Also schneiden sich L_1 und L_2 nicht in einem Konfigurationspunkt. Da L_0 beliebig war, haben wir sogar gezeigt:

Die 12 Konfigurationsgeraden bilden vier Tripel, derart, dass genau die Geraden eines Tripels keine Konfigurationspunkte gemeinsam haben. Wir wählen zwei dieser Tripel, etwa L_0, L_1, L_2

und M_0, M_1, M_2. Jede Gerade M_i schneidet jede Gerade L_j in einem Punkt $\mathbf{p}_{i,j}$ der Konfiguration. Weil sich keine zwei der drei Geraden M_i in einem Konfigurationspunkt schneiden, sind alle neun Punkte $\mathbf{p}_{i,j}$ voneinander verschieden. Sie sind also die Punkte unserer Konfiguration. Jetzt bilden wir ab

$$\mathbf{p}_{i,j} \mapsto (i,j) \in \mathbb{F}_3^2.$$

Das heißt also: die drei Geraden L_i entsprechen den drei senkrechten, die drei Geraden M_j den drei waagrechten Geraden im obigen Bild.

Dazu betrachten wir die Geraden, welche die Punkte $\mathbf{p}_{0,i}$ mit den Punkten $\mathbf{p}_{1,i+1}$ verbinden. (Die Indizes sollen hier $\in \mathbb{F}_3$ liegen, also modulo 3 genommen werden). Jede dieser Geraden muss auch noch L_2 schneiden. Das kann nur im Punkt $\mathbf{p}_{2,i+2}$ geschehen. Damit haben wir die drei Geraden, die im Bild von links unten nach rechts oben laufen. Die drei restlichen Geraden sind analog die Verbindungsgeraden von $\mathbf{p}_{0,i}$ mit $\mathbf{p}_{i,i+2}$. □

Satz 3.7 *Die Wendepunktskonfiguration einer glatten ebenen Kubik ist projektiv eindeutig. Genauer: Es gibt eine projektive Transformation, welche die neun Wendepunkte auf die neun Punkte*

$$(0:1:-\omega^i), \quad (-\omega^j:0:1), \quad (1:-\omega^k:0), \quad i,j,k = 0,1,2,$$

abbildet.

Beweis. Wir gehen davon aus, dass - wie im Beweis von Satz 3.6 gezeigt - die 12 Wendepunktsgeraden aus vier Tripeln

$$L_0, L_1, L_2, \quad M_0, M_1, M_2, \quad N_0, N_1, N_2, \quad O_0, O_1, O_2$$

bestehen, so dass sich keine zwei Geraden desselben Tripels in einem Wendepunkt schneiden. Dann wählen wir die Koordinaten so, das O_i die Gleichung $x_i = 0$ hat $(i = 0,1,2)$. Auf jeder dieser drei Geraden liegen drei Wendepunkte, keiner davon ein Koordinatenpunkt. Deswegen können wir die Koordinaten dieser Punkte allgemein wie folgt ansetzen:

$$\begin{array}{lccc} \text{auf } O_0: & (0:1:\lambda_0) & (0:1:\mu_0) & (0:1:\nu_0) \\ \text{auf } O_1: & (\lambda_1:0:1) & (\mu_1:0:1) & (\nu_1:0:1) \\ \text{auf } O_2: & (1:\lambda_2:0) & (1:\mu_2:0) & (1:\nu_2:0) \end{array}$$

Weiter können wir o.B.d.A. annehmen, dass sich diese neun Punkte folgendermaßen auf die neun anderen Geraden verteilen:

die Geraden	enthalten die Punkte
L_i	in den Spalten
M_i	in den Haupt-Diagonalen
N_i	in den Neben-Diagonalen

des obigen 3×3-Schemas.

Die Kollinearitätsbedingungen sind

$$det \begin{pmatrix} 0 & 1 & \lambda_0 \\ \lambda_1 & 0 & 1 \\ 1 & \lambda_2 & 0 \end{pmatrix} = \lambda_0\lambda_1\lambda_2 + 1 = 0$$

und analog

$$\mu_0\mu_1\mu_2 + 1 = \nu_0\nu_1\nu_2 + 1 = 0,$$

$$det \begin{pmatrix} 0 & 1 & \lambda_0 \\ \mu_1 & 0 & 1 \\ 1 & \nu_2 & 0 \end{pmatrix} = \lambda_0\mu_1\nu_2 + 1 = 0$$

und analog

$$\lambda_1\mu_2\nu_0 + 1 = \lambda_2\mu_0\nu_1 + 1 = 0,$$

$$det \begin{pmatrix} 0 & 1 & \lambda_0 \\ \nu_1 & 0 & 1 \\ 1 & \mu_2 & 0 \end{pmatrix} = \lambda_0\mu_2\nu_1 + 1 = 0$$

und analog

$$\lambda_1\mu_0\nu_2 + 1 = \lambda_2\mu_1\nu_2 + 1 = 0.$$

Auf unserer Situation operiert noch die Gruppe der Diagonalmatrizen

$$\begin{pmatrix} c_0 & 0 & 0 \\ 0 & c_1 & 0 \\ 0 & 0 & c_2 \end{pmatrix}, \quad c_1c_2c_3 \neq 0.$$

Hier wählen wir

$$\frac{c_1}{c_2} = -\lambda_0, \quad \frac{c_2}{c_0} = -\lambda_1$$

um

$$\begin{aligned} (0:1:\lambda_0) &\rightarrow (0:c_1:c_2\lambda_0) = (0:1:-1) \\ (\lambda_1:0:1) &\rightarrow (c_0\lambda_1:0:c_2) = (-1:0:1) \end{aligned}$$

also $\lambda_0 = \lambda_1 = -1$ zu erreichen. Aus der Kollinearitätsbedingung folgt dann auch $\lambda_2 = -1$.

