Algebraische Kurven

Wolfgang M. Ruppert

Sommersemester 2021

Vorlesungsskript zu einer im Sommersemester 2021 in Erlangen gehaltenen Vorlesung

Datei: algku0.tex. Version vom 21.7.2021

Vorbemerkungen:

(1) Die Vorlesung war ursprünglich als Master-Vorlesung geplant. Da jedoch Bedarf an einer 5-ECTS-Vorlesung „Geometrie für Lehramt“ bestand, habe ich die Vorlesung etwas umstrukturiert. Die (ungefähr) erste Hälfte der Vorlesung konnte als „Geometrie für Lehramt“ gehört werden. Hier versuchte ich, mit minimalen algebraischen Vorkenntnissen auszukommen. Inhaltlich handelt es sich dabei um die Kapitel 1 bis 5 des vorliegenden Skripts. Der Rest der Vorlesung setzt deutlich mehr Algebra voraus.

(2) Um inhaltlich nicht bei den Grundlagen stehenzubleiben, wurde in Kapitel 6 „Algebraische Varietäten - vertieft“ einiges aus der Algebraischen Geometrie (ohne Beweise) zusammengestellt. Auch später wurde einiges nicht bewiesen, wie die Existenz eines nichtsingulären Modells einer Kurve und der Satz von Riemann-Roch. Wichtiger war mir, den Umgang mit algebraischen Kurven zu zeigen.

(3) Als Anwendungen finden sich kurze Abschnitte über Codierungstheorie (Kapitel 5, Abschnitt 5) und Kryptographie (Kapitel 13, Abschnitt 6).

(4) Dieses Vorlesungsskript wurde aus den in der Vorlesung verwendeten Folien erstellt.

Inhaltsverzeichnis

KAPITEL 1

Einführung

Mit der Erfindung der kartesischen Koordinaten durch Descartes und Fermat in der ersten Hälfte des 17. Jahrhunderts wurde es möglich, geometrische Fragestellungen algebraisch zu formulieren und mit den Methoden der Algebra zu behandeln. Heutzutage lernt man bereits in der Schule, wie man einfache geometrische Gebilde wie Geraden, Parabeln, Ebenen und Kugeln durch Gleichungen beschreibt.
In der Algebraischen Geometrie studiert man nun allgemein Lösungsmengen polynomialer Gleichungen. Dazu gehören geometrische Objekte, aber auch diophantische Gleichungen.

Ausgangspunkt der Algebraischen Geometrie sind folgende Situationen:

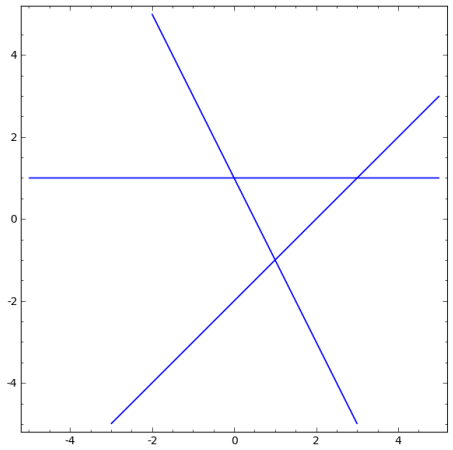
- Man übersetzt geometrische Aufgabenstellungen in algebraische Gleichungen und versucht sie zu lösen.
- Man deutet algebraische Gleichungen geometrisch und versucht sie auf diese Weise besser zu verstehen.

1. Beispiele für Beziehung von Algebra und Geometrie

Bevor wir richtig beginnen, wollen wir zwei einfache Beispiele für das fruchtbare Zusammenwirken von Geometrie und Algebra geben.

Beispiel: Gegeben seien die drei Geraden

$$y = x - 2, \quad y = -2x + 1, \quad y = 1.$$



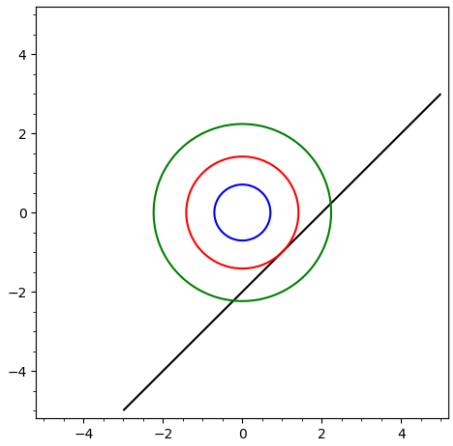
Bestimmt werden sollen alle Kreise, die alle drei Geraden berühren.

- Ein Kreis $K_r(u, v)$ mit Mittelpunkt (u, v) und Radius r wird beschrieben durch die Gleichung

$$(x - u)^2 + (y - v)^2 = w \quad \text{mit} \quad w = r^2.$$

Datei: algku1.tex. Version vom 21.7.2021

Ein Kreis und eine Gerade können sich in keinem Punkt, einem Punkt oder zwei Punkten schneiden, wie die folgende Skizze zeigt.



- **Erinnerung:** Die Diskriminante einer quadratischen Gleichung

$$ax^2 + bx + c = 0 \text{ mit } a, b, c \in \mathbb{R} \text{ und } a \neq 0$$

ist definiert als

$$D = b^2 - 4ac.$$

Es gibt drei Fälle:
  - Fall $D > 0$: Die quadratische Gleichung hat die zwei (verschiedenen) reellen Lösungen

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}.$$

  - Fall $D = 0$: Die quadratische Gleichung hat genau eine Lösung, nämlich

$$x = \frac{-b}{2a}.$$

  - Fall $D < 0$: Die quadratische Gleichung hat keine reelle Lösung.
- Wir überlegen zunächst, wann der Kreis $K_r(u, v)$ eine der gegebenen Geraden berührt.
  - Ein Punkt (x, y) liegt genau dann im Durchschnitt der Geraden $y = x - 2$ und des Kreises $K_r(u, v)$, wenn gilt

$$\begin{aligned}
&\iff \quad y = x - 2 \text{ und } (x-u)^2 + (y-v)^2 = w \quad \iff \\
&\iff \quad y = x - 2 \text{ und } (x-u)^2 + (x-2-v)^2 = w \quad \iff \\
&\iff \quad y = x - 2 \text{ und } 2x^2 + (-2u - 2v - 4)x + (u^2 + v^2 + 4v - w + 4) = 0.
\end{aligned}$$

Die Diskriminante der quadratischen Gleichung (in x) $2x^2 + (-2u - 2v - 4)x + (u^2 + v^2 + 4v - w + 4) = 0$ ist

$$\begin{aligned}
f(u, v, w) &= (-2u - 2v - 4)^2 - 4 \cdot 2 \cdot (u^2 + v^2 + 4v - w + 4) = \\
&= -4u^2 + 8uv - 4v^2 + 16u - 16v + 8w - 16.
\end{aligned}$$

Ist $f(u, v, w) > 0$, so scheiden sich Gerade und Kreis in zwei Punkten, ist $f(u, v, w) = 0$, so gibt es genau einen Schnittpunkt, ist $f(u, v, w) < 0$, so gibt es überhaupt keine Schnittpunkte.
Wann berührt der Kreis $K_r(u, v)$ die Gerade $y = x - 2$? Genau dann, wenn sich Kreis und Gerade in genau einem Punkt schneiden (Achtung: Dies ist eine spezielle Eigenschaft von Kreisen und gilt nicht allgemein!), d.h. wenn gilt

$$f(u, v, w) = -4u^2 + 8uv - 4v^2 + 16u - 16v + 8w - 16 = 0.$$

- – Ein Punkt (x, y) liegt genau dann im Durchschnitt der Geraden $y = -2x+1$ mit dem Kreis $K_r(u, v)$ (mit $w = r^2$), wenn gilt

$$\begin{aligned}
&\iff \quad y = -2x + 1 \text{ und } (x-u)^2 + (y-v)^2 = w \quad \iff \\
&\iff \quad y = -2x + 1 \text{ und } (x-u)^2 + (-2x+1-v)^2 = w \quad \iff \\
&\iff \quad y = -2x + 1 \text{ und } 5x^2 + (-2u+4v-4)x + (u^2+v^2-2v-w+1) = 0.
\end{aligned}$$

  Die Diskriminante der quadratischen Gleichung $5x^2+(-2u+4v-4)x+(u^2+v^2-2v-w+1) = 0$ ist

$$g(u, v, w) = -16u^2 - 16uv - 4v^2 + 16u + 8v + 20w - 4.$$

  Wie eben folgt, dass die Gerade $y = -2x + 1$ genau dann den Kreis $K_r(u, v)$ (mit $w = r^2$) berührt, wenn

$$g(u, v, w) = -16u^2 - 16uv - 4v^2 + 16u + 8v + 20w - 4 = 0$$

  gilt.
- – Ein Punkt (x, y) liegt genau dann im Durchschnitt der Geraden $y = 1$ mit dem Kreis $K_r(u, v)$ (mit $w = r^2$), wenn gilt

$$\begin{aligned}
&\iff \quad y = 1 \text{ und } (x-u)^2 + (y-v)^2 = w \quad \iff \\
&\iff \quad y = 1 \text{ und } (x-u)^2 + (1-v)^2 = w \quad \iff \\
&\iff \quad y = 1 \text{ und } x^2 - 2ux + (u^2+v^2-2v-w+1) = 0.
\end{aligned}$$

  Die Diskriminante der quadratischen Gleichung $x^2 - 2ux + (u^2 + v^2 - 2v - w + 1) = 0$ ist

$$h(u, v, w) = -4v^2 + 8v + 4w - 4.$$

  Wie oben folgt, dass die Gerade $y = 1$ genau dann den Kreis $K_r(u, v)$ (mit $w = r^2$) berührt, wenn gilt

$$h(u, v, w) = -4v^2 + 8v + 4w - 4 = 0.$$

- Damit erhalten wir: Ein Kreis $K_r(u, v)$ (mit $w = r^2$) berührt genau dann alle drei gegebenen Geraden, wenn folgende Gleichungen erfüllt sind:

$$\begin{aligned}
f(u, v, w) &= -4u^2 + 8uv - 4v^2 + 16u - 16v + 8w - 16 = 0, \\
g(u, v, w) &= -16u^2 - 16uv - 4v^2 + 16u + 8v + 20w - 4 = 0, \\
h(u, v, w) &= -4v^2 + 8v + 4w - 4 = 0.
\end{aligned}$$

  Wir haben die Aufgabenstellung jetzt also auf das Lösen der drei Gleichungen in u, v, w zurückgeführt.
- Wir wollen jetzt die Lösungen des Gleichungssystems $f(u, v, w) = g(u, v, w) = h(u, v, w) = 0$ in u, v, w bestimmen. Wegen

$$h(u, v, w) = 0 \quad \iff \quad w = v^2 - 2v + 1$$

  definieren wir

$$\begin{aligned}
F(u, v) &= \frac{1}{4} f(u, v, v^2 - 2v + 1) = -u^2 + 2uv + v^2 + 4u - 8v - 2, \\
G(u, v) &= \frac{1}{16} g(u, v, v^2 - 2v + 1) = -u^2 - uv + v^2 + u - 2v + 1,
\end{aligned}$$

  denn dann gilt

$$f(u, v, w) = g(u, v, w) = h(u, v, w) = 0 \quad \iff \quad w = v^2 - 2v + 1 \text{ und } F(u, v) = G(u, v) = 0.$$

- Wir wollen nun $F(u,v) = G(u,v) = 0$ lösen. Es gilt:

$$\begin{aligned}
& F(u,v) = G(u,v) = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & F(u,v) = 0 \text{ und } \frac{1}{3}(G(u,v) - F(u,v)) = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & -u^2 + 2uv + v^2 + 4u - 8v - 2 = 0 \text{ und } -uv - u + 2v + 1 = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & -u^2 - 2uv - v^2 + 4u - 8v - 2 = 0 \text{ und } (2-u)v = u - 1 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & v = \frac{u-1}{2-u} \text{ und } -u^2 - 2uv - v^2 + 4u - 8v - 2 = 0 \text{ und } u \neq 2 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & v = \frac{u-1}{2-u} \text{ und } -\frac{u^4 - 6u^3 + 7u^2 + 6u - 9}{(u-2)^2} = 0 \text{ und } u \neq 2 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & v = \frac{u-1}{2-u} \text{ und } u^4 - 6u^3 + 7u^2 + 6u - 9 = 0.
\end{aligned}$$

- Verwenden wir nun $w = v^2 - 2v + 1$, so folgt schließlich

$$\begin{aligned}
& f(u,v,w) = g(u,v,w) = h(u,v,w) = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & u^4 - 6u^3 + 7u^2 + 6u - 9 = 0, \quad v = \frac{u-1}{2-u}, \quad w = (\frac{2u-3}{u-2})^2.
\end{aligned}$$

- Die Gleichung für u können wir numerisch lösen und erhalten dann folgende vier Lösungen:

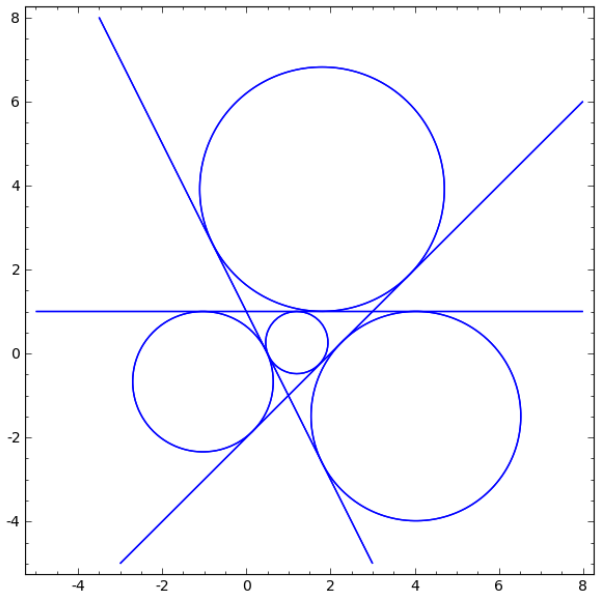
i	u_i	v_i	w_i	r_i
1	-1.03	-0.67	2.79	1.67
2	1.20	0.26	0.55	0.74
3	1.80	3.91	8.45	2.91
4	4.03	-1.49	6.21	2.49

Die vier Kreise $K_{r_i}(u_i, v_i)$ berühren also alle drei Geraden.

Mit SAGE kann man u_i, v_i, w_i, r_i wie folgt finden:

```
var("u")
f=u^4-6*u^3+7*u^2+6*u-9
U=f.roots(ring=RR)
for u,_ in U:
  v=(u-1)/(2-u)
  w=((2*u-3)/(u-2))^2
  r=w^0.5
  print(u,v,w,r)
```

-

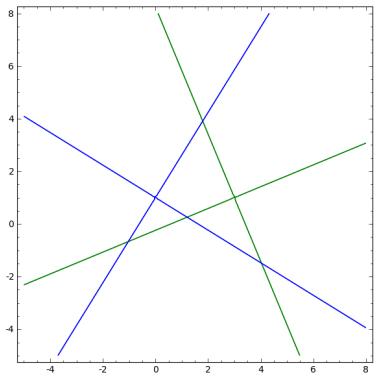


Wir haben also ein geometrisches Problem in die Algebra übersetzt, die entsprechenden Gleichungen manipuliert und gelöst. Als Ergebnis erhalten wir vier Kreise.

- Wir kommen nochmals zurück zu den Gleichungen $F(u,v) = G(u,v) = 0$, d.h.

$$-u^2 + 2uv + v^2 + 4u - 8v - 2 = 0 \text{ und } -u^2 - uv + v^2 + u - 2v + 1 = 0.$$

Wir lassen die Kurven zeichnen und erhalten folgendes Bild:



Dies legt die Vermutung nahe, dass es sich bei beiden Gleichungen um Geradenpaare handelt.

- Durch Probieren findet man die Zerlegungen

$$\begin{aligned} F(u,v) &= -u^2 + 2uv + v^2 + 4u - 8v - 2 = \\ &= (v + u - 4 + \sqrt{2}(u-3))(v + u - 4 - \sqrt{2}(u-3)) \\ G(u,v) &= -u^2 - uv + v^2 + u - 2v + 1 = \\ &= (v - \frac{1}{2}u - 1 + \frac{1}{2}\sqrt{5}u)(v - \frac{1}{2}u - 1 - \frac{1}{2}\sqrt{5}u) \end{aligned}$$

Die Schnittpunkte lassen sich hier natürlich sofort direkt ausrechnen:

$$\begin{aligned} u_1 &= \frac{3}{2} - \sqrt{2} - \frac{1}{2}\sqrt{5}, & v_1 &= \frac{1}{2} - \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{5} - \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_1 &= \frac{9}{2} - 2\sqrt{2} + \frac{1}{2}\sqrt{5}, \\ u_2 &= \frac{3}{2} - \sqrt{2} + \frac{1}{2}\sqrt{5}, & v_2 &= \frac{1}{2} - \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{5} + \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_2 &= \frac{9}{2} - 2\sqrt{2} - \frac{1}{2}\sqrt{5}, \\ u_3 &= \frac{3}{2} + \sqrt{2} - \frac{1}{2}\sqrt{5}, & v_3 &= \frac{1}{2} + \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{5} + \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_3 &= \frac{9}{2} + 2\sqrt{2} + \frac{1}{2}\sqrt{5}, \\ u_4 &= \frac{3}{2} + \sqrt{2} + \frac{1}{2}\sqrt{5}, & v_4 &= \frac{1}{2} + \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{5} - \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_4 &= \frac{9}{2} + 2\sqrt{2} - \frac{1}{2}\sqrt{5}. \end{aligned}$$

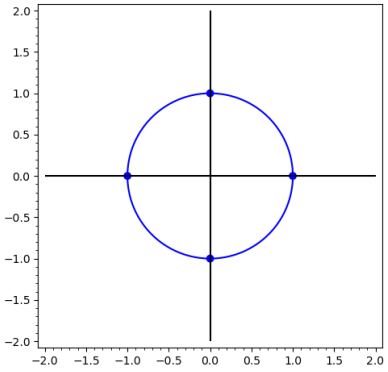
(Die Nummerierung ist so gewählt, dass es zu den nummerischen Lösungen passt.)