Setzen wir das in die Kollinearitätsbedingungen ein, so bleiben die folgenden acht Gleichungen übrig:

$$\mu_0\mu_1\mu_2 = \nu_0\nu_1\nu_2 = -1$$

$$\mu_0\nu_1 = \mu_0\nu_2 = 1, \quad \mu_1\nu_2 = \mu_1\nu_0 = 1, \quad \mu_2\nu_0 = \mu_2\nu_1 = 1.$$

Aus den letzten sechs Gleichungen folgt

$$\mu_0 = \mu_1 = \mu_2 =: \mu, \quad \nu_0 = \nu_1 = \nu_2 =: \nu.$$

Und damit folgt aus den ersten beiden Gleichungen, dass jede der Zahlen μ, ν von der Form $-\omega^k$ ist. Weil die drei Punkte auf der Geraden O_0 voneinander verschieden sind, sehen wir (eventuell nach Vertauschen der Geraden L_1 und L_2)

$$\mu = -\omega, \quad \nu = -\omega^2.$$

Das ist die Behauptung. □

Was wird aus der Gleichung der Kubik, so wie sie am Anfang dieses Paragraphen steht, wenn wir ihre Wendepunkte auf die im letzten Satz angegebene Form transformieren?

Setzen wir etwa die drei Punkte auf O_0

$$(0:1:-1), \quad (0:1:-\omega), \quad (0:1:-\omega^2)$$

in die Gleichung ein. Es folgt der Reihe nach

$$\begin{array}{llll} a_{030} & -a_{021} & +a_{012} & -a_{003} = 0 \\ a_{030} & -a_{021}\omega & +a_{012}\omega^2 & -a_{003} = 0 \\ a_{030} & -a_{021}\omega^2 & +a_{012}\omega & -a_{003} = 0 \end{array}$$

Multiplizieren wir hier die i-te Zeile mit ω^{i-1}, $i = 1, 2, 3$, addieren die drei Zeilen, und benutzen

$$1 + \omega + \omega^2 = 0,$$

so bleibt nur die Bedingung

$$a_{012}(1 + 1 + 1) = 3a_{012} = 0$$

übrig. Es folgt

$$a_{012} = 0.$$

Multiplizieren wir aber die zweite Zeile mit ω^2 und die dritte mit ω, so folgt genauso

$$a_{021} = 0.$$

Schließlich folgt hiermit aus jeder der drei Zeilen

$$a_{030} = a_{003}.$$

Dasselbe Verfahren, angewendet auf die Punkte in O_1 und in O_2 ergibt insgesamt

$$a_{300} = a_{030} = a_{003}, \quad a_{111} \text{ beliebig},$$

während alle anderen Koeffizienten $= 0$ sein müssen. Unsere Gleichung muss von der Form

$$a \cdot (x_0^3 + x_1^3 + x_2^3) + b \cdot x_1x_2x_3 = 0$$

sein. Hier muss $a \neq 0$ sein, weil die Kurve sonst reduzibel wäre. Wir können die Gleichung durch a dividieren, bzw. gleich $a = 1$ annehmen. Schließlich können wir noch $b = 6m$ schreiben und erhalten die Hesse Normalform

$$x_0^3 + x_1^3 + x_2^3 + 6m \cdot x_1x_2x_3 = 0.$$

Wir haben Teil a) des folgenden Satzes bewiesen:

Satz 3.8 *Es sei $C \subset \mathbb{P}_2$ eine nicht-singuläre Kubik.*

a) Durch eine projektive Transformation kann man die Gleichung von C in Hesse Normalform transformieren.

b) C ist invariant unter einer zu $\mathbb{Z}_3 \times \mathbb{Z}_3$ isomorphen Gruppe projektiver Transformationen.

Beweis von b): Wegen a) können wir die Gleichung von C in Hesse Normalform annehmen. Dann betrachten wir die Transformationen σ, τ mit den Matrizen

$$S := \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}, \quad T := \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix}.$$

Wegen

$$S : (x_0 : x_1 : x_2) \mapsto (x_2 : x_0 : x_1), \quad T : (x_0 : x_1 : x_2) \mapsto (x_0 : \omega x_1 : \omega^2 x_2)$$

ist C invariant unter σ und τ, und dann auch unter der von σ und τ erzeugten Gruppe.

Man sieht sofort $S^3 = T^3 = \mathbb{1}_3$, deswegen ist $\sigma^3 = \tau^3 = id$. Die Produkte

$$ST = \begin{pmatrix} & & \omega^2 \\ 1 & & \\ & \omega & \end{pmatrix}, \quad TS = \begin{pmatrix} & & 1 \\ \omega & & \\ & \omega^2 & \end{pmatrix}$$

stimmen leider nicht überein. Die Matrizen S und T erzeugen keine kommutative Gruppe. Aber zum Glück ist

$$TS = \omega \cdot ST,$$

die Matrizenprodukte unterscheiden sich nur um einen Skalar. Daraus folgt $\sigma\tau = \tau\sigma$. Die von σ und τ erzeugte Gruppe H ist abelsch. Die Abbildung

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \ni (i, j) \mapsto \sigma^i \tau^j \in H$$

ist surjektiv. Wenn sie nicht injektiv wäre, hätte H weniger als neun Elemente. Aber wenn wir die Transformationen $\sigma^i\tau^j$ aug einen Wendepunkt, etwa $(0 : 1 : -1)$ anwenden, erhalten wir alle neun Wendepunkte als Bilder. Deswegen hat die Gruppe H genau neun Elemente. □

3.3 Die Gruppenstruktur

Wieder sei $C \subset \mathbb{P}_2$ eine glatte Kubik. Ein Wendepunkt $\mathbf{0} \in C$ werde fest gehalten.

Satz 3.9 *Auf der Menge C kann man eine Operation*

$$+ : C \times C \to C$$

definieren so, dass

- *C mit dieser Operation $+$ eine abelsche Gruppe ist;*
- *das neutrale Element der fixierte Wendepunkt $\mathbf{0}$ ist;*
- *drei Punkte $\mathbf{p}, \mathbf{q}, \mathbf{r} \in C$ kollinear sind, genau dann, wenn*

$$\mathbf{p} + \mathbf{q} + \mathbf{r} = \mathbf{0}.$$

Beweis. Wir betrachten einen Punkt $\mathbf{p} \in C$ und die Gerade $L := \mathbf{p0}$. Ist $\mathbf{q}$ der dritte Schnittpunkt von L mit C, so muss

$$\mathbf{p} + \mathbf{0} + \mathbf{q} = \mathbf{0}, \quad \mathbf{p} + \mathbf{q} = \mathbf{0}$$

sein. Dadurch ist $-\mathbf{p} = \mathbf{q}$ festgelegt. Das ist nun etwas salopp formuliert. Die drei Punkte $\mathbf{p}, \mathbf{q}, \mathbf{0}$ brauchen ja nicht alle voneinander verschieden zu sein. Wenn $i_{\mathbf{p}}(C, L) = 2$ ist, d.h., wenn L die Tangente in $\mathbf{p}$ ist, dann setzen wir $\mathbf{q} := \mathbf{p}$. Es könnte aber auch $\mathbf{p} = \mathbf{0}$ gewesen sein. Dann nehmen wir als L die Tangente an C in $\mathbf{0}$. Das ist eine Wendetangente, in diesem Fall muss also auch $\mathbf{r} = \mathbf{0}$ sein. Wir müssen die Schnittpunkte einer Geraden mit C also immer mit ihrer Vielfachheit zählen.

Wenn $\mathbf{p}, \mathbf{q}, \mathbf{r} \in C$ auf einer Geraden liegen, so muss

$$\mathbf{p} + \mathbf{q} = -\mathbf{r}$$

sein. Und $\mathbf{p} + \mathbf{q} = -(-\mathbf{r})$ ist der dritte Schnittpunkt der Geraden $\mathbf{r0}$ mit C. Damit ist die Operation $'+'$ wie folgt festgelegt:

Seien $\mathbf{p}, \mathbf{q} \in C$. Wir legen die Gerade $L = \mathbf{pq}$ durch beide Punkte und nennen $\mathbf{r}$ den dritten Schnittpunkt von C mit L. Wir legen durch $\mathbf{r}$ und $\mathbf{0}$ die Gerade $M := \mathbf{r0}$. Dann ist $\mathbf{p} + \mathbf{q}$ der dritte Schnittpunkt von M mit C.

Diese Operation ist wohldefiniert, wenn wir Schnittpunkte immer mit Multiplizität zählen. Man sieht auch sofort, dass $\mathbf{0}$ ein neutrales Element ist: Sei $\mathbf{p} \neq \mathbf{0}$ und L die Gerade $\mathbf{p0}$. Sei $\mathbf{r}$ der dritte Schnittpunkt von L mit C. Dann ist $L = M := \mathbf{r0}$ und $\mathbf{p}$ ist seinerseits der dritte Schnittpunkt von $\mathbf{r0}$ mit C. Weil die Gerade $L = \mathbf{pq}$ nicht von der Reihenfolge der beiden Punkte $\mathbf{p}$ und $\mathbf{q}$ abhängt, ist die Operation $'+'$ kommutativ. Es bleibt die Assoziativität zu zeigen, und das ist genau das Problem!

Seien $\mathbf{p}, \mathbf{q}, \mathbf{r} \in C$ drei Punkte. Wir definieren

L	:=	Gerade $\mathbf{pq}$	$\mathbf{a}$	:=	dritter Schnittpunkt in $L \cap C$,
M	:=	Gerade $\mathbf{a0}$	$\mathbf{p}+\mathbf{q}$	:=	dritter Schnittpunkt in $M \cap C$,
N	:=	Gerade $(\mathbf{p}+\mathbf{q})\mathbf{r}$	$\mathbf{b}$	:=	dritter Schnittpunkt in $N \cap C$,
L'	:=	Gerade $\mathbf{qr}$	$\mathbf{a}'$	:=	dritter Schnittpunkt in $L' \cap C$,
M'	:=	Gerade $\mathbf{a}'\mathbf{0}$	$\mathbf{q}+\mathbf{r}$	:=	dritter Schnittpunkt in $M' \cap C$,
N'	:=	Gerade $(\mathbf{q}+\mathbf{r})\mathbf{p}$	$\mathbf{b}'$	:=	dritter Schnittpunkt in $N' \cap C$.

Dann ist also $(\mathbf{p} + \mathbf{q}) + \mathbf{r}$ der dritte Schnittpunkt von $\mathbf{b0}$ mit C und $\mathbf{p} + (\mathbf{q} + \mathbf{r})$ der dritte Schnittpunkt von $\mathbf{b}'\mathbf{0}$ mit C. Es genügt $\mathbf{b} = \mathbf{b}'$ zu zeigen. Äquivalent dazu ist, dass die Punkte $\mathbf{p}, \mathbf{b}$ und $\mathbf{q} + \mathbf{r}$ kollinear sind.