2. Rationale Kreispunkte

Rationale Punkte auf dem Einheitskreis: Wir suchen nach Punkten (x,y) des Einheitskreises mit rationalen Koeffizienten, d.h. Lösungen der Gleichung

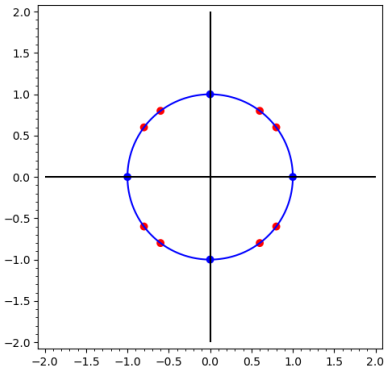
$$x^2 + y^2 = 1 \quad \text{mit} \quad x, y \in \mathbb{Q}.$$

Es gibt einige „triviale“ Lösungen der Gleichung, beispielsweise $(1,0),(-1,0),(0,1),(0,-1)$.



Gibt es weitere Punkte? Bekanntlich gilt $3^2+4^2=5^2$, woraus sich $(\frac{3}{5})^2+(\frac{4}{5})^2=1$ ergibt. Also ist $(\frac{3}{5},\frac{4}{5})$ ein rationaler Kreispunkt. Aus Symmetriegründen erhält man dann gleich folgende rationale Kreispunkte:

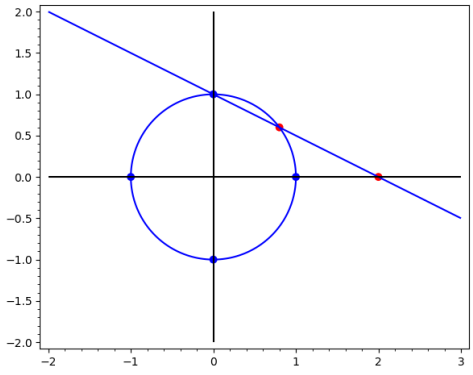
$$(\frac{3}{5},\frac{4}{5}),(\frac{3}{5},-\frac{4}{5}),(-\frac{3}{5},\frac{4}{5}),(-\frac{3}{5},-\frac{4}{5}),(\frac{4}{5},\frac{3}{5}),(\frac{4}{5},-\frac{3}{5}),(-\frac{4}{5},\frac{3}{5}),(-\frac{4}{5},-\frac{3}{5}).$$



Gibt es weitere rationale Punkte auf dem Einheitskreis?

Eine geometrische Idee:

- Wir starten mit dem Punkt $(0,1)$. Sei (x_0,y_0) irgendein, von $(0,1)$ verschiedener Kreispunkt. Wir legen eine Gerade durch $(0,1)$ und (x_0,y_0):



  Setzen wir zusätzlich $x_0\neq 0$, also $(x_0,y_0)\neq(0,-1)$ voraus, so wird die Gerade durch folgende Gleichung beschrieben:

$$\frac{y-1}{x-0}=\frac{y_0-1}{x_0-0},$$

  also

$$y=\frac{y_0-1}{x_0}x+1.$$

- Den Schnittpunkt mit der x-Achse erhalten wir, wenn wir $y = 0$ setzen und nach x auflösen:

$$0 = \frac{y_0 - 1}{x_0} x + 1 \quad \Longleftrightarrow \quad \frac{y_0 - 1}{x_0} x = -1 \quad \Longleftrightarrow \quad x = \frac{x_0}{1 - y_0}.$$

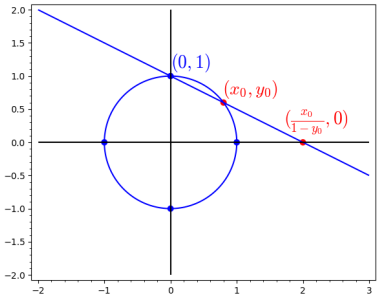
Die Gerade schneidet die x-Achse also im Punkt

$$(\frac{x_0}{1 - y_0}, 0).$$

Wir ordnen jetzt jedem von $(0, 1)$ verschiedenen Punkt des Kreises die x-Koordinate des Schnittpunkts der Verbindungsgeraden zu:

$$(x_0, y_0) \mapsto \frac{x_0}{1 - y_0}.$$

(Diese Abbildung funktioniert auch für $(x_0, y_0) = (0, -1)$.)



- Wir nehmen nun umgekehrt irgendeinen Punkt $(t, 0)$ der x-Achse und bestimmen die Gerade durch die Punkte $(0, 1)$ und $(t, 0)$, wobei wir zunächst $t \neq 0$ voraussetzen:

$$\frac{y - 1}{x - 0} = \frac{1 - 0}{0 - t} = -\frac{1}{t}$$

oder

$$y = -\frac{1}{t} x + 1.$$

Wir bemerken, dass gilt

$$t = -\frac{x}{y - 1} = \frac{x}{1 - y}.$$

Nun bestimmen wir den zweiten Schnittpunkt der Geraden mit dem Einheitskreis.

Dazu setzen wir die Geradengleichung in die Kreisgleichung ein:

$$\begin{aligned} x^2 + \left(-\frac{1}{t} x + 1\right)^2 = 1 \quad &\Longleftrightarrow \quad x^2 + \frac{1}{t^2} x^2 - \frac{2}{t} x + 1 = 1 \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \left(1 + \frac{1}{t^2}\right) x^2 = \frac{2}{t} x \quad \overset{x \neq 0}{\Longleftrightarrow} \\ &\Longleftrightarrow \quad \left(1 + \frac{1}{t^2}\right) x = \frac{2}{t} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad x = \frac{\frac{2}{t}}{1 + \frac{1}{t^2}} = \frac{2t}{t^2 + 1}. \end{aligned}$$

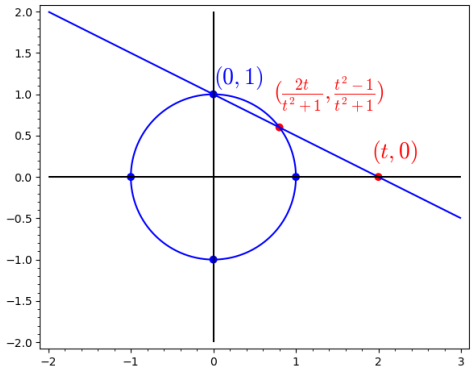
- Den zugehörigen y-Wert erhalten wir, wenn wir den x-Wert in die Geradengleichung einsetzen:

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

Wir erhalten also als Schnittpunkt

$$(x, y) = \left(\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1}\right).$$

(Diese Gleichung gilt auch für $t = 0$.)



Mit Hilfe unserer geometrischen Überlegungen haben wir die Kreispunkte parametrisiert. Wir formulieren das Ergebnis als Satz:

SATZ. *Die Abbildung*

$$\lambda : \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : x^2 + y^2 = 1\} \setminus \{(0, 1)\} \to \mathbb{Q}, \quad (x, y) \mapsto \frac{x}{1 - y}$$

ist bijektiv mit der Umkehrabbildung

$$\mu : \mathbb{Q} \to \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : x^2 + y^2 = 1\} \setminus \{(0, 1)\}, \quad t \mapsto (\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1}).$$

(Wir verzichten hier auf einen rein algebraischen Beweis.)

Der Satz erlaubt es, beliebig viele rationale Punkte auf dem Einheitskreis anzugeben. Hier sind ein paar Beispiele.

Beispiele:

t	0	1	-1	2	3	4	5
$\mu(t)$	$(0, -1)$	$(1, 0)$	$(-1, 0)$	$(\frac{4}{5}, \frac{3}{5})$	$(\frac{3}{5}, \frac{4}{5})$	$(\frac{8}{17}, \frac{15}{17})$	$(\frac{5}{13}, \frac{12}{13})$

Wir können nun auch die im 1. Quadranten gelegenen rationalen Kreispunkte, d.h. die Punkte

$$(x, y) \text{ mit } x^2 + y^2 = 1 \text{ und } x, y \in \mathbb{Q}_{>0}$$

gut beschreiben:

FOLGERUNG. *Die Punkte (x, y) mit $x, y \in \mathbb{Q}_{>0}$ und $x^2 + y^2 = 1$ lassen sich durch die rationalen Zahlen > 1 parametrisieren. Genauer:*

$$\begin{array}{rcl} \{(x, y) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} : x^2 + y^2 = 1\} & \simeq & \mathbb{Q}_{>1} \\ (x, y) & \longmapsto & \dfrac{x}{1 - y} \\ (\dfrac{2t}{t^2 + 1}, \dfrac{t^2 - 1}{t^2 + 1}) & \longleftarrow & t \end{array}$$

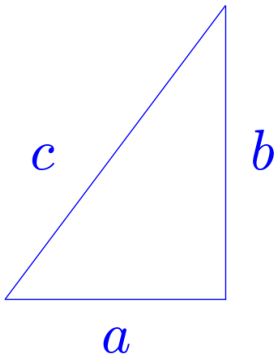
Dabei sind die angegebenen Abbildungen invers zueinander.

3. Pythagoreische Tripel

Pythagoreische Tripel: Ein **pythagoreisches Tripel** ist ein Tripel (a, b, c) natürlicher Zahlen $a, b, c \in \mathbb{N}$, wenn gilt:

$$a^2 + b^2 = c^2,$$

d.h. wenn a, b, c die Seitenlängen eines rechtwinkligen Dreiecks sind (Satz des Pythagoras). Manchmal spricht man dann auch von einem pythagoreischen Dreieck.



Ein pythagoreisches Tripel (a, b, c) nennt man **primitiv**, wenn gilt $\mathrm{ggT}(a, b, c) = 1$. Ein bekanntes Beispiel ist

$$(3, 4, 5).$$

Ist (a, b, c) ein pythagoreisches Tripel und $k \in \mathbb{N}$, so folgt aus

$$(ka)^2 + (kb)^2 = (kc)^2,$$

dass auch (ka, kb, kc) ein pythagoreisches Tripel ist. Man kann sich überlegen, dass sich alle pythagoreische Tripel auf diese Weise aus primitiven pythagoreischen Tripeln ergeben.
Sei nun (a, b, c) ein pythagoreisches Tripel. Dann folgt aus $a^2 + b^2 = c^2$ natürlich $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$. Also ist $(\frac{a}{c}, \frac{b}{c})$ ein im 1. Quadranten gelegener rationaler Punkt des Einheitskreises. Nach der Folgerung gibt es also einen Parameter $t \in \mathbb{Q}_{>1}$, sodass gilt

$$\frac{a}{c} = \frac{2t}{t^2+1}, \quad \frac{b}{c} = \frac{t^2-1}{t^2+1}.$$

Der Parameter ist

$$t = \frac{\frac{a}{c}}{1 - \frac{b}{c}} = \frac{a}{c-b}.$$

Schreiben wir $t = \frac{m}{n}$ mit $m, n \in \mathbb{N}$, $m > n$, $\mathrm{ggT}(m, n) = 1$, so gilt

$$\frac{a}{c} = \frac{2 \cdot \frac{m}{n}}{(\frac{m}{n})^2 + 1} = \frac{2mn}{m^2+n^2}, \quad \frac{b}{c} = \frac{(\frac{m}{n})^2 - 1}{(\frac{m}{n})^2 + 1} = \frac{m^2-n^2}{m^2+n^2}.$$

Anders geschrieben:

$$a = 2mn \cdot \frac{c}{m^2+n^2}, \quad b = (m^2-n^2) \cdot \frac{c}{m^2+n^2}, \quad c = (m^2+n^2) \cdot \frac{c}{m^2+n^2}.$$

- Ist m oder n gerade, wählt man $c = m^2 + n^2$, so erhält man das Tripel
$$(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2).$$
- Sind m und n ungerade Zahlen, wählt man $c = \frac{m^2+n^2}{2}$, so ist c eine natürliche Zahl und man erhält das Tripel
$$(a, b, c) = (mn, \frac{m^2-n^2}{2}, \frac{m^2+n^2}{2}).$$

Man kann beweisen, was wir hier nicht tun wollen, dass man auf diese Weise alle primitiven pythagoreischen Tripel erhält:

SATZ (Beschreibung aller primitiven pythagoreischen Tripel). *Sei*

$$P = \{(a,b,c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} : a^2 + b^2 = c^2, \mathrm{ggT}(a,b,c) = 1\}$$

die Menge der primitiven pythagoreischen Tripel. Dann ist die Abbildung

$$\alpha : P \to \mathbb{Q}_{>1}, \quad (a,b,c) \mapsto \frac{a}{c-b}$$

bijektiv mit der Umkehrabbildung

$$\beta : \mathbb{Q}_{>1} \to P, \quad \frac{m}{n} \mapsto \begin{cases} (2mn, m^2-n^2, m^2+n^2), & \text{falls } m,n \in \mathbb{N}, m > n, \mathrm{ggT}(m,n) = 1, \\ & m \text{ oder } n \text{ gerade}, \\ (mn, \frac{m^2-n^2}{2}, \frac{m^2+n^2}{2}), & \text{falls } m,n \in \mathbb{N}, m > n, \mathrm{ggT}(m,n) = 1, \\ & m \text{ und } n \text{ ungerade}. \end{cases}$$

Beispiele: Hier sind alle primitiven pythagoreischen Tripel (a,b,c) mit $c \leq 100$. Es gibt 32 Stück.

(a,b,c)	$\alpha((a,b,c)) = \frac{a}{c-b} = \frac{m}{n}$
$(3,4,5)$	3
$(4,3,5)$	2
$(5,12,13)$	5
$(12,5,13)$	$\frac{3}{2}$
$(8,15,17)$	4
$(15,8,17)$	$\frac{5}{3}$
$(7,24,25)$	7
$(24,7,25)$	$\frac{4}{3}$
$(20,21,29)$	$\frac{5}{2}$
$(21,20,29)$	$\frac{7}{3}$
$(12,35,37)$	6
$(35,12,37)$	$\frac{7}{5}$
$(9,40,41)$	9
$(40,9,41)$	$\frac{5}{4}$
$(28,45,53)$	$\frac{7}{2}$
$(45,28,53)$	$\frac{9}{5}$

(a,b,c)	$\alpha((a,b,c)) = \frac{a}{c-b} = \frac{m}{n}$
$(11,60,61)$	11
$(60,11,61)$	$\frac{6}{5}$
$(16,63,65)$	8
$(33,56,65)$	$\frac{11}{3}$
$(56,33,65)$	$\frac{7}{4}$
$(63,16,65)$	$\frac{9}{7}$
$(48,55,73)$	$\frac{8}{3}$
$(55,48,73)$	$\frac{11}{5}$
$(13,84,85)$	13
$(36,77,85)$	$\frac{9}{2}$
$(77,36,85)$	$\frac{11}{7}$
$(84,13,85)$	$\frac{7}{6}$
$(39,80,89)$	$\frac{13}{3}$
$(80,39,89)$	$\frac{8}{5}$
$(65,72,97)$	$\frac{13}{5}$
$(72,65,97)$	$\frac{9}{4}$

Nun haben wir für alle rationalen Zahlen $\frac{m}{n} \in \mathbb{Q}_{>1}$ mit $\mathrm{ggT}(m,n) = 1$ und $m \leq 10$ die zugehörigen Tripel bestimmt:

$\frac{m}{n}$	$\beta(\frac{m}{n})$
2	$(4,3,5)$
3	$(3,4,5)$
$\frac{3}{2}$	$(12,5,13)$
4	$(8,15,17)$
$\frac{4}{3}$	$(24,7,25)$
5	$(5,12,13)$
$\frac{5}{2}$	$(20,21,29)$
$\frac{5}{3}$	$(15,8,17)$
$\frac{5}{4}$	$(40,9,41)$
6	$(12,35,37)$
$\frac{6}{5}$	$(60,11,61)$
7	$(7,24,25)$
$\frac{7}{2}$	$(28,45,53)$
$\frac{7}{3}$	$(21,20,29)$
$\frac{7}{4}$	$(56,33,65)$
$\frac{7}{5}$	$(35,12,37)$

$\frac{m}{n}$	$\beta(\frac{m}{n})$
$\frac{7}{6}$	$(84,13,85)$
8	$(16,63,65)$
$\frac{8}{3}$	$(48,55,73)$
$\frac{8}{5}$	$(80,39,89)$
$\frac{8}{7}$	$(112,15,113)$
9	$(9,40,41)$
$\frac{9}{2}$	$(36,77,85)$
$\frac{9}{4}$	$(72,65,97)$
$\frac{9}{5}$	$(45,28,53)$
$\frac{9}{7}$	$(63,16,65)$
$\frac{9}{8}$	$(144,17,145)$
10	$(20,99,101)$
$\frac{10}{3}$	$(60,91,109)$
$\frac{10}{7}$	$(140,51,149)$
$\frac{10}{9}$	$(180,19,181)$

Die vorangegangenen Überlegungen hatten mit der Kurve $x^2 + y^2 = 1$ zu tun. Durch die angegebene Parametrisierung sieht man, dass es unendlich viele rationale Punkte auf dieser Kurve gibt. Dies ändert sich, wenn man den Exponenten 2 durch eine größere Zahl ersetzt.