Wir betrachten *das Büschel* von Kubiken

$$\lambda C + \mu L M' N, \quad (\lambda : \mu) \in \mathbb{P}_1.$$

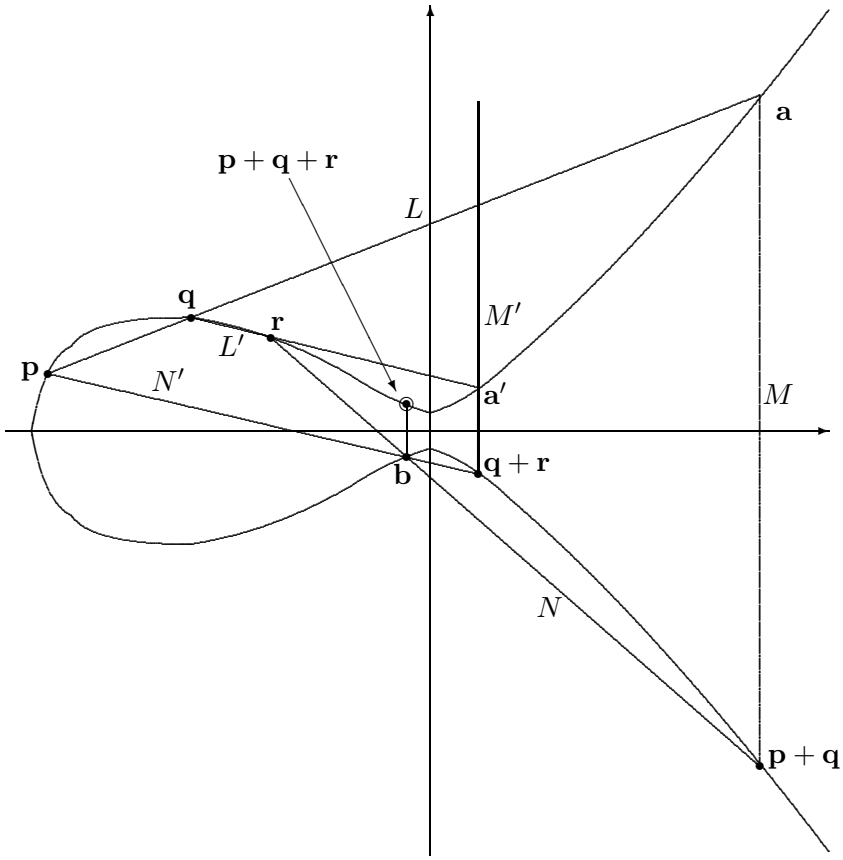
Auch diese Schreibweise ist wieder etwas salopp. Statt der Kurven C und $LM'N$ sollte man ihre definierenden Polynome nehmen und alle möglichen Linearkombinationen hinschreiben. Der Durchschnitt $C \cap (L \cup M' \cup N)$ besteht aus den neun Punkten

$$\mathbf{p}, \mathbf{q}, \mathbf{a} \in L, \quad \mathbf{q} + \mathbf{r}, \mathbf{0}, \mathbf{a}' \in M', \quad \mathbf{p} + \mathbf{q}, \mathbf{r}, \mathbf{b} \in N.$$

Jede Kubik des Büschels geht durch diese neun Punkte. In dem Büschel gibt es eine Kubik C', die L' in $\mathbf{q}, \mathbf{r}, \mathbf{a}'$ und in einem vierten Punkt schneidet. Nach Bezout geht das nur, wenn C' die Gerade L' abspaltet, etwa $C' = L' \cup Q$ mit einem Kegelschnitt Q. Keiner der sechs anderen Punkte

$$\mathbf{p}, \mathbf{a}, \mathbf{q}+\mathbf{r}, \mathbf{0}, \mathbf{p}+\mathbf{q}, \mathbf{b}$$

liegt auf L'. Sie müssen alle auf Q liegen. Aber die drei Punkte $\mathbf{p}+\mathbf{q}, \mathbf{0}, \mathbf{a} \in M$ sind kollinear. Deswegen muss der Kegelschnitt Q die Gerade M abspalten, etwa $Q = M \cup L''$. Dabei ist L'' eine Gerade, welche die drei Punkte $\mathbf{p}, \mathbf{q}+\mathbf{r}, \mathbf{b} \notin M$ enthält. □



Diese Gruppenstruktur ist so fundamental für Kurven vom Grad drei, dass sie sogar auf manche singulären Kubiken durchschlägt. Wir betrachten einige Beispiele.

Beispiel: Addition auf der Neilschen Parabel. Wir schreiben die affine Gleichung $y^2 - x^3 = 0$ und die homogene Form $x_0x_2^2 - x_1^3 = 0$. Wir können die Kurve durch

$$\mathbb{C} \ni t \mapsto (t^2, t^3), \text{ bzw. } (1 : t^2 : t^3)$$

parametrisieren. Mit der unendlich-fernen Gerade $x_0 = 0$ hat die Kurve den einzigen Schnittpunkt $(0 : 0 : 1)$. Dies muss ein Wendepunkt sein. Ihn wollen wir als Ursprung nehmen. Der soll natürlich zu $t = 0$ gehören. deswegen ersetzen wir t durch $1/t$ und gehen über zur Parametrisierung

$$\mathbb{C} \ni \mapsto (t^3 : t : 1).$$

Dadurch werden jetzt alle Punkte von C bis auf die Singularität $(1:0:0)$ parametrisiert.