Die Fermat-Gleichung: Für $n \geq 3$ hat die Gleichung

$$a^n + b^n = c^n \quad \text{mit} \quad a,b,c \in \mathbb{N}$$

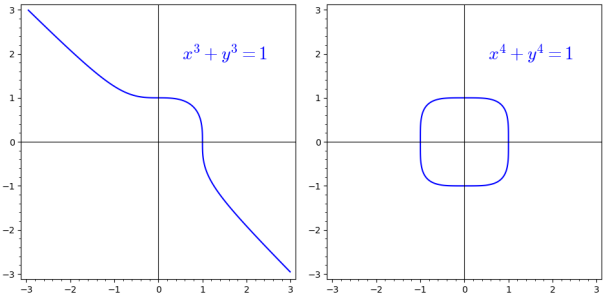
keine Lösung. Dies wurde von Fermat behauptet, von Wiles (1995) bewiesen. (Der Beweis ist nichttrivial.) Gilt $a^n + b^n = c^n$, so folgt $(\frac{a}{c})^n + (\frac{b}{c})^n = 1$, also hat man das Problem, nach rationalen Punkten (Punkten mit rationalen Koordinaten) auf der Kurve

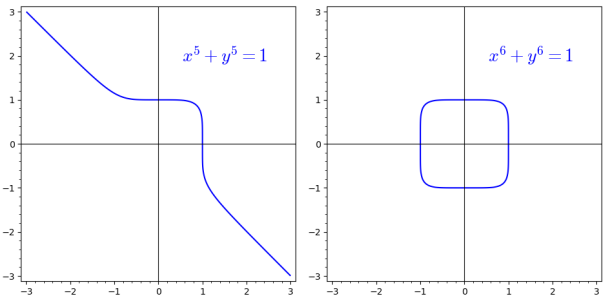
$$x^n + y^n = 1$$

zu suchen. Es wurde bewiesen, dass es nur die folgenden trivialen Lösungen gibt:

$$\begin{cases} (1,0),(-1,0),(0,1),(0,-1) & \text{für gerades } n, \\ (1,0),(0,1) & \text{für ungerades } n. \end{cases}$$

Die folgenden Bilder zeigen die reellen Kurven für einige n.

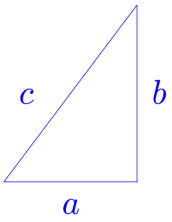




4. Kongruenzzahlen

Kongruenzzahlen: Eine natürliche Zahl N heißt **Kongruenzzahl**, wenn sie Flächeneinhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen ist, d.h. wenn es $a, b, c \in \mathbb{Q}_{>0}$ gibt mit

$$N = \frac{1}{2}ab \quad \text{und} \quad a^2 + b^2 = c^2.$$



Beispielsweise ist 6 eine Kongruenzzahl, weil $6 = \frac{1}{2} \cdot 3 \cdot 4$ und $3^2 + 4^2 = 5^2$ gilt.
Ist N eine Kongruenzzahl mit $N = \frac{1}{2}ab$ und $a^2 + b^2 = c^2$, sind $r, s \in \mathbb{N}$, so gilt $N\frac{r^2}{s^2} = \frac{1}{2} \cdot \frac{r}{s}a \cdot \frac{r}{s}b$ und $(\frac{r}{s}a)^2 + (\frac{r}{s}b)^2 = (\frac{r}{s}c)^2$. Ist also $N\frac{r^2}{s^2} \in \mathbb{N}$, so ist dies ebenfalls eine Kongruenzzahl.
Daher kann man sich auf die Betrachtung quadratfreier Zahlen beschränken.

Bemerkung: Eine natürliche Zahl n nennt man **quadratfrei**, wenn sie nicht durch das Quadrat einer Primzahl p teilbar ist. Jede natürlich Zahl $n \in \mathbb{N}$ lässt sich eindeutig zerlegen

$$n = k^2\ell \text{ mit } k, \ell \in \mathbb{N}, \ell \text{ quadratfrei.}$$

Man nennt ℓ auch den quadratfreien Anteil von n (SAGE: `squarefree_part`). Ein paar Beispiele:

$$\begin{aligned}
&1 = 1^2 \cdot 1, \quad 2 = 1^2 \cdot 2, \quad 3 = 1^2 \cdot 2, \quad 4 = 2^2 \cdot 1, \quad 5 = 1^2 \cdot 5,\\
&6 = 1^2 \cdot 6, \quad 7 = 1^2 \cdot 7, \quad 8 = 2^2 \cdot 2,\\
&12 = 2^2 \cdot 3, \quad 18 = 3^2 \cdot 2, \quad 20 = 2^2 \cdot 5, \quad 24 = 2^2 \cdot 6, \quad 27 = 3^2 \cdot 3,\\
&28 = 2^2 \cdot 7, \quad 32 = 2^4 \cdot 2, \quad \ldots
\end{aligned}$$

Unsere Beschreibung der rationalen Punkte des Einheitskreises führt nun zu einer Beschreibung der Kongruenzzahlen:

SATZ.

- *Ist N eine quadratfreie Kongruenzzahl, so gibt es $m, n, k \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$, $m > n$ und*
$$N = \frac{(m^2 - n^2)mn}{k^2}.$$
- *Sind $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$ und $m > n$ und zerlegt man $(m^2 - n^2)mn$ in ein Quadrat k^2 und einen quadratfreien Teil N, also*
$$(m^2 - n^2)mn = Nk^2,$$
so ist N eine quadratfreie Kongruenzzahl. Ein zugehöriges rechtwinkliges Dreieck mit passenden Seitenlängen wird gegeben durch
$$a = \frac{2mn}{k}, \quad b = \frac{m^2 - n^2}{k}, \quad c = \frac{m^2 + n^2}{k}.$$

Beweis:

- Sei N eine Kongruenzzahl, d.h. $N = \frac{1}{2}ab$ und $a^2 + b^2 = c^2$ mit $a, b, c \in \mathbb{Q}_{>0}$. Dann ist $(\frac{a}{c}, \frac{b}{c})$ ein rationaler Kreispunkt im 1. Quadranten, es gibt also $m, n \in \mathbb{N}$ mit $m > n$, $\mathrm{ggT}(m, n) = 1$ und

$$\frac{a}{c} = \frac{2mn}{m^2 + n^2}, \quad \frac{b}{c} = \frac{m^2 - n^2}{m^2 + n^2},$$

also

$$a = 2mn \cdot \frac{c}{m^2 + n^2}, \quad b = (m^2 - n^2) \cdot \frac{c}{m^2 + n^2}.$$

Dann ist

$$N = \frac{1}{2}ab = \frac{1}{2} \cdot 2mn \cdot \frac{c}{m^2 + n^2} \cdot (m^2 - n^2) \cdot \frac{c}{m^2 + n^2} = mn(m^2 - n^2) \cdot \left(\frac{c}{m^2 + n^2}\right)^2.$$

Wir schreiben

$$\frac{c}{m^2 + n^2} = \frac{\ell}{k} \text{ mit } \ell, k \in \mathbb{N}, \mathrm{ggT}(\ell, k) = 1$$

und erhalten dann

$$N = mn(m^2 - n^2) \cdot \frac{\ell^2}{k^2}, \quad \text{also} \quad Nk^2 = mn(m^2 - n^2) \cdot \ell^2.$$

Da N quadratfrei sein soll, folgt aus $\mathrm{ggT}(k, \ell) = 1$ sofort $\ell = 1$, und damit

$$Nk^2 = mn(m^2 - n^2).$$

Es ist dann

$$\frac{c}{m^2 + n^2} = \frac{1}{k},$$

woraus sich

$$a = \frac{2mn}{k}, \quad b = \frac{m^2 - n^2}{k}, \quad c = \frac{m^2 + n^2}{k}$$

ergibt.

- Man sieht, dass $a^2 + b^2 = c^2$, $a, b, c \in \mathbb{Q}_{>0}$ und $N = \frac{1}{2}ab$ gilt. Nach Konstruktion ist N quadratfrei, was dann die Behauptung beweist. ■

Bemerkung: Mit dem vorangegangenen Satz kann man Kongruenzahlen konstruieren: Man lässt m und n laufen (mit $m > n$ und $\mathrm{ggT}(m, n) = 1$), zerlegt $mn(m^2 - n^2) = Nk^2$ mit quadratfreiem N. Dann ist N eine Kongruenzzahl.

Beispiel: Wir wählen $m = 2021$ und $n = 1000$. Dann gilt mit den Bezeichnungen des vorangegangenen Satzes

$$\begin{aligned} Nk^2 &= mn(m^2 - n^2) = 6233655261000 = 2^3 \cdot 3 \cdot 5^3 \cdot 19 \cdot 43 \cdot 47 \cdot 53 \cdot 1021 = \\ &= (2 \cdot 3 \cdot 5 \cdot 19 \cdot 43 \cdot 47 \cdot 53 \cdot 1021) \cdot (2 \cdot 5)^2 = 62336552610 \cdot 10^2. \end{aligned}$$

Daher ist

$$N = 62336552610$$

eine (quadratfreie) Kongruenzzahl. Ein zugehöriges rechtwinkliges Dreieck mit Flächeninhalt N hat die Seitenlängen

$$a = \frac{2mn}{k} = 404200, \quad b = \frac{m^2 - n^2}{k} = \frac{3084441}{10}, \quad c = \frac{m^2 + n^2}{k} = \frac{5084441}{10}.$$

Beispiele: Nach dem eben beschriebenen Verfahren haben wir m bis 10000 laufen lassen. Dabei wurden folgende quadratfreien Kongruenzzahlen $N \leq 50$ gefunden:

N	(a,b,c)	m	n	k
5	$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$	2401	961	1494696
5	$\left(\frac{20}{3}, \frac{3}{2}, \frac{41}{6}\right)$	5	4	6
5	$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$	9	1	12
5	$\left(\frac{4920}{1519}, \frac{1519}{492}, \frac{3344161}{747348}\right)$	1681	720	747348
6	$(3,4,5)$	3	1	2
6	$(4,3,5)$	2	1	1
6	$\left(\frac{120}{7}, \frac{7}{10}, \frac{1201}{70}\right)$	25	24	70
6	$\left(\frac{3404}{1551}, \frac{4653}{851}, \frac{7776485}{1319901}\right)$	2738	529	1319901
6	$\left(\frac{4653}{851}, \frac{3404}{1551}, \frac{7776485}{1319901}\right)$	3267	2209	2639802
6	$\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)$	49	1	140
7	$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$	16	9	60
7	$\left(\frac{35}{12}, \frac{24}{5}, \frac{337}{60}\right)$	25	7	120
13	$\left(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690}\right)$	361	289	19380
13	$\left(\frac{780}{323}, \frac{323}{30}, \frac{106921}{9690}\right)$	325	36	9690
14	$\left(\frac{21}{2}, \frac{8}{3}, \frac{65}{6}\right)$	9	7	12
14	$\left(\frac{21840}{3713}, \frac{3713}{780}, \frac{21914881}{2896140}\right)$	4225	2016	2896140
14	$\left(\frac{3713}{780}, \frac{21840}{3713}, \frac{21914881}{2896140}\right)$	6241	2209	5792280
14	$\left(\frac{8}{3}, \frac{21}{2}, \frac{65}{6}\right)$	8	1	6
15	$\left(4, \frac{15}{2}, \frac{17}{2}\right)$	4	1	2
15	$\left(\frac{15}{2}, 4, \frac{17}{2}\right)$	5	3	4
15	$\left(\frac{161}{68}, \frac{2040}{161}, \frac{141121}{10948}\right)$	529	49	21896
15	$\left(\frac{2040}{161}, \frac{161}{68}, \frac{141121}{10948}\right)$	289	240	10948
21	$\left(12, \frac{7}{2}, \frac{25}{2}\right)$	4	3	2
21	$\left(\frac{4200}{527}, \frac{527}{100}, \frac{503521}{52700}\right)$	625	336	52700
21	$\left(\frac{527}{100}, \frac{4200}{527}, \frac{503521}{52700}\right)$	961	289	105400
21	$\left(\frac{7}{2}, 12, \frac{25}{2}\right)$	7	1	4
22	$\left(\frac{140}{3}, \frac{33}{35}, \frac{4901}{105}\right)$	50	49	105
22	$\left(\frac{33}{35}, \frac{140}{3}, \frac{4901}{105}\right)$	99	1	210

N	(a,b,c)	m	n	k
29	$\left(\frac{52780}{99}, \frac{99}{910}, \frac{48029801}{90090}\right)$	4901	4900	90090
29	$\left(\frac{99}{910}, \frac{52780}{99}, \frac{48029801}{90090}\right)$	9801	1	180180
30	$(12,5,13)$	3	2	1
30	$(5,12,13)$	5	1	2
30	$\left(\frac{119}{26}, \frac{1560}{119}, \frac{42961}{3094}\right)$	289	49	6188
30	$\left(\frac{1560}{119}, \frac{119}{26}, \frac{42961}{3094}\right)$	169	120	3094
31	$\left(\frac{720}{287}, \frac{8897}{360}, \frac{2566561}{103320}\right)$	1600	81	103320
31	$\left(\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320}\right)$	1681	1519	206640
34	$\left(24, \frac{17}{6}, \frac{145}{6}\right)$	9	8	6
34	$\left(\frac{112}{9}, \frac{153}{28}, \frac{3425}{252}\right)$	49	32	252
34	$\left(\frac{136}{15}, \frac{15}{2}, \frac{353}{30}\right)$	17	8	30
34	$\left(\frac{15}{2}, \frac{136}{15}, \frac{353}{30}\right)$	25	9	60
34	$\left(\frac{153}{28}, \frac{112}{9}, \frac{3425}{252}\right)$	81	17	504
34	$\left(\frac{17}{6}, 24, \frac{145}{6}\right)$	17	1	12
34	$\left(\frac{3927}{248}, \frac{992}{231}, \frac{939905}{57288}\right)$	1089	833	114576
34	$\left(\frac{992}{231}, \frac{3927}{248}, \frac{939905}{57288}\right)$	961	128	57288
38	$\left(\frac{1700}{279}, \frac{5301}{425}, \frac{1646021}{118575}\right)$	1250	289	118575
38	$\left(\frac{5301}{425}, \frac{1700}{279}, \frac{1646021}{118575}\right)$	1539	961	237150
39	$\left(\frac{156}{5}, \frac{5}{2}, \frac{313}{10}\right)$	13	12	10
39	$\left(\frac{5}{2}, \frac{156}{5}, \frac{313}{10}\right)$	25	1	20
41	$\left(\frac{1023}{40}, \frac{3280}{1023}, \frac{1054721}{40920}\right)$	1089	961	81840
41	$\left(\frac{1189}{420}, \frac{840}{29}, \frac{354481}{12180}\right)$	841	41	24360
41	$\left(\frac{123}{20}, \frac{40}{3}, \frac{881}{60}\right)$	41	9	120
41	$\left(\frac{3280}{1023}, \frac{1023}{40}, \frac{1054721}{40920}\right)$	1025	64	40920
41	$\left(\frac{40}{3}, \frac{123}{20}, \frac{881}{60}\right)$	25	16	60
41	$\left(\frac{840}{29}, \frac{1189}{420}, \frac{354481}{12180}\right)$	441	400	12180
46	$\left(\frac{168}{11}, \frac{253}{42}, \frac{7585}{462}\right)$	72	49	462
46	$\left(\frac{253}{42}, \frac{168}{11}, \frac{7585}{462}\right)$	121	23	924

Die obige Tabelle enthält nicht alle (quadratfreien) Kongruenzzahlen ≤ 50, es fehlen noch die Zahlen 23, 37, 47. Die folgende Tabelle liefert passende Werte, um auch die Zahlen 23, 37, 47 als Kongruenzzahlen nachzuweisen:

N	m	n
23	24336	17689
37	777925	1764
47	14561856	2289169

Bemerkung: Fermat hat bewiesen, dass 1 und 2 keine Kongruenzzahlen sind.

Bemerkung: Ist N Kongruenzzahl, so kann es mehrere zugehörige rechtwinklige Dreiecke geben. Beispielsweise haben folgende rechtwinkligen Dreiecke alle den Flächeninhalt 6: $(a,b,c) = (3,4,5)$ und $(a,b,c) = (\frac{7}{10}, \frac{120}{7}, \frac{1201}{70})$.

Bemerkung: Der vorangegangene Satz liefert zwar eine Möglichkeit, Kongruenzzahlen zu konstruieren. Man kann mit ihm aber nicht effektiv testen, ob eine gegebene Zahl N eine Kongruenzzahl ist oder nicht.

Der folgende Satz bringt einen neuen Kurventyp ins Spiel:

SATZ. *Für eine natürliche Zahl N gilt die Äquivalenz:*

$$N \text{ ist Kongruenzzahl} \quad \Longleftrightarrow \quad \text{es gibt } x, y \in \mathbb{Q}_{>0} \text{ mit } y^2 = x^3 - N^2 x.$$

Genauer:

- *Ist N eine Kongruenzzahl, (a, b, c) ein zugehöriges rationales rechtwinkliges Dreieck mit Flächeninhalt N, setzt man*
$$x = \frac{Na}{c-b}, \quad y = \frac{2N^2}{c-b},$$
so gilt
$$x, y \in \mathbb{Q}_{>0} \quad \text{und} \quad y^2 = x(x^2 - N^2).$$
- *Ist $(x, y) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ mit*
$$y^2 = x(x^2 - N^2),$$
setzt man
$$a = \frac{2Nx}{y}, \quad b = \frac{x^2 - N^2}{y}, \quad c = \frac{x^2 + N^2}{y},$$
so sind a, b, c die Seiten eines rationalen rechtwinkligen Dreiecks mit Flächeninhalt N, insbesondere ist also N eine Kongruenzzahl.

Man kann die vorangegangenen Punkte auch so zusammenfassen:

- *Sei*
$$D_N = \{(a, b, c) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} : a^2 + b^2 = c^2, N = \frac{1}{2}ab\}$$
und
$$X_N = \{(x, y) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} : y^2 = x^3 - N^2 x\}.$$
Die Abbildung
$$\gamma : D_N \to X_N, \quad (a, b, c) \mapsto (\frac{Na}{c-b}, \frac{2N^2}{c-b})$$
ist bijektiv mit Umkehrabbildung
$$\delta : X_N \to D_N, \quad (x, y) \mapsto (\frac{2Nx}{y}, \frac{x^2 - N^2}{y}, \frac{x^2 + N^2}{y}).$$

Beweis:

- Sei N eine Kongruenzzahl, $a, b, c \in \mathbb{Q}_{>0}$ die Seitenlängen eines zugehörigen rechtwinkligen Dreiecks. Für $t = \frac{a}{c-b}$ gilt dann
$$a = \frac{2t}{t^2+1} \cdot c, \quad b = \frac{t^2-1}{t^2+1} \cdot c$$
und
$$N = \frac{1}{2}ab = \frac{1}{2} \cdot \frac{2t}{t^2+1} \cdot c \cdot \frac{t^2-1}{t^2+1} \cdot c = \frac{t(t^2-1)}{(t^2+1)^2} \cdot c^2.$$
Wir formen die letzte Gleichung äquivalent um:
$$N = \frac{t(t^2-1)}{(t^2+1)^2} \cdot c^2 \quad \Longleftrightarrow \quad N = \frac{N^4 \cdot t(t^2-1)}{N^4(t^2+1)^2} \cdot c^2 = \frac{N \cdot (Nt)((Nt)^2 - N^2)}{((Nt)^2 + N^2)^2} \cdot c^2 \quad \Longleftrightarrow$$
$$\Longleftrightarrow \quad \left(\frac{(Nt)^2 + N^2}{c}\right)^2 = (Nt) \cdot ((Nt)^2 - N^2).$$
Setzen wir
$$x = Nt, \quad y = \frac{(Nt)^2 + N^2}{c},$$
so gilt
$$y^2 = x(x^2 - N^2) \quad \text{und} \quad x \in \mathbb{Q}_{>0}, \quad y \in \mathbb{Q}_{>0}.$$

Wir erhalten damit die Darstellungen

$$\begin{aligned} a &= \frac{2t}{t^2+1}\cdot c = \frac{2N\cdot Nt}{(Nt)^2+N^2}\cdot c = \frac{2Nx}{y}, \\ b &= \frac{t^2-1}{t^2+1}\cdot c = \frac{(Nt)^2-N^2}{(Nt)^2+N^2}\cdot c = \frac{x^2-N^2}{y}, \\ c &= \frac{(Nt)^2+N^2}{y} = \frac{x^2+N^2}{y}. \end{aligned}$$

Mit $t = \frac{a}{c-b}$ gilt weiter

$$\begin{aligned} x &= Nt = \frac{Na}{c-b}, \\ y &= \frac{N^2(t^2+1)}{c} = \frac{N^2((\frac{a}{c-b})^2+1)}{c} = \frac{N^2(a^2+(c-b)^2)}{c(c-b)^2} = \\ &= \frac{N^2(a^2+b^2+c^2-2bc)}{c(c-b)^2} = \frac{N^2(2c^2-2bc)}{c(c-b)^2} = \frac{N^2\cdot 2c(c-b)}{c(c-b)^2} = \\ &= \frac{2N^2}{c-b}. \end{aligned}$$

- Wir rechnen dies direkt nach. Seien also $x, y \in \mathbb{Q}_{>0}$ mit

$$y^2 = x(x^2-N^2) \quad \text{und} \quad a = \frac{2Nx}{y}, \quad b = \frac{x^2-N^2}{y}, \quad c = \frac{x^2+N^2}{y}.$$

Wegen $y > 0$ und $x > 0$ folgt $x^2 - N^2 > 0$ und damit $a, b, c > 0$. Es ist

$$\begin{aligned} a^2+b^2 &= \frac{4N^2x^2+(x^2-N^2)^2}{y^2} = \frac{4N^2x^2+(x^4-2N^2x^2+N^4)}{y^2} = \\ &= \frac{x^4+2N^2x^2+N^4}{y^2} = \frac{(x^2+N^2)^2}{y^2} = c^2 \end{aligned}$$

und

$$\frac{1}{2}ab = \frac{1}{2}\cdot\frac{2Nx}{y}\cdot\frac{x^2-N^2}{y} = \frac{Nx(x^2-N^2)}{y^2} = \frac{Ny^2}{y^2} = N.$$

Dies beweist die Behauptung.

- Dies folgt aus (1) und (2). Man kann dies aber auch eigenständig beweisen. ■

Beispiel: Wir wissen, dass $N = 6$ eine Kongruenzzahl ist. Ein zugehöriges rationales rechtwinkliges Dreieck ist $(a, b, c) = (3, 4, 5)$. Wir berechnen mit den Formeln des Satzes

$$x = \frac{Na}{c-b} = \frac{6\cdot 3}{5-4} = 18, \quad y = \frac{2N^2}{c-b} = \frac{2\cdot 6^2}{5-4} = 72$$

und erhalten damit den Punkt

$$(18, 72)$$

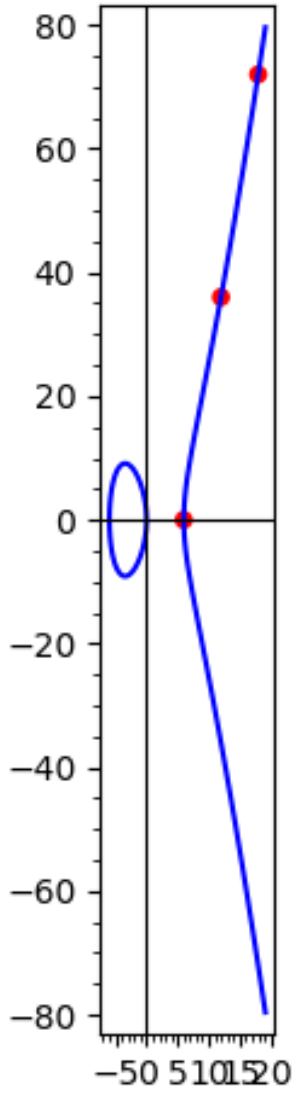
auf der Kurve $y^2 = x^3 - 36x$.
Das Dreieck $(b, a, c) = (4, 3, 5)$ führt zu

$$x = \frac{Na}{c-b} = \frac{6\cdot 4}{5-3} = 12, \quad y = \frac{2N^2}{c-b} = \frac{2\cdot 6^2}{5-3} = 36,$$

also den Kurvenpunkt

$$(12, 36).$$

Das folgende Bild zeigt die Kurve $y^2 = x(x^2 - 36)$ und die Kurvenpunkte $(6, 0)$, $(12, 36)$, $(18, 72)$, die alle auf der Geraden $y = 6(x - 6)$ liegen.



Beispiele: Für die Beispiele von oben haben wir nun den zum Tripel (a,b,c) gehörigen Punkte (x,y) der Kurve $y^2 = x^3 - N^2x$ aufgelistet:

N	(a,b,c)	(x,y)
5	$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$	$\left(\frac{12005}{961}, \frac{1205400}{29791}\right)$
5	$\left(\frac{20}{3}, \frac{3}{2}, \frac{41}{6}\right)$	$\left(\frac{25}{4}, \frac{75}{8}\right)$
5	$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$	$(45, 300)$
5	$\left(\frac{4920}{1519}, \frac{1519}{492}, \frac{3344161}{747348}\right)$	$\left(\frac{1681}{144}, \frac{62279}{1728}\right)$
6	$(3,4,5)$	$(18,72)$
6	$(4,3,5)$	$(12,36)$
6	$\left(\frac{120}{7}, \frac{7}{10}, \frac{1201}{70}\right)$	$\left(\frac{25}{4}, \frac{35}{8}\right)$
6	$\left(\frac{3404}{1551}, \frac{4653}{851}, \frac{7776485}{1319901}\right)$	$\left(\frac{16428}{529}, \frac{2065932}{12167}\right)$
6	$\left(\frac{4653}{851}, \frac{3404}{1551}, \frac{7776485}{1319901}\right)$	$\left(\frac{19602}{2209}, \frac{2021976}{103823}\right)$
6	$\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)$	$(294, 5040)$
7	$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$	$\left(\frac{112}{9}, \frac{980}{27}\right)$
7	$\left(\frac{35}{12}, \frac{24}{5}, \frac{337}{60}\right)$	$(25, 120)$
13	$\left(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690}\right)$	$\left(\frac{4693}{289}, \frac{192660}{4913}\right)$
13	$\left(\frac{780}{323}, \frac{323}{30}, \frac{106921}{9690}\right)$	$\left(\frac{4225}{36}, \frac{272935}{216}\right)$
14	$\left(\frac{21}{2}, \frac{8}{3}, \frac{65}{6}\right)$	$(18,48)$
14	$\left(\frac{21840}{3713}, \frac{3713}{780}, \frac{21914881}{2896140}\right)$	$\left(\frac{4225}{144}, \frac{241345}{1728}\right)$
14	$\left(\frac{3713}{780}, \frac{21840}{3713}, \frac{21914881}{2896140}\right)$	$\left(\frac{87374}{2209}, \frac{24155040}{103823}\right)$
14	$\left(\frac{8}{3}, \frac{21}{2}, \frac{65}{6}\right)$	$(112, 1176)$
15	$\left(4, \frac{15}{2}, \frac{17}{2}\right)$	$(60, 450)$
15	$\left(\frac{15}{2}, 4, \frac{17}{2}\right)$	$(25, 100)$
15	$\left(\frac{161}{68}, \frac{2040}{161}, \frac{141121}{10948}\right)$	$\left(\frac{7935}{49}, \frac{703800}{343}\right)$
15	$\left(\frac{2040}{161}, \frac{161}{68}, \frac{141121}{10948}\right)$	$\left(\frac{289}{16}, \frac{2737}{64}\right)$
21	$\left(12, \frac{7}{2}, \frac{25}{2}\right)$	$(28, 98)$
21	$\left(\frac{4200}{527}, \frac{527}{100}, \frac{503521}{52700}\right)$	$\left(\frac{625}{16}, \frac{13175}{64}\right)$
21	$\left(\frac{527}{100}, \frac{4200}{527}, \frac{503521}{52700}\right)$	$\left(\frac{20181}{289}, \frac{2734200}{4913}\right)$
21	$\left(\frac{7}{2}, 12, \frac{25}{2}\right)$	$(147, 1764)$
22	$\left(\frac{140}{3}, \frac{33}{35}, \frac{4901}{105}\right)$	$\left(\frac{1100}{49}, \frac{7260}{343}\right)$
22	$\left(\frac{33}{35}, \frac{140}{3}, \frac{4901}{105}\right)$	$(2178, 101640)$

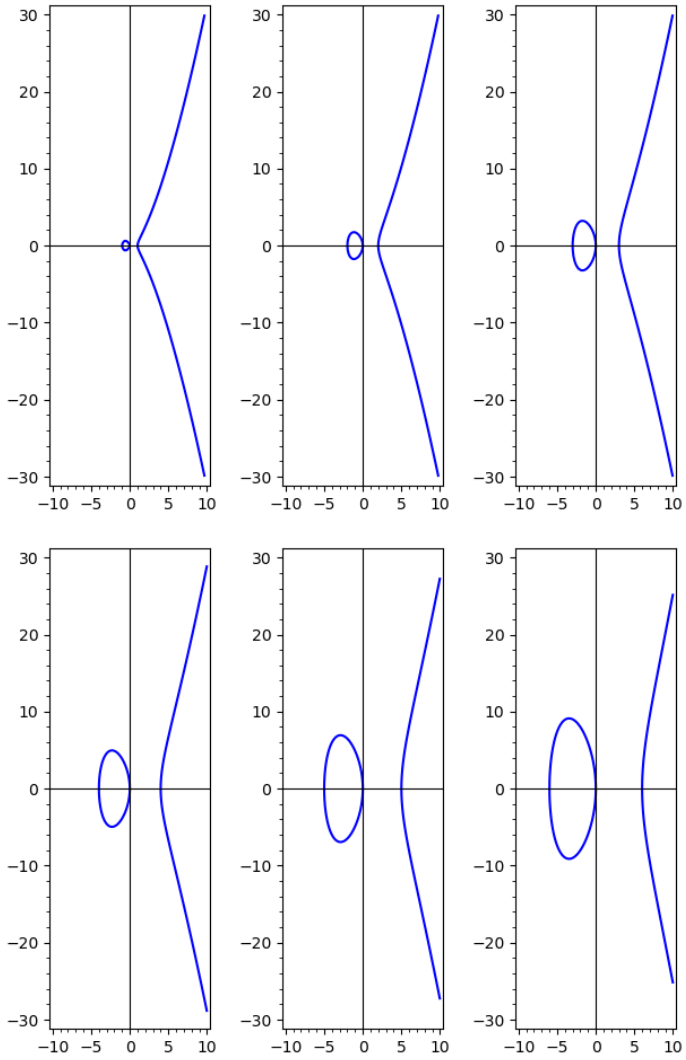
N	(a,b,c)	(x,y)
29	$\left(\frac{52780}{99}, \frac{99}{910}, \frac{48029801}{90090}\right)$	$\left(\frac{142129}{4900}, \frac{1082367}{343000}\right)$
29	$\left(\frac{99}{910}, \frac{52780}{99}, \frac{48029801}{90090}\right)$	$(284229, 151531380)$
30	$(12,5,13)$	$(45, 225)$
30	$(5,12,13)$	$(150, 1800)$
30	$\left(\frac{119}{26}, \frac{1560}{119}, \frac{42961}{3094}\right)$	$\left(\frac{8670}{49}, \frac{795600}{343}\right)$
30	$\left(\frac{1560}{119}, \frac{119}{26}, \frac{42961}{3094}\right)$	$\left(\frac{169}{4}, \frac{1547}{8}\right)$
31	$\left(\frac{720}{287}, \frac{8897}{360}, \frac{2566561}{103320}\right)$	$\left(\frac{49600}{81}, \frac{11032280}{729}\right)$
31	$\left(\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320}\right)$	$\left(\frac{1681}{49}, \frac{29520}{343}\right)$
34	$\left(24, \frac{17}{6}, \frac{145}{6}\right)$	$\left(\frac{153}{4}, \frac{867}{8}\right)$
34	$\left(\frac{112}{9}, \frac{153}{28}, \frac{3425}{252}\right)$	$\left(\frac{833}{16}, \frac{18207}{64}\right)$
34	$\left(\frac{136}{15}, \frac{15}{2}, \frac{353}{30}\right)$	$\left(\frac{289}{4}, \frac{4335}{8}\right)$
34	$\left(\frac{15}{2}, \frac{136}{15}, \frac{353}{30}\right)$	$\left(\frac{850}{9}, \frac{23120}{27}\right)$
34	$\left(\frac{153}{28}, \frac{112}{9}, \frac{3425}{252}\right)$	$(162, 2016)$
34	$\left(\frac{17}{6}, 24, \frac{145}{6}\right)$	$(578, 13872)$
34	$\left(\frac{3927}{248}, \frac{992}{231}, \frac{939905}{57288}\right)$	$\left(\frac{2178}{49}, \frac{65472}{343}\right)$
34	$\left(\frac{992}{231}, \frac{3927}{248}, \frac{939905}{57288}\right)$	$\left(\frac{16337}{64}, \frac{2069529}{512}\right)$
38	$\left(\frac{1700}{279}, \frac{5301}{425}, \frac{1646021}{118575}\right)$	$\left(\frac{47500}{289}, \frac{10071900}{4913}\right)$
38	$\left(\frac{5301}{425}, \frac{1700}{279}, \frac{1646021}{118575}\right)$	$\left(\frac{58482}{961}, \frac{11046600}{29791}\right)$
39	$\left(\frac{156}{5}, \frac{5}{2}, \frac{313}{10}\right)$	$\left(\frac{169}{4}, \frac{845}{8}\right)$
39	$\left(\frac{5}{2}, \frac{156}{5}, \frac{313}{10}\right)$	$(975, 30420)$
41	$\left(\frac{1023}{40}, \frac{3280}{1023}, \frac{1054721}{40920}\right)$	$\left(\frac{44649}{961}, \frac{4437840}{29791}\right)$
41	$\left(\frac{1189}{420}, \frac{840}{29}, \frac{354481}{12180}\right)$	$(841, 24360)$
41	$\left(\frac{123}{20}, \frac{40}{3}, \frac{881}{60}\right)$	$\left(\frac{1681}{9}, \frac{67240}{27}\right)$
41	$\left(\frac{3280}{1023}, \frac{1023}{40}, \frac{1054721}{40920}\right)$	$\left(\frac{42025}{64}, \frac{8598315}{512}\right)$
41	$\left(\frac{40}{3}, \frac{123}{20}, \frac{881}{60}\right)$	$\left(\frac{1025}{16}, \frac{25215}{64}\right)$
41	$\left(\frac{840}{29}, \frac{1189}{420}, \frac{354481}{12180}\right)$	$\left(\frac{18081}{400}, \frac{1023729}{8000}\right)$
46	$\left(\frac{168}{11}, \frac{253}{42}, \frac{7585}{462}\right)$	$\left(\frac{3312}{49}, \frac{139656}{343}\right)$
46	$\left(\frac{253}{42}, \frac{168}{11}, \frac{7585}{462}\right)$	$(242, 3696)$

Bemerkung: Die Kurven

$$y^2 = x(x^2 - N^2) \quad \text{oder auch} \quad y^2 = x^3 - N^2x \quad \text{oder auch } y^2 = x(x-N)(x+N)$$

sind Beispiele von sogenannten **elliptischen Kurven**. Diese Kurven enthalten immer die Punkte $(0,0)$, $(N,0)$, $(-N,0)$.

Die folgenden Bilder zeigen die Kurven für $N = 1, 2, 3, 4, 5, 6$.