Wir müssen die Kollinearitätsbedingung für drei Punkte $(t^3:t:1), (u^3:u:1), (v^3:v:1)$ auswerten. Sie lautet

$$det \begin{pmatrix} t^3 & t & 1 \\ u^3 & u & 1 \\ v^3 & v & 1 \end{pmatrix} = 0.$$

Wir ziehen die erste Zeile von den beiden anderen Zeilen ab und bringen die Determinante in die Form

$$det \begin{pmatrix} t^3 & t & 1 \\ u^3-t^3 & u-t & 0 \\ v^3-t^3 & v-t & 0 \end{pmatrix}.$$

Wir klammern die Faktoren $(u-t)$ bzw. $v-t$ aus der zweiten, bzw. dritten Zeile aus und entwickeln die Determinante nach ihrer dritten Spalte, um

$$(u^2+ut+t^2)-(v^2+vt+t^2) = (u-v)(u+v+t)$$

zu erhalten. Insgesamt ist die Determinante

$$(t-u)(t-v)(u-v)\cdot(t+u+v).$$

Der erste Faktor verschwindet, wenn zwei Kurvenpunkte zusammenfallen. Ist dies nicht der Fall, so wird die Bedingung

$$t+u+v=0.$$

Das bedeutet: Die Gruppenoperation auf der Kurve ist die Addition im Parameter-Raum $\mathbb{C}$.

Beispiel: Multiplikation auf dem Folium. Wir wählen als Gleichung

$$y^2 = x^2\cdot(x+1) \quad \text{bzw.} \quad x_0x_2^2 - x_1^2(x_0+x_1) = 0.$$

Nach etwas Probieren findet man eine Parametrisierung

$$\mathbb{C} \ni\mapsto \Big((1-t)^3 : 4t(1-t) : 4t(1+t)\Big).$$

Das ist jetzt so gemacht, dass $t=1$ auf den Wendepunkt $(0:0:1)$ geht und beide Parameter $0,\infty$ auf den singulären Punkt $(1:0:0)$. Die Kurvenpunkte außerhalb der Singularität werden durch $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$ parametrisiert.

Die Kollinearitätsbedingung ist

$$det \begin{pmatrix} (1-t)^3 & 4t(1-t) & 4t(1+t) \\ (1-u)^3 & 4u(1-u) & 4u(1+u) \\ (1-v)^3 & 4v(1-v) & 4v(1+v) \end{pmatrix} = 0.$$

Diese Determinante habe ich jetzt mit MAPLE ausgewertet und faktorisiert. Das Ergebnis ist

$$32(t-u)(t-v)(u-v)\cdot(tuv-1).$$

Wieder verschwindet der erste Faktor, wenn zwei Punkte zusammenfallen. Ist dies nicht der Fall, so ist die Kollinearitätsbedingung

$$t \cdot u \cdot v = 1.$$

Das bedeutet: Die Gruppenstruktur auf den glatten Kurvenpunkten ist die Multiplikation auf $\mathbb{C}^*$.

Ich nehme an, dass man ganz ähnlich Gruppenstrukturen auch auf den vier reduziblen Kubiken ohne mehrfache Komponenten bekommt. Und zwar sollten rauskommen

Kurve	Gruppe
drei Geraden durch einen Punkt	$\mathbb{C} \times \mathbb{Z}_3$
drei Geraden nicht durch einen Punkt	$\mathbb{C}^* \times \mathbb{Z}_3$
Kegelschnitt und Tangente	$\mathbb{C} \times \mathbb{Z}_2$
Kegelschnitt und Sekante	$\mathbb{C}^* \times \mathbb{Z}_2$

Es wäre interessant, dem mal nachzugehen. Bei den drei Geraden nicht durch einenPunkt sollte natürlich genau der Satz von Menelaos rauskommen.

3.4 Parametrisierung

Die beiden Sorten irreduzibler Kubiken (Neilsche Parabel, Folium) haben wir am Ende des letzten Paragraphen durch Polynome parametrisiert. Die habe ich vom Himmel fallen lassen. Aber systematisch geht man so vor: Wir betrachten alle Geraden durch den singulären Punkt. Eine solche Gerade schneidet die Kurve höchstens noch in einem weiteren Punkt. Ordnet man diesem Kurvenpunkt die (Steigung der) Gerade zu, so bekommt man eine Parametrisierung.

Beispiel: Neilsche Parabel. Die affine Gleichung ist

$$y^2 = x^3.$$

Die Geraden

$$y = t \cdot x$$

durch die Singularität $\mathbf{0}$ parametrisieren wir durch ihre Steigung $t \in \mathbb{C}$ (oder $t \in \mathbb{P}_1(\mathbb{C})$. Ersetzen wir in der Kurvengleichung y durch $t \cdot x$, so finden wir

$$t^2 \cdot x^2 = x^3, \quad \text{bzw.} \quad x = t^2$$

und $y = t \cdot x = t^3$.

Beispiel: Folium. Die affine Gleichung

$$y^2 = x^2 \cdot (x + 1)$$

beschreibt eine Kurve mit Singularität im Ursprung. Wieder eliminieren wir $y = t \cdot x$ und erhalten

$$t^2 \cdot x^2 = x^2 \cdot (x + 1), \quad t^2 = x + 1, \quad x = t^2 - 1.$$

Damit wird $y = t^3 - t$ und wir haben eine Parametrisierung

$$x = t^2 - 1, \quad y = t^3 - t.$$

Ich habe im letzten Paragraphen etwas andere Parametrisierungen benutzt, weil ich ja z.B. den Wendepunkt im Unendlichen durch $t = 0$ parametrisieren wollte.