Bemerkung: Die Beschäftigung mit Kongruenzzahlen hat eine lange Geschichte. Zwar sind viele Ergebnisse bekannt, es gibt aber auch eine Reihe offener Fragen. Ein neueres Ergebnis ist das folgende [**Tunnell**]:

Satz (Tunnell 1983). *Sei N eine quadratfreie natürliche Zahl,*

$$A = \begin{cases} \{(x,y,z) \in \mathbb{Z}^3 : 4x^2 + y^2 + 8z^2 = \frac{N}{2}, z \text{ gerade}\}, & \text{falls } N \text{ gerade}, \\ \{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = N, z \text{ gerade}\}, & \text{falls } N \text{ ungerade} \end{cases}$$

und

$$B = \begin{cases} \{(x,y,z) \in \mathbb{Z}^3 : 4x^2 + y^2 + 8z^2 = \frac{N}{2}, z \text{ ungerade}\}, & \text{falls } N \text{ gerade}, \\ \{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = N, z \text{ ungerade}\}, & \text{falls } N \text{ ungerade} \end{cases}$$

Dann gilt:

$$N \text{ Kongruenzzahl} \quad \Longrightarrow \quad \#A = \#B$$
$$N \text{ Kongruenzzahl} \quad \overset{BSD\text{-}Vermutung}{\Longleftarrow} \quad \#A = \#B$$

(Dabei steht BSD-Vermutung für eine Vermutung von Birch und Swinnerton-Dyer.)

KAPITEL 2

Affine algebraische Mengen und ebene affine Kurven

Wir legen im Folgenden einen Körper K zugrunde, also beispielsweise

- den Körper $\mathbb{Q}$ der rationalen Zahlen,
- den Körper $\mathbb{R}$ der reellen Zahlen,
- den Körper $\mathbb{C}$ der komplexen Zahlen,
- einen endlichen Körper $\mathbb{F}_p$ mit p Elementen, wobei p eine Primzahl ist,
- einen algebraischen abgeschlossenen Körper K.

Ein Körper K ist **algebraisch abgeschlossen**, wenn jedes Polynom $f \in K[x]$ vom Grad ≥ 1 (mindestens) eine Nullstelle in K besitzt.
Dann erhält man eine Zerlegung

$$f(x) = c \prod_{i=1}^{r} (x - \alpha_i)^{m_i}$$

mit $c, \alpha_1, \ldots, \alpha_r \in K$, $c \neq 0$ und $m_i \in \mathbb{N}$, wobei $\alpha_1, \ldots, \alpha_r$ die verschiedenen Wurzeln/Nullstellen von f sind.
Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen (Fundamentalsatz der Algebra).
Man kann zeigen, dass jeder Körper K in einem algebraisch abgeschlossenen Körper enthalten ist, der algebraisch über K ist. Ein solcher Körper ist bis auf Isomorphie eindeutig bestimmt und wird als **algebraischer Abschluss** $\overline{K}$ von K bezeichnet. (Dass $\overline{K}$ algebraisch über K ist, bedeutet, dass zu jedem $\xi \in \overline{K}$ ein Polynom $f \in K[x] \setminus \{0\}$ existiert mit $f(\xi) = 0$.)

Beispielsweise ist $\mathbb{C}$ der algebraische Abschluss von $\mathbb{R}$.
Ein **Polynom f in den Variablen $x_1, \ldots, x_n$ mit Koeffizienten aus dem Körper K** ist ein Ausdruck

$$f = \sum_{i_1 \geq 0, \ldots, i_n \geq 0} a_{i_1, \ldots, i_r} x_1^{i_1} \ldots x_n^{i_n},$$

wobei die Summe endlich ist und $a_{i_1, \ldots, i_n} \in K$ gilt. Man schreibt auch manchmal

$$f(x_1, \ldots, x_n).$$

Die Menge aller solchen Polynome schreibt man als

$$K[x_1, \ldots, x_n].$$

Man kann Polynome addieren und multiplizieren, wodurch $K[x_1, \ldots, x_n]$ zu einem kommutativen Ring mit 1 wird. Man denkt sich $K \subseteq K[x_1, \ldots, x_n]$, die Zahlen aus K entsprechen dann den konstanten Polynomen.
In Polynome kann man für $x_1, \ldots, x_n$ auch Werte einsetzen:

$$f(p_1, \ldots, p_n),$$

wobei $p_1, \ldots, p_n$ aus einem kommutativen Ring sind, der K enthält.

Erinnerung: Ist $A \in \mathrm{M}_n(K)$ eine quadratische Matrix mit Einträgen aus K, so bildet man das charakteristische Polynom

$$\chi_A(x) = \det(x\mathbf{1}_n - A) \quad \text{oder} \quad \chi_A(x) = \det(A - x\mathbf{1}_n).$$

Datei: algku2.tex. Version vom 19.7.2021

Der Satz von Cayley-Hamilton besagt dann, dass man die Nullmatrix erhält, wenn man die Matrix in ihr charakteristisches Polynom einsetzt:

$$\chi_A(A) = 0.$$

1. Affine algebraische Mengen

DEFINITION. *Der n-dimensionale affine Raum über K wird definiert als*

$$\mathbb{A}^n = \{P = (a_1, \ldots, a_n) : a_i \in \overline{K}\}.$$

$\mathbb{A}^1$ *wird als affine Gerade,* $\mathbb{A}^2$ *als affine Ebene bezeichnet.*

Ist $f \in \overline{K}[x_1, \ldots, x_n]$ ein Polynom (in den Variablen $x_1, \ldots, x_n$) und $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$, so kann man $f(P) = f(a_1, \ldots, a_n)$ bilden, d.h. man kann f als Funktion auf $\mathbb{A}^n$ betrachten. Daher ist folgende Definition sinnvoll:

DEFINITION. *Eine Teilmenge $X \subseteq \mathbb{A}^n$ heißt* **algebraische Menge in** $\mathbb{A}^n$*, falls es Polynome $f_1, \ldots, f_r \in \overline{K}[x_1, \ldots, x_n]$ gibt mit*

$$X = \{P \in \mathbb{A}^n : f_1(P) = \cdots = f_r(P) = 0\}.$$

(Man schreibt auch kurz $X = \{f_1 = \cdots = f_r = 0\}$.)

Beispiele:

- $\mathbb{A}^n$ und $\emptyset \subseteq \mathbb{A}^n$ sind algebraische Mengen, denn es ist $\mathbb{A}^n = \{f = 0\}$ für das Nullpolynom $f = 0 \in \overline{K}[x_1, \ldots, x_n]$ und $\emptyset = \{g = 0\}$ für das konstante Polynom $g = 1 \in \overline{K}[x_1, \ldots, x_n]$.
- Ein Punkt $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ bzw. $\{P\}$ ist eine algebraische Menge, denn $\{P\} = \{x_1 - a_1 = \cdots = x_n - a_n = 0\}$.
- Sind $X = \{f_1 = \cdots = f_r = 0\}$ und $Y = \{g_1 = \cdots = g_s = 0\}$ algebraische Mengen in $\mathbb{A}^n$, so sind auch die Vereinigung

  $$X \cup Y = \{f_1 g_1 = \cdots = f_1 g_s = f_2 g_1 = \cdots = f_2 g_s = \cdots = f_r g_1 = \cdots = f_r g_s = 0\}$$

  und der Durchschnitt

  $$X \cap Y = \{f_1 = \cdots = f_r = g_1 = \cdots = g_s = 0\}$$

  algebraische Mengen in $\mathbb{A}^n$. (Man kann auch zeigen, dass der Durchschnitt beliebig vieler algebraischer Mengen algebraisch ist.)
- **Bemerkung:** Die algebraischen Teilmengen von $\mathbb{A}^n$ bilden die abgeschlossenen Teilmengen einer Topologie auf $\mathbb{A}^n$, der sogenannten **Zariski-Topologie**.

Die algebraische Teilmengen von $\mathbb{A}^1$:

- Ist X eine algebraische Teilmenge von $\mathbb{A}^1$, so gibt es (nach Definition) Polynome $f_1, \ldots, f_r \in \overline{K}[x]$ mit

  $$X = \{f_1 = \cdots = f_r = 0\} = \{\alpha \in \overline{K} : f_1(\alpha) = \cdots = f_r(\alpha) = 0\}.$$

  Es ist

  $$X = \{f_1 = 0\} \cap \cdots \cap \{f_r = 0\}.$$
- Ist $f_i = 0$ (das Nullpolynom), so ist $\{f_i = 0\} = \mathbb{A}^1$.
- Ist $f_i \neq 0$, so gibt es eine Zerlegung

  $$f_i(x) = c \cdot (x - \alpha_1)^{m_1} \ldots (x - \alpha_s)^{m_s}$$

  mit den verschiedenen Nullstellen $\alpha_1, \ldots, \alpha_s$ von f_i und $c \neq 0$. Dann ist

  $$\{f_i = 0\} = \{\alpha_1, \ldots, \alpha_s\}.$$
- Insgesamt sehen wir, dass X entweder $\mathbb{A}^1$ ist oder aus endlich vielen Punkten besteht.

- Da auch jede endliche Teilmenge von X algebraisch ist - $X = \{\beta_1, \ldots, \beta_m\}$ ist die Nullstellenmenge des Polynoms $f(x) = (x - \beta_1) \ldots (x - \beta_m)$ - so erhalten wir insgesamt folgendes Ergebnis:

$$X \subseteq \mathbb{A}^1 \text{ algebraisch} \quad \Longleftrightarrow \quad \begin{cases} X = \mathbb{A}^1 \\ \text{oder} \\ \#X < \infty. \end{cases}$$

Geraden in $\mathbb{A}^2$: Eine Gerade in $\mathbb{A}^2$ ist eine Teilmenge der Gestalt

$$G = \{(x, y) \in \mathbb{A}^2 : a + bx + cy = 0\}$$

mit $a, b, c \in \overline{K}$ und $(b, c) \neq 0$. (Natürlich ist eine Gerade auch eine algebraische Teilmenge von $\mathbb{A}^2$.)

Zwei Geraden

$$G_1 = \{(x, y) \in \mathbb{A}^2 : a_1 + b_1 x + c_1 y = 0\}$$

und

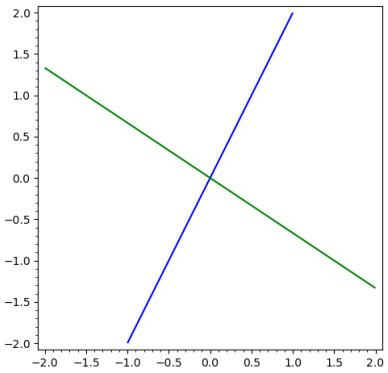
$$G_2 = \{(x, y) \in \mathbb{A}^2 : a_2 + b_2 x + c_2 y = 0\}$$

können in folgenden Beziehungen stehen:

- Sind (b_1, c_1) und (b_2, c_2) linear unabhängig, so gilt

$$G_1 \cap G_2 = \{(x_0, y_0)\}, \text{ wobei } (x_0, y_0) \text{ durch } \begin{pmatrix} b_1 & c_1 \\ b_2 & c_2 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} -a_1 \\ -a_2 \end{pmatrix}$$

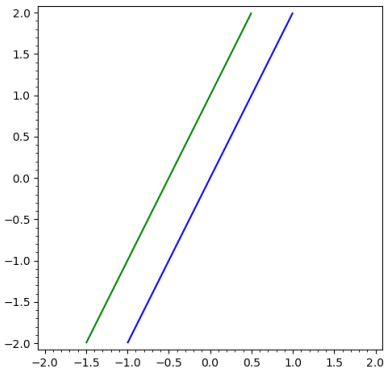
  eindeutig bestimmt ist. (G_1 und G_2 schneiden sich in einem Punkt.)

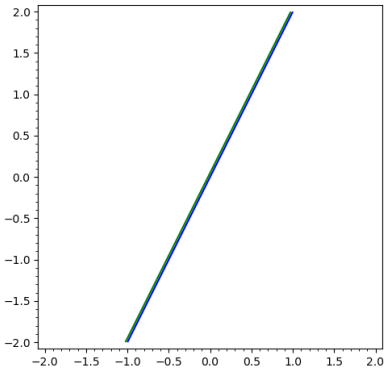


- Sind (b_1, c_1) und (b_2, c_2) linear abhängig, aber (a_1, b_1, c_1) und (a_2, b_2, c_2) linear unabhängig, so gilt

$$G_1 \cap G_2 = \emptyset.$$

  (G_1 und G_2 sind parallel.)



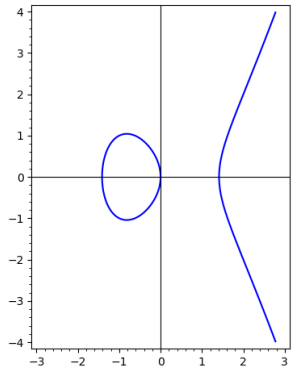
- Sind (a_1, b_1, c_1) und (a_2, b_2, c_2) linear abhängig, so gilt
$$G_1 = G_2.$$


- Eine Gerade $G = \{(x, y) \in \mathbb{A}^2 : a + bx + cy = 0\}$ lässt sich in parametrisierter Form darstellen, d.h. man findet $\alpha, \beta, \gamma, \delta \in \overline{K}$ mit $(\beta, \delta) \neq 0$, sodass gilt:
$$G = \{(\alpha + \beta t, \gamma + \delta t) \in \mathbb{A}^2 : t \in \overline{K}\}.$$
Explizit kann man sofort folgende Parametrisierungen angeben:
$$G = \begin{cases} \{(x, -\frac{a}{c} - \frac{b}{c}x) : x \in \overline{K}\} & \text{für } c \neq 0, \\ \{(-\frac{a}{b}, y) : y \in \overline{K}\} & \text{für } c \neq 0. \end{cases}$$
- Zu zwei verschiedenen Punkten $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in \mathbb{A}^2$ gibt es genau eine Gerade $G = \{(x, y) \in \mathbb{A}^2 : a + bx + cy = 0\}$, die beide Punkte enthält. (a, b, c) wird bis auf eine Konstante bestimmt durch die Gleichung
$$\begin{pmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0.$$
- Sind $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ zwei verschiedene Punkte in $\mathbb{A}^2$, so ist
$$G = \{((1-t)x_1 + tx_2, (1-t)y_1 + ty_2) : t \in \overline{K}\}$$
eine Parameterdarstellung der Geraden durch P_1 und P_2. (Dies kennt man aus der Linearen Algebra, wobei die Vektorschreibweise
$$(1-t)\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + t\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \quad t \in \overline{K}$$
vielleicht übersichtlicher ist.)
- Drei Punkte $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{A}^2$ liegen genau dann auf einer Geraden, wenn gilt
$$\begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix} = 0.$$
(Man nennt solche Punkte auch kollinear.)

DEFINITION.
- *Die Menge der K-rationalen Punkte von $\mathbb{A}^n$ wird definiert als*
$$\mathbb{A}^n(K) = \{P = (a_1, \ldots, a_n) \in \mathbb{A}^n : a_1, \ldots, a_n \in K\}.$$
- *Man sagt, eine algebraische Menge $X \subseteq \mathbb{A}^n$ ist über K definiert, falls es Polynome $g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$ gibt mit*
$$X = \{P \in \mathbb{A}^n : g_1(P) = \cdots = g_s(P) = 0\} = \{g_1 = \cdots = g_s = 0\}.$$
(Man schreibt dann auch X/K.)

- *Ist $X \subseteq \mathbb{A}^n$ über K definiert (mit den obigen Bezeichnungen), so heißt*
$$X(K) = X \cap \mathbb{A}^n(K) = \{P \in K^n : g_1(P) = \cdots = g_s(P) = 0\}$$
die Menge der K-rationalen Punkte von X.

Beispiel: Als Grundkörper wählen wir $\mathbb{R}$. Durch
$$y^2 = x^3 - 2x$$
wird eine algebraische Menge X in $\mathbb{A}^2$ definiert, die über $\mathbb{R}$ definiert ist. Die $\mathbb{R}$-rationalen Punkte von X kann man im Bild sehen:



X enthält aber auch andere Punkte, die nicht über $\mathbb{R}$ definiert sind, beispielsweise
$$(1, i),$$
wo $i \in \mathbb{C}$ mit $i^2 = -1$ gilt.

Beispiel: Als Grundkörper wählen wir $\mathbb{R}$. Durch
$$x^2 + y^2 + 1 = 0$$
wird eine algebraische Menge X in $\mathbb{A}^2$ definiert, die über $\mathbb{R}$ definiert ist. X enthält offensichtlich keine $\mathbb{R}$-rationalen Punkte:
$$X(\mathbb{R}) = \emptyset.$$
X enthält aber Punkte, beispielsweise $(i, 0)$ (mit $i \in \mathbb{C}$, $i^2 = -1$).

Beispiele: Als Grundkörper wählen wir $K = \mathbb{Q}$.

- $X = \{(x, y) \in \mathbb{A}^2 : x^2 + y^2 = 1\}$ ist eine über $\mathbb{Q}$ definierte algebraische Menge. Im letzten Kapitel haben wir die Menge der $\mathbb{Q}$-rationalen Punkte parametrisiert beschrieben:
$$X(\mathbb{Q}) = \{(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}) : t \in \mathbb{Q}\} \cup \{(0, 1)\}.$$
- Als Verallgemeinerung von (1) betrachten wir für $d \in \mathbb{N}$ die über $\mathbb{Q}$ definierte algebraische Menge
$$F_d = \{(x, y) \in \mathbb{A}^2 : x^d + y^d = 1\}.$$
Die von Wiles (1995) bewiesene Fermat-Vermutung liefert
$$F_d(\mathbb{Q}) = \begin{cases} \{(1, 0), (0, 1)\} & \text{für ungerade } d \geq 3, \\ \{(\pm 1, 0), (0, \pm 1)\} & \text{für gerade } d \geq 3. \end{cases}$$
- Für $N \in \mathbb{N}$ betrachten wir die über $\mathbb{Q}$ definierte algebraische Menge
$$K_N = \{(x, y) \in \mathbb{A}^2 : y^2 = x^3 - N^2 x\}.$$
Offensichtlich gilt
$$\{(0, 0), (N, 0), (-N, 0)\} \subseteq K_n(\mathbb{Q}).$$

Mit Hilfe der im letzten Kapitel angegebenen Charakterisierung von Kongruenzzahlen kann man zeigen:

$$N \text{ ist Kongruenzzahl} \quad \Longleftrightarrow \quad \{(0,0),(N,0),(-N,0)\} \neq K_n(\mathbb{Q}).$$

- $X = \{1, i, -i\} \subseteq \mathbb{A}^1$ ist wegen $X = \{x \in \mathbb{A}^1 : (x-1)(x^2+1) = 0\}$ eine über $\mathbb{Q}$ definierte algebraische Menge mit $X(\mathbb{Q}) = \{1\}$.
- $X = \{(x,y) \in \mathbb{A}^2 : x^2 - 2y^2 = 0\}$ eine eine über $\mathbb{Q}$ definierte algebraische Menge. Die Menge der $\mathbb{Q}$-rationalen Punkte von X ist $X(\mathbb{Q}) = \{(0,0)\}$.
- Die algebraische Menge $X = \{(x,y) \in \mathbb{A}^2 : x - \sqrt{2}y = 0\}$ ist nicht über $\mathbb{Q}$ definiert, wohl aber über $\mathbb{Q}(\sqrt{2})$ (oder $\mathbb{R}$ oder $\mathbb{C}$).
- Sei $X = \{(1,i),(-1,-i)\} \subseteq \mathbb{A}^2$ (über $\mathbb{C}$ definiert). Wäre X über $\mathbb{R}$ definiert, so gäbe es Polynome $f_1, \ldots, f_r \in \mathbb{R}[x,y]$ mit

  $$X = \{P \in \mathbb{A}^2 : f_1(P) = \cdots = f_r(P) = 0\}.$$

  Wir können schreiben

  $$f_j(x,y) = \sum_{k,l} a_{j,k,l} x^k y^l \text{ mit } a_{j,k,l} \in \mathbb{R}.$$

  Aus $(1,i) \in X$ folgt $f_j(1,i) = 0$, d.h.

  $$\sum_{k,l} a_{j,k,l} 1^k i^l = 0.$$

  Komplexe Konjugation liefert

  $$0 = \overline{\sum_{k,l} a_{j,k,l} 1^k i^l} = \sum_{k,l} a_{j,k,l} 1^k (-i)^l = f_j(1,-i).$$

  Da dies für alle j gilt, würde $(1,-i) \in X$ folgen, ein Widerspruch. Daher ist X nicht über $\mathbb{R}$ definiert.
- Mit der gleichen Argumentation wie im letzten Beispiel erhält man Folgendes: Ist $X \subseteq \mathbb{A}^2$ eine über $\mathbb{R}$ definierte algebraische Menge, und gilt

  $$\{(1,i),(-1,-i)\} \subseteq X,$$

  so folgt

  $$\{(1,i),(1,-i),(-1,-i),(-1,i)\} \subseteq X.$$

Affiner Koordinatenwechsel: Ein affiner Koordinatenwechsel wird gegeben durch eine Abbildung

$$\phi : \mathbb{A}^n \to \mathbb{A}^n, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

mit $A = (a_{ij}) \in \mathrm{GL}_n(\overline{K})$ und $b_i \in \overline{K}$.
Ist $A \in \mathrm{GL}_n(K)$ und $b_i \in K$, so sagt man, der Koordinatenwechsel ist über K definiert.

Bemerkung: Geometrische Eigenschaften, wie sie im Folgenden beschrieben werden, ändern sich nicht bei Koordinatenwechsel. Dies muss man natürlich eigentlich zeigen. Wir werden dies aber meist nicht tun.

Leicht beweist man folgendes Lemma:

LEMMA. *Sind P_1, P_2, P_3 drei Punkte in $\mathbb{A}^2$, die nicht auf einer Geraden liegen, so gibt es (genau) einen Koordinatenwechsel $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ mit*

$$\phi(P_1) = (0,0), \quad \phi(P_2) = (1,0), \quad \phi(P_3) = (0,1).$$

Beweis: Der Einfachkeit halber schreiben wir Punkte aus $\mathbb{A}^2$ jetzt als Vektoren in $\overline{K}^2$. Wir suchen dann eine Matrix $A \in \mathrm{GL}_2(\overline{K})$ und $b \in \overline{K}^2$ mit

$$AP_1 + b = \begin{pmatrix}0\\0\end{pmatrix}, \quad AP_2 + b = \begin{pmatrix}1\\0\end{pmatrix}, \quad AP_3 + b = \begin{pmatrix}0\\1\end{pmatrix}.$$

Wir formen die Bedingung äquivalent um:

$$\begin{aligned} & AP_1 + b = \begin{pmatrix}0\\0\end{pmatrix}, \quad AP_2 + b = \begin{pmatrix}1\\0\end{pmatrix}, \quad AP_3 + b = \begin{pmatrix}0\\1\end{pmatrix} \quad \Longleftrightarrow \\ \Longleftrightarrow \quad & b = -AP_1, \quad AP_2 - AP_1 = \begin{pmatrix}1\\0\end{pmatrix}, \quad AP_3 - AP_1 = \begin{pmatrix}0\\1\end{pmatrix} \quad \Longleftrightarrow \\ \Longleftrightarrow \quad & b = -AP_1, \quad A(P_2 - P_1) = \begin{pmatrix}1\\0\end{pmatrix}, \quad A(P_3 - P_1) = \begin{pmatrix}0\\1\end{pmatrix} \quad \Longleftrightarrow \\ \Longleftrightarrow \quad & b = -AP_1, \quad A(P_2 - P_1 | P_3 - P_1) = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \end{aligned}$$

Wäre die Matrix $(P_2 - P_1|P_3 - P_1)$ nicht invertierbar, so gäbe es ein $\lambda \in \overline{K}$ mit

$$P_3 - P_1 = \lambda(P_2 - P_1), \quad \text{also} \quad P_3 = (1-\lambda)P_1 + \lambda P_2,$$

P_3 läge also auf der Geraden durch P_1, P_2, was der Voraussetzung widerspricht. Aus der Invertierbarkeit von $(P_2 - P_1|P_3 - P_1)$ folgt dann sofort, dass A und b eindeutig bestimmt sind. ■

2. Ebene affine Kurven

DEFINITION. *K sei der zugrundeliegende Körper mit algebraischem Abschluss $\overline{K}$.*

- *Eine ebene affine Kurve C wird durch ein Polynom $f(x,y) \in \overline{K}[x,y] \setminus \overline{K}$ gegeben. Man sagt auch, dass C durch die Gleichung $f(x,y) = 0$ definiert wird. Die zugehörige affine algebraische Menge ist*

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

  Zwei Polynome, die sich nur um eine (multiplikative) Konstante unterscheiden, ergeben die gleiche Kurve. Ist $f(x,y) \in \overline{K}[x,y]$ irreduzibel, so nennt man C irreduzibel, andernfalls reduzibel.
- *Kann man $f(x,y) \in K[x,y]$ wählen, so sagt man, die Kurve ist über K definiert. Die Menge der K-rationalen Punkte ist*

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

  Etwas allgemeiner betrachtet man für einen Oberkörper L von K die Menge der L-rationalen Punkte von C:

  $$C(L) = \{(x,y) \in \mathbb{A}^2(L) : f(x,y) = 0\}.$$

  Ist $f(x,y)$ in $K[x,y]$ irreduzibel, so nennt man C irreduzibel über K. Ist $f(x,y)$ im Polynomring $\overline{K}[x,y]$ irreduzibel, so nennt man C absolut irreduzibel.

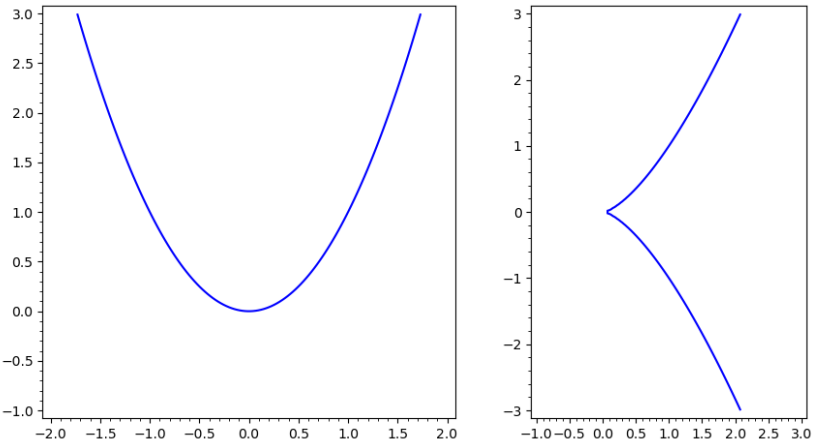
Beispiele:

- Sind $a, b, c \in \overline{K}$ mit $(b,c) \neq (0,0)$ so definiert $a + bx + cy$ eine Kurve G mit

  $$G(\overline{K}) = \{(x,y) \in \mathbb{A}^2 : a + bx + cy = 0\},$$

  d.h. $G(\overline{K})$ ist eine affine Gerade. Da $G(\overline{K})$ den Vektor (a,b,c) und damit die Gleichung $a+bx+cy$ bis auf eine Konstante bestimmt, nennen wir G auch einfach affine Gerade.

- $y = x^2$ definiert eine Parabel, $y^2 = x^3$ die sogenannte Neilsche Parabel. Sowohl Parabel als auch Neilsche Parabel sind absolut irreduzibel.

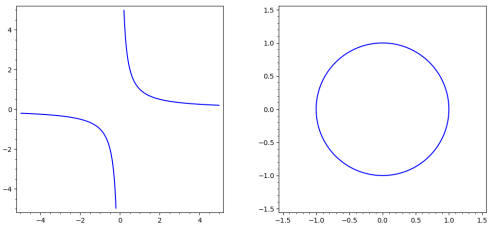


  (Die Bilder zeigen eigentlich die $\mathbb{R}$-rationalen Punkte der Kurven.)
- $f = x^2 - y^2 = (x-y)(x+y)$ definiert eine ebene Kurve C über $\mathbb{R}$ mit
$$\begin{aligned} C(\mathbb{R}) &= \{(x,y) \in \mathbb{R}^2 : (x-y)(x+y) = 0\} = \\ &= \{(x,y) \in \mathbb{R}^2 : y = x\} \cup \{(x,y) \in \mathbb{R}^2 : y = -x\}. \end{aligned}$$
  C besteht also aus den beiden Geraden $y = x$ und $y = -x$.
- Auch $f = x^2 + y^2$ definiert eine ebene Kurve über $\mathbb{R}$. Allerdings ist
$$C(\mathbb{R}) = \{(0,0)\}$$
  nur ein Punkt. Über dem algebraischen Abschluss ist
$$C(\mathbb{C}) = \{(x,y) \in \mathbb{C}^2 : y = ix \text{ oder } y = -ix\},$$
  d.h. $C(\mathbb{C})$ besteht aus den beiden Geraden $y = ix$ und $y = -ix$. Also ist C irreduzibel, aber nicht absolut irreduzibel.
- Wir betrachten die durch $f = 1 + 2x^3 + 3y^3$ über $\mathbb{F}_5$ definierte Kurve C. Durch Ausprobieren aller 25 Punkte von $\mathbb{A}^2(\mathbb{F}_5)$ findet man
$$C(\mathbb{F}_5) = \{(0,2), (1,4), (2,1), (3,0), (4,3)\},$$
  insbesondere ist $\#C(\mathbb{F}_5) = 5$.

Bemerkung: Ein Grundproblem der Zahlentheorie ist folgendes: Bestimme für eine über $\mathbb{Q}$ definierte Kurve C die Menge der $\mathbb{Q}$-rationalen Punkte $C(\mathbb{Q})$ von C.

Affiner Koordinatenwechsel: Sei C durch eine Gleichung $f(x,y) = 0$ definiert. Ist
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} \widetilde{x} \\ \widetilde{y} \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$
ein affiner Koordinatenwechsel (mit neuen Koordinaten $\widetilde{x}, \widetilde{y}$), so definiert
$$\widetilde{f}(\widetilde{x}, \widetilde{y}) = f(a_{11}\widetilde{x} + a_{12}\widetilde{y} + b_1, a_{21}\widetilde{x} + a_{22}\widetilde{y} + b_2)$$
eine Kurve $\widetilde{C}$. Man sagt $\widetilde{C}$ ist affin äquivalent zu C. Dann ist
$$\widetilde{C}(\overline{K}) \to C(\overline{K}), \quad (\widetilde{x}, \widetilde{y}) \mapsto (a_{11}\widetilde{x} + a_{12}\widetilde{y} + b_1, a_{21}\widetilde{x} + a_{22}\widetilde{y} + b_2)$$
eine Bijektion.
Sind C und der Koordinatenwechsel über K definiert, so ist auch $\widetilde{C}$ über K definiert und
$$\widetilde{C}(K) \to C(K), \quad (\widetilde{x}, \widetilde{y}) \mapsto (a_{11}\widetilde{x} + a_{12}\widetilde{y} + b_1, a_{21}\widetilde{x} + a_{22}\widetilde{y} + b_2)$$
ist eine Bijektion.

Beispiel: Wir betrachten die Kurven $xy = 1$ und $x^2+y^2 = 1$ über $\mathbb{R}$. Die Bilder zeigen die reellen Punkte der Kurven:



Wir betrachten die Kurven nun über $\mathbb{C}$. Wir führen neue Koordinaten u, v ein durch

$$x = u + iv, \quad y = u - iv, \qquad \text{also} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

(Die Determinante ist $-2i \neq 0$, also handelt es sich um einen affinen Koordinatenwechsel.) Dann erhalten wir aus $xy = 1$ sofort $(u + iv)(u - iv) = 1$, also $u^2 + v^2 = 1$. Die beiden Kurven $xy = 1$ und $x^2 + y^2 = 1$ sind also affin äquivalent über $\mathbb{C}$.

Bemerkung: Geometrische Eigenschaften, wie sie im Folgenden beschrieben werden, ändern sich nicht bei Koordinatenwechsel. Dies muss man natürlich eigentlich zeigen. Wir werden dies aber meist nicht tun.

Wir wollen nun Kurven lokal um einen Punkt näher betrachten.

Überlegung: Sei C eine ebene Kurve gegeben durch eine Gleichung $f(x, y) = 0$ und $P = (x_0, y_0) \in C(\overline{K})$. Wir bilden die Taylorreihenentwicklung von f in (x_0, y_0):

$$f = a_1(x - x_0) + a_2(y - y_0) + a_3(x - x_0)^2 + a_4(x - x_0)(y - y_0) + a_5(y - y_0)^2 + \dots$$

Es folgt

$$\begin{aligned} \frac{\partial f}{\partial x} &= a_1 + 2a_3(x - x_0) + a_4(y - y_0) + \dots, \\ \frac{\partial f}{\partial y} &= a_2 + a_4(x - x_0) + 2a_5(y - y_0) + \dots \end{aligned}$$

und damit

$$\frac{\partial f}{\partial x}(P) = a_1, \quad \frac{\partial f}{\partial y}(P) = a_2.$$

Ist $(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) = (a_1, a_2) \neq (0, 0)$, so ist

$$a_1(x - x_0) + a_2(y - y_0) = \frac{\partial f}{\partial x}(P)(x - x_0) + \frac{\partial f}{\partial y}(P)(y - y_0)$$

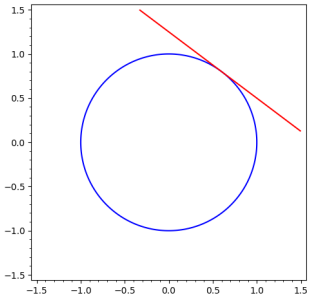
die lineare Approximation von f in P.

DEFINITION. *Sei eine Kurve C gegeben durch ein Polynom $f(x, y)$ und $P = (x_0, y_0) \in C(\overline{K})$.*

- *Die Kurve C heißt singulär im Punkt P bzw. hat eine Singularität im Punkt P, wenn gilt*
$$(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) = (0, 0).$$
- *Ist $(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) \neq (0, 0)$, so heißt P nichtsingulärer oder glatter Punkt der Kurve C, und*
$$\frac{\partial f}{\partial x}(P)(x - x_0) + \frac{\partial f}{\partial y}(P)(y - y_0) = 0$$
heißt die Tangente von C im Punkt P.

Beispiele:

- Sei C gegeben durch $f = x^2 + y^2 - 1 = 0$ und $P = (\frac{3}{5}, \frac{4}{5}) \in C(\mathbb{Q})$. Es ist $\frac{\partial f}{\partial x} = 2x$ und $\frac{\partial f}{\partial y} = 2y$, also
$$(\frac{\partial f}{\partial x}(P), (\frac{\partial f}{\partial y}(P)) = (2x(P), 2y(P)) = (\frac{6}{5}, \frac{8}{5}).$$
Daher ist C in P nichtsingulär mit Tangente
$$\frac{6}{5}(x - \frac{3}{5}) + \frac{8}{5}(y - \frac{4}{5}) = 0 \quad \text{bzw.} \quad 3x + 4y = 5.$$



- Sei C gegeben durch $f = y^2 - x^3 = 0$. Offensichtlich ist C singulär in $P = (0, 0)$.

Bemerkung: Bei Koordinatenwechsel gehen Singularitäten in Singularitäten und Tangenten in Tangenten über.