Definition 3.2 *Die ebene algebraische Kurve C heißt* rational*, wenn es drei Polynome*

$$p, q, r \in \mathbb{C}[t]$$

gibt, derart, dass durch

$$(p(t) : q(t) : r(t)) \ \ \textit{mit } t \in \mathbb{P}_1(\mathbb{C})$$

alle Punkte der Kurve parametrisiert werden.

Äquivalent dazu ist, dass der affine Teil der Kurve C durch zwei rationale Funktionen q/p, $r/p \in \mathbb{C}(t)$ parametrisiert werden kann.

Geraden und irreduzible Kegelschnitte sind rational. Und wir haben soeben bewiesen:

Satz 3.10 *Irreduzible, singuläre Kubiken sind rational.*

Im Gegensatz dazu gilt:

Satz 3.11 *Glatte Kubiken sind nicht rational.*

Beweis. (Abgeschrieben aus dem Buch

- M. Reid. Undergraduate Algebraic Geometry. 1988)

Wir nehmen die Gleichung in WNF an, affin geschrieben

$$y^2 = 4x^3 - g_2 x - g_3.$$

Solange $g_2 \neq 0$ ist können wir eine der Nullstellen des Polynoms auf der rechten Seite in den Nullpunkt verschieben und o.B.d.A. $g_3 = 0$ annehmen. Ersetzen wir noch y durch $2y$, so nimmt unsere Gleichung eine Form

$$y^2 = x \cdot (x - \lambda) \cdot (x - \mu)$$

an, wo die drei Nullstellen $0, \lambda, \mu$ der rechten Seite alle voneinander verschieden sind. Jezt ersetzen wir noch

$$x \text{ durch } \mu x, \quad y \text{ durch } \sqrt{\mu} y$$

und bringen unsere Gleichung auf die Form

$$y^2 = x \cdot (x - 1) \cdot (x - \lambda), \quad \lambda \neq 0,\, 1,$$

bzw. homogen

$$x_0 x_2^2 = x_1 \cdot (x_1 - x_0) \cdot (x_1 - \lambda x_0).$$

Jetzt nehmen wir an, wir könnten unsere Kurvenpunkte durch Polynome $f, g, h \in \mathbb{C}[t]$ parametrisieren:

$$(x_0 : x_1 : x_2) = (f(t) : g(t) : h(t)) = (1 : \frac{g}{f} : \frac{h}{f}), \quad t \in \mathbb{C}.$$

Die entstandenen Brüche kürzen wir:

$$\frac{g}{f} = \frac{p}{q}, \quad \frac{h}{f} = \frac{r}{s},$$

wobei $p, q \in \mathbb{C}[t]$ keinen gemeinsamen Linearfaktor haben, ebenso wie $r, s \in \mathbb{C}[t]$. Dann hätten wir also

$$\frac{r^2}{s^2} = \frac{p}{q} \cdot (\frac{p}{q} - 1) \cdot (\frac{p}{q} - \lambda).$$

Wäre hier $p/q = const \in \mathbb{C}$, so auch r/s und wir bekämen aus unserer Parametrisierung nur einen einzigen Kurvenpunkt. Wir können also annehmen, dass p/q nicht konstant ist. Wir multiplizieren unsere Gleichung mit den Nennern durch und finden

$$q^3 \cdot r^2 = s^2 \cdot p \cdot (p - q) \cdot (p - \lambda q).$$

Weil p und q teilerfremd sind, sind dies auch $p - q$ und q, sowie $p - \lambda q$ und q. Weil außerdem r und s teilerfremd sind, folgt

$$s^2 = a \cdot q^3, \quad a \in \mathbb{C}.$$

Insbesondere muss q ein Quadrat sein. Aus der gekürzten Gleichung

$$r^2 = a \cdot p \cdot (p - q) \cdot (p - \lambda q)$$

folgt mit der Teilerfremdheit der Polynome $p, p - q$ und $p - \lambda q$, dass diese Polynome alle drei Quadrate sind.

Wir haben vier teilerfremde Linearkombinationen

$$p,\ q,\ p - q,\ p - \lambda q$$

der Polynome p und q, die alle Quadrate sind. Die Linearkombinationen sind verschieden in dem Sinn, dass die vier Linearkombinationen $\mu_i - \lambda_i q$ zu vier verschiedenen Punkten $(\mu_i : \lambda_i) \in \mathbb{P}_1$ gehören. Das ist im Widerspruch mit

Lemma 3.2 *Es seien $p, q \in \mathbb{C}[t]$ teilerfremde Polynome, nicht beide konstant. Dann können keine vier verschiedenen Linearkombinationen dieser Polynome Quadrate in $\mathbb{C}[t]$ sein.*

Beweis (Unendlicher Abstieg). Wir nehmen an, es gebe solche Polynome. Wir wählen p und q so dass $max\{deg(p), deg(q)\}$ minimal (aber immer noch > 0) ist. Durch eine projektive Transformation im $\mathbb{P}_1$ der Koeffizienten, können wir sie auf die Form

$$p,\ q,\ p - q,\ p - \lambda q$$

bringen. Dann ist insbesondere

$$p = u^2, \quad q = v^2$$

mit Polynomen $u, v \in \mathbb{C}[t]$, die

$$0 < max\{deg(u), deg(v)\} < max\{deg(p), deg(q)\}$$

erfüllen. Weil p und q teilerfremd sind, sind dies auch u und v. Deswegen, und weil

$$p - q = u^2 - v^2 = (u - v)(u + v), \quad p - \lambda q = (u - \sqrt{\lambda}v)(u + \sqrt{\lambda}v)$$

Quadrate sind, müssen alle vier Polynome

$$u - v, \quad u + v, \quad u - \sqrt{\lambda}v, \quad u + \sqrt{\lambda}v$$

Quadrate sein. Es sind vier verschiedene Linearkombinationen von u und v. Dann konnten p und q nicht minimales $max\{deg(p), deg(q)\}$ gehabt haben. Widerspruch!