LEMMA. *Ist* $f(x, y) = \sum_{i=0}^{m} a_i x^i y^{m-i} \in K[x, y]$ *ein homogenes Polynom vom Grad* m*, dann gibt es* $\alpha_i, \beta_i \in \overline{K}$ *mit*
$$f(x, y) = \prod_{i=1}^{m} (\alpha_i x + \beta_i y).$$

Beweis: Ist $f(x, y) = 0$, so ist nichts zu zeigen. Sei nun d mit $a_d \neq 0$, $a_{d+1} = a_{d+2} = \cdots = 0$. Es gibt $\lambda_i \in \overline{K}$ mit
$$a_0 + a_1 t + \cdots + a_{d-1} t^{d-1} + a_d t^d = a_d (t - \lambda_1) \ldots (t - \lambda_d).$$
Dann ist
$$\begin{aligned} f(x, y) &= a_0 y^m + a_1 x y^{m-1} + \cdots + a_{d-1} x^{d-1} y^{m-d+1} + a_d x^d y^{m-d} = \\ &= y^m (a_0 + a_1 (\frac{x}{y}) + \cdots + a_{d-1} (\frac{x}{y})^{d-1} + a_d (\frac{x}{y})^d) = \\ &= a_d y^m (\frac{x}{y} - \lambda_1) \ldots (\frac{x}{y} - \lambda_d) = \\ &= a_d y^{m-d} (x - \lambda_1 y) \ldots (x - \lambda_d y), \end{aligned}$$
was die Behauptung beweist. ■

Multiplizität einer Kurve in einem Punkt: Sei C eine durch $f(x, y) = 0$ definierte ebene Kurve und $P = (x_0, y_0) \in \mathbb{A}^2$ ein Punkt. Die Taylorreihenentwicklung von f um (x_0, y_0) hat dann die Gestalt
$$f = \sum_{i,j} a_{ij} (x - x_0)^i (y - y_0)^j.$$
Der homogene Anteil vom Grad ℓ ist
$$f_\ell = \sum_{i+j=\ell} a_{ij} (x - x_0)^i (y - y_0)^j.$$
Wir können dann schreiben
$$f = f_m + f_{m+1} + f_{m+2} + \ldots \quad \text{mit} \quad f_m \neq 0.$$
Dann heißt m die **Multiplizität** von C in P. Wir unterscheiden einige Fälle:

- $m = 0$: Dann ist $P \notin C(\overline{K})$.

- $m = 1$: Dann ist P glatter Punkt von C. Der lineare Anteil $f_1 = a_{10}(x-x_0)+a_{01}(y-y_0)$ liefert die Tangente $a_{10}(x-x_0)+a_{01}(y-y_0) = 0$ von C in P.
- $m \geq 2$: Dann ist C singulär in P. Man kann faktorisieren

$$f_m(x,y) = \prod_{i=1}^{m}(\alpha_i(x-x_0)+\beta_i(y-y_0)) \quad \text{mit} \quad \alpha_i,\beta_i \in \overline{K} \quad \text{und} \quad (\alpha_i,\beta_i) \neq 0.$$

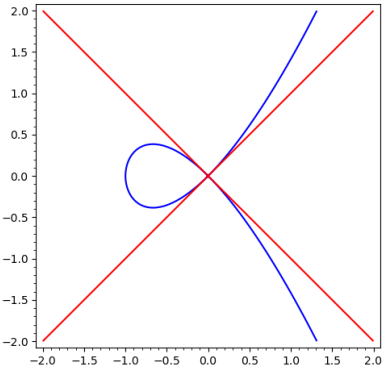
Die Geraden $\alpha_i(x-x_0)+\beta_i(y-y_0) = 0$ nennt man (auch) **Tangenten** von C in P.

Beispiele:

- Wir betrachten die Kurve C mit der Gleichung $y^2 = x^2 + x^3$ bzw. $f(x,y) = x^2 - y^2 + x^3 = 0$ über $\mathbb{R}$ und den Punkt $P = (0,0)$. Die Taylorreihenentwicklung von $f(x,y)$ in $(0,0)$ ist

$$f(x,y) = (x^2 - y^2) + x^3,$$

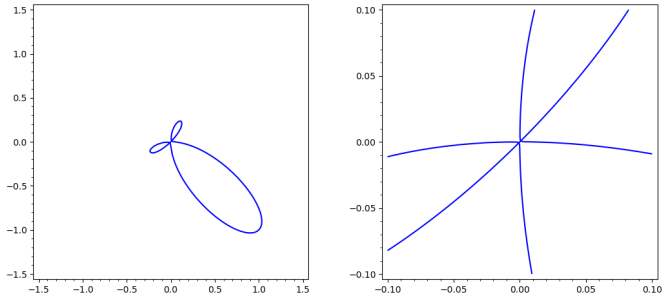
daher ist die Multiplizität von C in P einfach 2 und $y = x$ und $y = -x$ sind die Tangenten.



- Wir betrachten die durch

$$xy(x-y) + x^4 + y^4 = 0$$

definierte Kurve. Hier ist $(0,0)$ ein singulärer Punkt mit Multiplizität 3. Die Tangenten sind $x = 0$, $y = 0$, $y = x$.



Wir wollen nun Schnitte von Kurven betrachten. Für praktische Anwendungen erinnern wir an ein Hilfsmittel aus der Algebra, die Resultanten:

Resultanten: Seien $f(x,y), g(x,y) \in K[x,y]$ von 0 verschiedene Polynome, die wir in der Form

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

schreiben können mit $m = \mathrm{grad}_y(f)$ und $n = \mathrm{grad}_y(g)$, d.h. $a_m(x) \neq 0$ und $b_n(x) \neq 0$. Dann ist die **Resultante** $R_y(f,g)(x)$ von $f(x,y)$ und $g(x,y)$ bzgl. y definiert durch die Determinante

$$R_y(f,g)(x) = \det \begin{pmatrix} a_m(x) & \dots & \dots & a_0(x) & & \\ & \ddots & & & \ddots & \\ & & a_m(x) & \dots & \dots & a_0(x) \\ b_n(x) & \dots & \dots & b_0(x) & & \\ & \ddots & & & \ddots & \\ & & b_n(x) & \dots & \dots & b_0(x) \end{pmatrix} \in K[x].$$

(Die Matrix hat $m+n$ Zeilen und Spalten, wobei zunächst n Zeilen mit den Koeffizienten von $f(x,y)$, dann m Zeilen mit den Koeffizienten von $g(x,y)$ eingetragen werden.) Wir geben zwei wichtige Eigenschaften an:

- Es gibt Polynome $A(x,y), B(x,y) \in K[x,y]$ mit
$$A(x,y)f(x,y) + B(x,y)g(x,y) = R_y(f,g)(x).$$
- Genau dann ist $R_y(f,g)(x) = 0$, wenn $f(x,y)$ und $g(x,y)$ einen gemeinsamen Teiler $h(x,y) \in K[x,y]$ mit $\mathrm{grad}_y h(x,y) \geq 1$ besitzen.

Natürlich kann man analog auch die Resultante bzgl. x bilden, die dann ein Polynom $R_x(f,g)(y)$ in y ist.

Beispiel:

$$f = -2x^2 + xy - y^2 + 2x - 2y + 1, \quad g = x^2 - xy + 2y^2 - x + y.$$

Wir schreiben f und g als Polynome in y:

$$f = -y^2 + (x-2)y + (-2x^2 + 2x + 1), \quad g = 2y^2 + (-x+1)y + (x^2 - x).$$

Nun tragen wir die Koeffizienten in die 4×4-Resultantenmatrix ein:

$$\begin{pmatrix} -1 & x-2 & -2x^2+2x+1 & 0 \\ 0 & -1 & x-2 & -2x^2+2x+1 \\ 2 & -x+1 & x^2-x & 0 \\ 0 & 2 & -x+1 & x^2-x \end{pmatrix}$$

Determinantenbildung liefert die Resultante:

$$R_y(f,g)(x) = 8x^4 - 14x^3 - 5x^2 + 8x + 7.$$

Bemerkung: Mit SAGE kann man auch Resultanten berechnen. Für die Polynome des letzten Beispiels erhält man die Resultante auf folgende Weise:

```
var("x,y")
f=-2*x^2+x*y-y^2+2*x-2*y+1
g=x^2-x*y+2*y^2-x+y
f.resultant(g,y)
```

Wir erhalten jetzt einfach folgenden Satz:

SATZ. *Seien C und D durch $f(x,y)$ bzw. $g(x,y)$ definierte Kurven über K. Sind $R_y(f,g)(x)$ und $R_x(f,g)(y)$ die Resultanten von $f(x,y)$ und $g(x,y)$ bzgl. y bzw. x, so gilt:*

- $$C(\overline{K}) \cap D(\overline{K}) \subseteq \{(x_0,y_0) \in \mathbb{A}^2 : R_y(f,g)(x_0) = R_x(f,g)(y_0) = 0\}.$$
- *Sind $f(x,y)$ und $g(x,y)$ teilerfremd, so sind die Resultanten $R_y(f,g)(x)$ und $R_x(f,g)(y)$ von 0 verschiedene Polynome einer Variablen. Insbesondere folgt*
$$\#C(\overline{K}) \cap D(\overline{K}) \leq \mathrm{grad}_x R_y(f,g) \cdot \mathrm{grad}_y R_x(f,g).$$

Beweis: Es gibt Polynome $A(x,y), B(x,y), U(x,y), V(x,y) \in K[x,y]$ mit

$$A(x,y)f(x,y) + B(x,y)g(x,y) = R_y(f,g)(x)$$

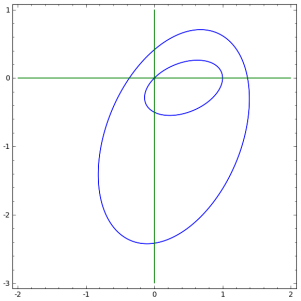
und

$$U(x,y)f(x,y) + V(x,y)g(x,y) = R_x(f,g)(y).$$

Ist $(x_0,y_0) \in C(\overline{K}) \cap D(\overline{K})$, so folgt mit $f(x_0,y_0) = g(x_0,y_0) = 0$ sofort $R_y(f,g)(x_0) = R_x(f,g)(y_0) = 0$ und damit die erste Behauptung. Haben $f(x,y)$ und $g(x,y)$ keinen gemeinsamen Teiler, so sind beide Resultanten $R_y(f,g)$ und $R_x(f,g)$ von 0 verschieden, was sofort die zweite Behauptung liefert. ■

Beispiel: Gegeben seien die ebenen affinen Kurven $f = 0$ und $g = 0$ durch

$$f = -2x^2 + xy - y^2 + 2x - 2y + 1, \quad g = x^2 - xy + 2y^2 - x + y.$$



Wir wollen den Schnitt bestimmen. Wir bilden die Resultanten

$$R_y(f,g)(x) = 8x^4 - 14x^3 - 5x^2 + 8x + 7, \quad R_x(f,g)(y) = 8y^4 - 2y^3 + 5y^2 - y + 1$$

und bestimmen die Nullstellen (über $\mathbb{C}$)

$$x = -0.54 \pm 0.36i, 1.42 \pm 0.15i \quad \text{bzw.} \quad y = -0.10 \pm 0.63i, 0.23 \pm 0.50i.$$

Dies gibt 16 mögliche Schnittpunkte (x,y). Durch Testen, in welchen Punkten sowohl f als auch g verwendet, erhalten wir die folgenden vier Schnittpunkte:

$$(-0.54 - 0.36i, -0.10 - 0.63i), \quad (1.42 - 0.15i, 0.23 + 0.50i),$$

$$(-0.54 + 0.36i, -0.10 + 0.63i), \quad (1.42 + 0.15i, 0.23 - 0.50i).$$

Beispiel: Gegeben seien die ebenen affinen Kurven $f = 0$ und $g = 0$ durch

$$\begin{aligned} f &= 179x^2 - 64xy - 192y^2 + 181x + 932y - 122, \\ g &= 35x^2 - 64xy + 64y^2 - 59x - 28y - 422. \end{aligned}$$

Um den Schnitt der Kurven zu bestimmen, bilden wir die Resultanten:

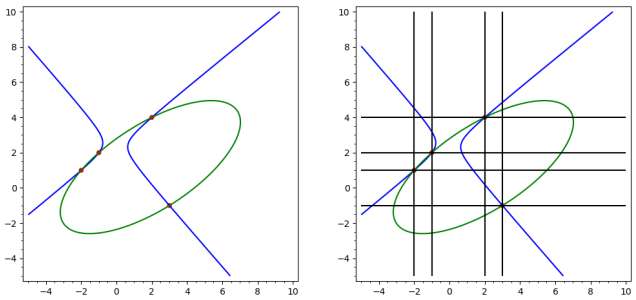
$$\begin{aligned} R_y(f,g)(x) &= 179372032x^4 - 358744064x^3 - 1255604224x^2 + 1434976256x + 2152464384 = \\ &= 179372032(x+2)(x+1)(x-2)(x-3), \\ R_x(f,g)(y) &= 179372032y^4 - 1076232192y^3 + 1255604224y^2 + 1076232192y - 1434976256 = \\ &= 179372032(y+1)(y-1)(y-2)(y-4). \end{aligned}$$

Für die Schnittpunkte (x_i, y_i) der Kurven gilt dann

$$x_i \in \{-2,-1,2,3\} \quad \text{und} \quad y_i \in \{-1,1,2,4\}.$$

Indem mal alle 16 Möglichkeiten durchprobiert, findet man die vier Schnittpunkte

$$(-2,1), \quad (-1,2), \quad (2,4), \quad (3,-1).$$



Wir geben eine Anwendung für die Singularitäten einer ebenen Kurve:

SATZ. *Sei C gegeben durch ein Polynom $f(x,y) \in K[x,y]$. Die Menge der Singularitäten von C ist*

$$\{P \in \mathbb{A}^2(\overline{K}) : f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0\}.$$

Ist C absolut irreduzibel, so hat C nur endlich viele Singularitäten.

Beweis: Da eine Singularität P von C durch die Gleichungen $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$ charakterisiert werden, ist klar, dass die angegebene Menge genau die Singularitäten beschreibt. Wir betrachten jetzt den Fall, dass $f(x,y)$ irreduzibel über $\overline{K}$ ist. Wir unterscheiden ein paar Fälle:

- *Fall 1:* $\frac{\partial f}{\partial y} \neq 0$. Wir schreiben

  $$f(x,y) = a_0(x) + a_1(x)y + \cdots + a_m(x)y^m \quad \text{mit} \quad a_m(x) \neq 0.$$

  Dann ist

  $$\frac{\partial f}{\partial y}(x,y) = a_1(x) + \cdots + m a_m(x) y^{m-1}.$$

  Da $f(x,y)$ irreduzibel ist, haben $f(x,y)$ und $\frac{\partial f}{\partial y}(x,y)$ keinen gemeinsamen Teiler. Also sind die beiden zugehörigen Resultanten $R_y(x)$ und $R_x(y)$ von 0 verschieden. Demnach haben $f(x,y) = 0$ und $\frac{\partial f}{\partial y}(x,y) = 0$ nur endlich viele Schnittpunkte, weswegen es auch nur endlich viele Singularitäten geben kann.
- *Fall 2:* $\frac{\partial f}{\partial x} \neq 0$. Diesen Fall behandelt man genauso wie Fall 1.
- *Fall 3:* $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$. Sei

  $$f = \sum_{i,j} a_{ij} x^i y^j.$$

  Dann ist

  $$\frac{\partial f}{\partial x} = \sum_{i,j} i a_{ij} x^{i-1} y^j \quad \text{und} \quad \frac{\partial f}{\partial y} = \sum_{i,j} j a_{ij} x^i y^{j-1}$$

  und damit $ia_{ij} = 0$ und $ja_{ij} = 0$. In Charakteristik 0 ist dies nicht möglich, da mindestens ein Indexpaar (i,j) mit $i > 0$ oder $j > 0$ existiert. Also ist die Charakteristik p. Im Fall $a_{ij} \neq 0$ gilt dann $i \equiv j \equiv 0 \bmod p$. Wählen wir $b_{ij} \in \overline{K}$ mit $b_{ij}^p = a_{pi,pj}$, so folgt

  $$f = \sum_{i,j} a_{pi,pj} x^{pi} y^{pj} = \sum_{i,j} (b_{ij} x^i y^j)^p = (\sum_{i,j} b_{ij} x^i y^j)^p,$$

  was der Irreduzibilität von f über $\overline{K}$ widerspricht. Also kann dieser Fall überhaupt nicht eintreten. ■

Beispiele:

- Wir betrachten C mit $y^2 = x^3$. Die Kurve wird gegeben durch das Polynom $f = y^2 - x^3$. Dann gilt
$$f = y^2 - x^3, \quad \frac{\partial f}{\partial x} = -3x^2, \quad \frac{\partial f}{\partial y} = 2y.$$
Man sieht dann sofort, dass die einzige Singularität der Punkt $P = (0, 0)$ ist. (Man unterscheide zunächst zwischen Charakteristik $\neq 2$ und $\neq 3$.)
- $f = x^2$ definiert eine Kurve C, die wegen $\frac{\partial f}{\partial x} = 2x$ und $\frac{\partial f}{\partial y} = 0$ für alle Punkte der Form $(0, y)$ singulär ist. D.h. alle Kurvenpunkte sind singulär.