Auf das Problem der Rationalität ebener Kurven stießen die Mathematiker gegen Ende des 18. Jhdts, als sie versuchten algebraische Funktionen f (was immer dies sein mag) zu integrieren. Wann ist

$$\int f(x)dx$$

durch elementare Funktionen (was immer das sein mag) auszudrücken?

Beispiel. Das Integral

$$\int \frac{dx}{\sqrt{1 - x^2}} = arcsin(x) = sin^{-1}(x)$$

ist elementar auszuwerten. Ohne Kenntnis des Sinus und seiner Umkehrfunktion kann man dies so tun: Die Funktion

$$y = \sqrt{1 - x^2}$$

hat als Graphen den Einheitskreis $x^2 + y^2 = 1$. Er kann parametrisiert werden durch die rationalen Funktionen

$$x(t) = \frac{2t}{1 + t^2}, \quad y(t) = \frac{t^2 - 1}{1 + t^2}.$$

Substituiert man die im Integral, erhält man

$$\int \frac{dx}{\sqrt{1 - x^2}} = \int \frac{dx}{y} = \int \frac{1 + t^2}{t^2 - 1} \cdot \frac{2(1 + t^2) - 4t^2}{(1 + t^2)^2} dt = 2 \int \frac{1 - 2t^2}{(t^2 - 1)(t^2 + 1)} dt.$$

Dies kann man elementar mit Partialbruchzerlegung angehen und im Resultat

$$t = \frac{1}{x}(1 \pm \sqrt{1 - x^2})$$

zurück-substituieren.

Beispiel (Elliptisches Integral): Es sei $L(u)$ die Bogenlänge der Ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Der Einfachheit halber nehmen wir an $a = 1$. Dann wird

$$y = b \cdot \sqrt{1 - x^2}, \quad \frac{dy}{dx} = \frac{-bx}{\sqrt{1 - x^2}}.$$

Damit wird

$$L(u) = \int_0^u \sqrt{1 + (y')^2} dx = \int_0^u \sqrt{1 + \frac{b^2 x^2}{1 - x^2}} dx = \int_0^u \sqrt{\frac{1 + (b^2 - 1)x^2}{1 - x^2}} dx.$$

Mit der Substitution $k^2 = b^2 - 1$ wird daraus

$$\int_0^u \frac{1 - k^2 x^2}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} dx.$$

Trotz größter Bemühungen gelang es nicht dieses Integral durch elementare Funktionen auszuwerten.

Man kann natürlich versuchen, wie bei

$$y = \frac{1}{\sqrt{1 - x^2}}$$

auch hier rationale Funktionen $r_1(t), r_2(t) \in \mathbb{C}(t)$ zu finden, so, dass

$$x = r_1(t), \quad y := \sqrt{(1 - x^2)(1 - k^2 x^2)} = r_2(t).$$

Dann könnte man auch das elliptische Integral durch Integration rationaler Funktionen auswerten. Dieses Verfahren ist aber zum Scheitern verurteilt. Um das zu verstehen, vereinfachen wir die Situation etwas, indem wir

$$x = 1 + \frac{1}{\xi}, \quad \xi = \frac{1}{x - 1}$$

substituieren. Ist $p_4(x)$ das Polynom vom Grad vier unter der Wurzel bei y, so wird hieraus durch die Substitution

$$\left(1 - (1 + \frac{1}{\xi})\right)\left(1 + (1 + \frac{1}{\xi})\right)\left(1 - k^2(1 + \frac{1}{\xi})^2\right) = -\frac{1}{\xi^4}(2\xi + 1)(\xi^2 - k^2(\xi + 1)^2).$$

Könnte man $x = r_1$, $y = r_2$ durch rationale Funktionen substituieren, dann auch

$$\xi = \frac{1}{r_1 - 1}$$

und

$$\eta := \xi^2 \cdot y = \sqrt{-(2\xi + 1)(\xi^2 - k^2(\xi + 1)^2} = \sqrt{p_3(\xi)},$$

wo $p_3 \in \mathbb{C}[\xi]$ ein Polynom dritten Grades mit den drei paarweise verschiedenen Nullstellen

$$\xi_1 = -\frac{1}{2}, \quad \xi_2 = \frac{k}{1 - k}, \quad \xi_3 = -\frac{k}{1 + k}.$$

Dann könnte man auch die Kurve dritten Grades mit der affinen Gleichung

$$\eta^2 = \sqrt{p_3(\xi)}$$

durch rationale Funktionen parametrisieren. Die Kurve ist eine glatte Kubik, und wegen Satz 3.11 geht das eben nicht.

Das ist die schlechte Nachricht. Die gute Nachricht ist, dass die Mathematiker um 1800 trotzdem nicht aufgaben zu versuchen, das elliptische Integral zu verstehen. Der Durchbruch ist mit dem Namen Jacobi verbunden. Jedenfalls schrieb er gegen 1820 (noch auf Latein) eine Arbeit, in der er nicht das elliptische Integral, sondern dessen Umkehrfunktion betrachtete. Die Idee kann man sehr schön am Kreis-Integral

$$t := \int \frac{1}{\sqrt{1-x^2}} = arcsin(x)$$

verstehen. Die Funktion $t = arcsin(x)$ ist unendlich vieldeutig, aber irgenwie geschlängent bildet sie ihr Parameter-Intervall $[-1,1]$ auf die ganze t-Achse ab. Das ist schwer zu verstehen. Einfacher zu verstehen ist die Umkehrfunktion $x = sin(t)$. Sie ist periodisch und bildet die t-Achse $\infty : 1$ auf das x-Intervall $[-1,1]$ ab.

Jacobi fasste

$$z := \int_{-1}^{x} \frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}} dx$$

als komplexe Funktion des komplexen Arguments x auf. Nehmen wir o.B.d.A. $k < 1$ und $1/k > 1$ an. Dann hat der Radikand auf der reellen Achse die Nullstellen

$$-\frac{1}{k} < -1 < 1 < \frac{1}{k}.$$

Wenn man bei -1 anfängt zu integrieren und in Richtung $+1$ integriert, ist der Integrand reell, positiv (falls man die positive Wurzel nimmt) und bildet das Intervall $[-1,1]$ streng monoton auf ein reelles Intervall $[0,e_1]$ ab. Rechts von $x = 1$ wird der Integrand rein imaginär. Wählen wir den richtigen Zweig der Wurzel, so bildet das Integral das Intervall $[1,1/k]$ streng monoton auf eine Strecke $[e_1, e_1 + ie_2]$ mit $0 < e_2 \in \mathbb{R}$ ab. Ebenso kann man bei Wahl des richtigen Zweigs der Wurzel das Intervall $[-1,-1/k]$ auf die Strecke $0, ie_1$ abbilden. Jacobi zeigt, dass das elliptische Integral die obere Halbebene $Re(x) > 0$ bijektiv auf das Rechteck mit den Ecken $0, e_1, e_1 + ie_2, ie_2$ abbildet. Ähnlich wie beim Arcus-Sinus kann man durch sukzessive geeignete Wahl der Vorzeichen der Wurzel die ganze komplexe Zahlenebene durch Translate dieses Rechtecks überpflastern. Und die Unkehrfunktion dieser unendlich mehrdeutigen Funktion bildet doppelt-periodisch

$$\mathbb{C} \to \mathbb{P}_1(\mathbb{C})$$

ab.

Definition 3.3 *Es sei $\omega \in \mathbb{C}$ eine komplexe Zahl mit $Im(\omega) > 0$. Eine komplex-wertige Funktion $f : \mathbb{C} \to \mathbb{P}_1(\mathbb{C})$ heißt doppelt-periodisch mit den Perioden 1 und ω, wenn für alle $z \in \mathbb{Z}$*

$$f(z) = f(z+1) = f(z+\omega).$$

Die Teilmenge

$$\Omega := \mathbb{Z} + \mathbb{Z} \cdot \omega \subset \mathbb{C}$$

heißt das Periodengitter *von f.*

Ω ist eine Untergruppe von $\mathbb{C}$. Die Doppelt-Perodizität von f bedeutet, dass f wie folgt faktorisiert:

$$f: \quad \mathbb{C} \to \mathbb{C}/\Omega \to \mathbb{P}_1(\mathbb{C}).$$

In der Funktionentheorie zeigt man, dass jede doppelt-periodische holomorphe Funktion konstant ist. Aber es gibt doppelt-periodische meromorphe Funktionen. Die einfachste davon ist die Weierstraßsche $\wp$-Funktion

$$\wp(z) = \frac{1}{z^2} + \sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \left(\frac{1}{(z-m-n\omega)^2} - \frac{1}{(m+n\omega)^2} \right).$$

Es ist allerdings etwas mühsam, zu zeigen, dass diese Doppelreihe außerhalb der Gitterpunkte konvergiert und eine doppelt-periodische meromorphe Funktion auf $\mathbb{C}$ definiert. Aber das ist Standard-Stoff von Funktionentheorie II. Durch Laurent-Entwicklung um den Nullpunkt beweist man auch:

Satz 3.12 *Die Weierstraßsche $\wp$-Funktion erfüllt die Differentialgleichung*

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

mit

$$g_2 := 60 \sum_{(m,n)\neq(0,0} \frac{1}{(m+n\omega)^4}, \quad g_3 := 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\omega)^4}.$$

Bildet man jetzt ab

$$\mathbb{C} \ni x \mapsto (1 : \wp(z) : \wp'(z)) \in \mathbb{P}_2(\mathbb{C})$$

so liegt die Bildmenge in der Kurve C mit der Gleichung

$$x_0x_2^2 = 4x_1^3 - g_2x_0^2x_1 - g_3x_0^3.$$

Das ist eine Kubik in WNF. Nur noch erwähnen, nicht mehr beweisen möchte ich

Satz 3.13 *Diese Parametrisierung definiert eine Bijektion*

$$\mathbb{C}/\Omega \to C.$$

Unter dieser Bijektion geht die Addition in der Quotientengruppe $\mathbb{C}/\Omega$ über in die Gruppenoperation auf C aus 3.3.

Glatte Kurven vom Grad drei heißen *elliptische* Kurven. Sie spielen die Hauptrolle beim Beweis der Fermatschen Vermutung durch A.Wiles. Sehr lustig ist, dass sie über den Bestseller 'Fermats letzter Satz' von S.Singh sogar Eingang in die wissenschaftliche Populär-Literatur gefunden haben, ohne dass Singh mit einem einzigen Wort sagt, was das für Objekte sind.