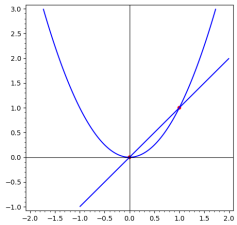
Schnittvielfachheiten: Sind C und D affine Kurven, so kann man eine Schnittvielfachheit $(C \cdot D)_P$ von C und D in einem Punkt $P \in \mathbb{A}^2$ definieren. Der Einfachkeit halber werden wir uns zunächst auf Schnitte von Kurven mit Geraden beschränken:

- Sei C eine Kurve und G eine Gerade, die nicht in C enthalten ist. Die Kurve C sei gegeben durch ein Polynom $f(x, y)$, für die Gerade G wählen wir eine Parametrisierung $x = \alpha + \beta t$, $y = \gamma + \delta t$, sodass $G = \{(\alpha + \beta t, \gamma + \delta t) : t \in \overline{K}\}$ gilt. Es gilt
$$C(\overline{K}) \cap G(\overline{K}) = \{(\alpha + \beta t, \gamma + \delta t) : f(\alpha + \beta t, \gamma + \delta t) = 0\}.$$
Wegen $G \not\subseteq C$ ist $f(\alpha + \beta t, \gamma + \delta t)$ nicht identisch 0, sodass wir das Polynom über dem algebraischen Abschluss in Linearfaktoren zerlegen können:
$$f(\alpha + \beta t, \gamma + \delta t) = c \prod_{i=1}^{r} (t - t_i)^{m_i}$$
mit $r \geq 0$, paarweise verschiedenen Zahlen $t_i \in \overline{K}$ und $m_i \in \mathbb{N}$. Setzen wir $P_i = (\alpha + \beta t_i, \gamma + \delta t_i)$, so gilt
$$C(\overline{K}) \cap G(\overline{K}) = \{P_1, \ldots, P_r\}.$$
- Die **Schnittmultiplizität** (oder auch **Schnittvielfachheit**) von C und G im Punkt P_i wird definiert durch
$$(C \cdot G)_{P_i} = m_i.$$
Ist $P \notin C(\overline{K}) \cap G(\overline{K})$, so setzt man $(C \cdot G)_P = 0$.
- Natürlich müsste man nun eigentlich noch zeigen, dass die Schnittmultiplizität unabhängig von der gewählten Geradenparametrisierung ist.

Bemerkung: Ist $P = (x_0, y_0) \in \mathbb{A}^2$, ist G eine Gerade durch P, so gibt es eine Parametrisierung $x = x_0 + \beta t$, $y = y_0 + \delta t$. Ist nun C eine durch $f(x, y) = 0$ definierte Kurve, setzt man die Parametrisierung in $f(x, y)$ ein, so kann man zerlegen
$$f(x_0 + \beta t, y_0 + \delta t) = t^m h(t) \quad \text{mit} \quad h(0) \neq 0.$$
Dann ist
$$(C \cdot G)_P = m.$$

Beispiel: Wir betrachten die durch $y = x^2$ bzw. $f(x, y) = y - x^2 = 0$ definierte Kurve C. Zunächst betrachten wir die Gerade G mit der Gleichung $y = x$.
Als Parametrisierung wählen wir $x = t$, $y = t$, denn es ist
$$G = \{(t, t) : t \in \overline{K}\}.$$
Einsetzen der Parametrisierung in die Kurvengleichung liefert
$$f(t, t) = t - t^2 = -t(t - 1).$$

Also erhält man für $t = 0$ und $t = 1$ jeweils Schnittpunkte mit Schnittmultiplizität 1, nämlich $P_1 = (0, 0)$ und $P_2 = (1, 1)$.



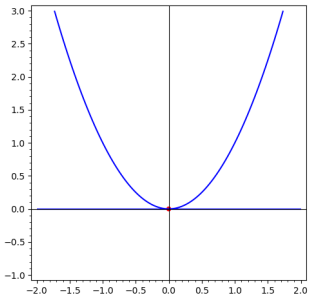
Nun betrachten wir wieder die Kurve $y = x^2$, die durch das Polynom $f(x, y) = y - x^2$ beschrieben wird, aber die Gerade G mit der Gleichung $y = 0$. Wegen

$$G = \{(x, 0) : x \in \overline{K}\} = \{(t, 0) : t \in \overline{K}\}$$

wählen wir als Parametrisierung $x = t$, $y = 0$. Einsetzen liefert

$$f(t, 0) = -t^2.$$

Den einzigen Schnittpunkt erhält man für $t = 0$, nämlich $P = (0, 0)$. Die Schnittmultiplizität ist $(C \cdot G)_P = 2$.

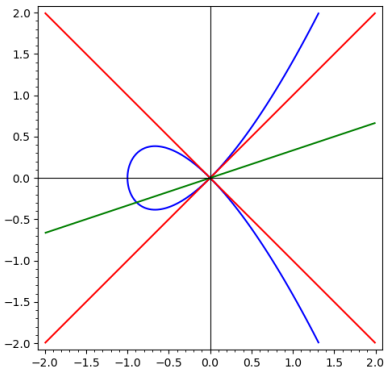


Bemerkung: Bei der Parametrisierung einer Geraden G muss man nicht künstlich einen Parameter t einführen, wenn eine andere Variable eventuell naheliegender ist. Wird die Gerade G beispielsweise durch $y = ax + b$ beschrieben, so ist

$$G = \{(x, ax + b) : x \in \overline{K}\},$$

sodass man auch x als Parameter verwenden kann.

Beispiel: Wir betrachten die Kurve C mit der Gleichung $y^2 = x^2 + x^3$, die durch das Polynom $f(x, y) = x^2 - y^2 + x^3$ beschrieben wird. Im Bild ist die Kurve zusammen mit den (rot gezeichneten) Tangenten im Nullpunkt $y = x$ und $y = -x$ zu sehen. Wir wollen den Schnittmultiplizität der Kurve mit einer durch den Nullpunkt gehenden Geraden (grün gezeichnet) bestimmen.



Wir betrachten zunächst Geraden G, die durch $y = ax$ beschrieben werden können:

$$G = \{(x, ax) : x \in \overline{K}\}.$$

Als Parametrisierung wählen wir $x = x$, $y = ax$ mit x als Parameter. (Für $x = 0$ erhält man den Nullpunkt.) Wir setzen in $f(x, y)$ ein:

$$f(x, ax) = x^2 - (ax)^2 + x^3 = (1 - a^2)x^2 + x^3.$$

- **Fall** $a = \pm 1$**:** Dann ist $f(x, ax) = x^3$, die Schnittmultiplizität ist 3. Die Geraden sind $y = x$ und $y = -x$, also die Tangenten im Punkt $(0, 0)$.
- **Fall** $a \neq \pm 1$**:** Dann ist

$$f(x, ax) = x^2 \cdot h(x) \text{ mit } h(x) = 1 - a^2 + x \text{ und } h(0) \neq 0.$$

  Die Schnittmultiplizität ist also 2.

Die einzige Gerade durch den Nullpunkt, die nicht in der Form $y = ax$ beschrieben werden kann, ist die Gerade G mit der Gleichung $x = 0$.
Wegen

$$G = \{(0, y) : y \in \overline{K}\}$$

wählen wir als Parametrisierung $x = 0$, $y = y$ mit dem Parameter y.
Einsetzen in $f(x, y)$ liefert

$$f(0, y) = -y^2,$$

die Schnittmultiplizität ist also 2.
Ergebnis: Sei G eine Gerade durch den Nullpunkt. Dann gilt:

$$(C \cdot G)_{(0,0)} = \begin{cases} 3, & \text{falls } G \text{ eine Tangente ist,} \\ 2, & \text{sonst.} \end{cases}$$

Das vorangegangene Beispiel wird in folgendem Satz verallgemeinert.

Satz. *Sei C eine durch $f(x, y)$ definierte ebene affine Kurve, P ein Punkt von C der Multiplizität $m \geq 1$, sowie G eine Gerade durch P, gegeben durch $a+bx+cy$. Wir setzen voraus, dass $a+bx+cy$ das Polynom $f(x, y)$ nicht teilt. Dann gilt:*

$$(C \cdot G)_P \begin{cases} = m & \textit{falls } G \textit{ keine Tangente ist,} \\ \geq m + 1 & \textit{falls } G \textit{ Tangente ist.} \end{cases}$$

Beweis: Wir können o.E. $P = (0, 0)$ annehmen. Wir schreiben

$$f(x, y) = f_m(x, y) + f_{m+1}(x, y) + \dots,$$

wobei $f_\ell(x, y)$ homogen vom Grad ℓ ist. Wir faktorisieren

$$f_m(x, y) = \prod_{i=1}^{m} (\lambda_i x + \mu_i y) \quad \text{mit} \quad \lambda_i, \mu_i \in \overline{K}.$$

Die Tangenten sind gegeben durch $\lambda_i x + \mu_i y = 0$ für $i = 1, \dots, m$. Die Gerade G können wir in der Form $x = \alpha t$, $y = \beta t$ parametrisieren. Die Schnittmultiplizität $(C \cdot G)_P$ ist die Vielfachheit der Nulltstelle $t = 0$ in $f(\alpha t, \beta t)$. Daher berechnen wir

$$\begin{aligned} f(\alpha t, \beta t) &= f_m(\alpha t, \beta t) + f_{m+1}(\alpha t, \beta t) + \dots = t^m f_m(\alpha, \beta) + t^{m+1} f_{m+1}(\alpha, \beta) + \dots = \\ &= t^m \left(f_m(\alpha, \beta) + t f_{m+1}(\alpha, \beta) + \dots \right) = \\ &= t^m \left(\prod_{i=1}^{m} (\lambda_i \alpha + \mu_i \beta) + t f_{m+1}(\alpha, \beta) + \dots \right). \end{aligned}$$

Wir unterscheiden zwei Fälle:

- Es gibt ein j mit $\lambda_j\alpha + \mu_j\beta = 0$: Dann ist

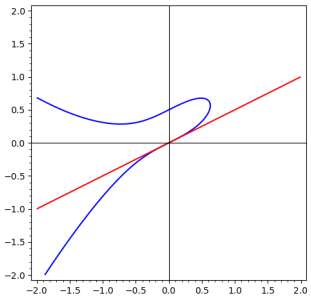
$$G = \{(\alpha t, \beta t) : t \in \overline{K}\} \subseteq \{\lambda_j x + \mu_j y = 0\}, \quad \text{also} \quad G = \{\lambda_j x + \mu_j y = 0\},$$

  d.h. G ist Tangente. Wegen $\prod_{i=1}^m (\lambda_i\alpha + \mu_i\beta) = 0$ folgt $f(\alpha t, \beta t) = t^{m+1}(\dots)$, sodass $(C \cdot G)_P \geq m+1$ gilt, wie behauptet.
- Für alle i ist $\lambda_i\alpha + \mu_i\beta \neq 0$. Dann ist

$$G = \{(\alpha t, \beta t) : t \in \overline{K}\} \not\subseteq \{\lambda_i x + \mu_i y = 0\}, \quad \text{also} \quad G \neq \{\lambda_i x + \mu_i y = 0\},$$

  also G keine Tangente. Wegen $\prod_{i=1}^m (\lambda_i\alpha + \mu_i\beta) \neq 0$ kann hier aus $f(\alpha t, \beta t)$ genau t^m ausgeklammert werden, sodass $(C \cdot G)_P = m$ gilt. Dies beweist die Behauptung. ■

DEFINITION. *Ein nichtsingulärer Punkt P einer ebenen affinen Kurve C heißt* **Wendepunkt**, *falls die Tangente T die Kurve C mit Multiplizität ≥ 3 in P schneidet. Die Tangente nennt man dann eine Wendetangente von C.*



Beispiel: Wir betrachten die durch $y = x^n$ definierte ebene affine Kurve C für $n \geq 2$. Ein beschreibendes Polynom ist also $f(x, y) = x^n - y$. Was passiert im Kurvenpunkt $P = (0, 0)$? Die Taylorentwicklung ist dort $f(x, y) = -y + x^n$ (wegen $n \geq 2$), also ist $(0, 0)$ ein nichtsingulärer Punkt mit der durch $y = 0$ gegebenen Tangente T. Wie oft schneidet die Tangente die Kurve im Nullpunkt? Wegen

$$T = \{(x, 0) : x \in \overline{K}\}$$

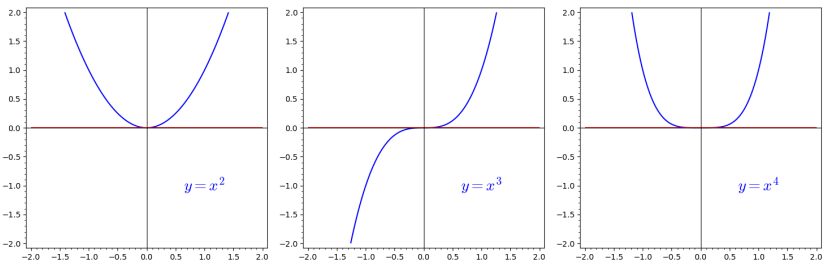
wählen wir als Parametrisierung $x = x$, $y = 0$ (mit Parameter x). Einsetzen in die Kurvengleichung ergibt

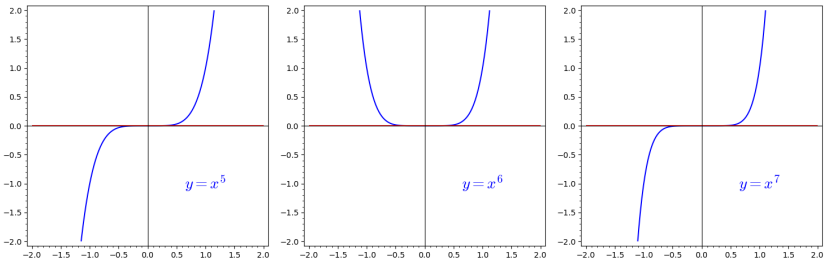
$$f(x, 0) = x^n.$$

Die Schnittmultiplizität ist also n:

$$(C \cdot T)_{(0,0)} = n.$$

Im Fall $n \geq 3$ ist $(0, 0)$ ein Wendepunkt und T die zugehörige Wendetangente.





Beispiel: Wir betrachten über $\mathbb{R}$ die Kurve $f = 0$ mit

$$f = x^3 + x^2 - 4xy + 4y^2 + x - 2y.$$

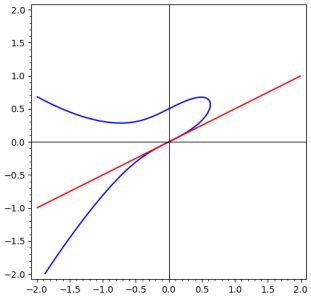
$(0, 0)$ ist offensichtlich ein nichtsingulärer Punkt mit Tangente $x = 2y$.
Die Tangente ist

$$T = \{(2y, y) : y \in \mathbb{C}\},$$

also wählen wir als Parametrisierung $x = 2y$, $y = y$ und als Parameter y.
Wir setzen diese in das Polynom f ein:

$$f(2y, y) = (2y)^3 + (2y)^2 - 4(2y)y + 4y^2 + 2y - 2y = 8y^3.$$

Die Tangente schneidet die Kurve in $(0, 0)$ mit Multiplizität 3. Also ist $(0, 0)$ ein Wendepunkt und die Tangente Wendetangente.



KAPITEL 3

Projektive Räume, projektive algebraische Mengen und ebene projektive Kurven

Projektive Räume sollen affine Räume vervollständigen bzw. kompaktifizieren.

1. Projektive Räume

DEFINITION.

- *Auf* $\mathbb{A}^{n+1} \setminus \{0\}$ *wird wie folgt eine Äquivalenzrelation definiert:*

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff b_0 = \lambda a_0, \ldots b_n = \lambda a_n \text{ für ein } \lambda \in \overline{K}^* \iff$$
$$\iff (b_0, \ldots, b_n) = (\lambda a_0, \ldots, \lambda a_n) \text{ für ein } \lambda \in \overline{K}^*.$$

- *Die Äquivalenzklasse von* $(a_0, \ldots, a_n)$ *wird mit* $(a_0 : \cdots : a_n)$ *bezeichnet. Dann gilt also*

$$(a_0 : \cdots : a_n) = (b_0 : \cdots : b_n) \iff (b_0, \ldots, b_n) = (\lambda a_0, \ldots, \lambda a_n) \text{ für ein } \lambda \in \overline{K}^*$$

und

$$(a_0 : a_1 : \cdots : a_n) = (\lambda a_0 : \lambda a_1 : \cdots : \lambda a_n) \text{ für alle } \lambda \in \overline{K}^*.$$

- *Die Menge der Äquivalenzklassen heißt n-dimensionaler projektiver Raum* $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$*. Also*

$$\mathbb{P}^n = \{(a_0 : \cdots : a_n) : (a_0, \ldots, a_n) \in \overline{K}^{n+1} \setminus \{0\}\}.$$

- $\mathbb{P}^1$ *bezeichnet man als projektive Gerade,* $\mathbb{P}^2$ *als projektive Ebene.*
- *Wie im affinen Fall definiert man die Menge der* K*-rationalen Punkte von* $\mathbb{P}^n$ *durch*

$$\mathbb{P}^n(K) = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n : a_i \in K\}.$$

Beispiel: In der projektiven Ebene $\mathbb{P}^2$ über $\mathbb{Q}$ gilt:

$$(2 : 3 : 5) = (1 : \frac{3}{2} : \frac{5}{2}) = (\frac{2}{3} : 1 : \frac{5}{3}) = (\frac{2}{5} : \frac{3}{5} : 1) = (-4 : -6 : -10) = \ldots$$

Bemerkung: Aus $(a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n(K)$ folgt noch nicht $a_i \in K$, wie das Beispiel

$$(\sqrt{2} : \frac{1}{\sqrt{2}}) = (2 : 1) \in \mathbb{P}^1(\mathbb{Q}) \text{ mit } \sqrt{2} \notin \mathbb{Q}$$

zeigt.

Da die Elemente von $\mathbb{P}^n$ Äquivalenzklassen sind, ist es sinnvoll, ein Repräsentantensystem anzugeben. Wir machen dies zunächst für $\mathbb{P}^1$ und $\mathbb{P}^2$.

- **Ein Repräsentantensystem für** $\mathbb{P}^1$**.** Sei $(a : b) \in \mathbb{P}^1$. Dann ist $a \neq 0$ oder $b \neq 0$.
  - **Fall** $a \neq 0$**:** Hier ist $(a : b) = (1 : \frac{b}{a})$.
  - **Fall** $a = 0$**:** Da dann $b \neq 0$ ist, folgt $(a : b) = (0 : b) = (0 : 1)$.

  Damit erhalten wir

$$\mathbb{P}^1 = \{(1 : x) : x \in \overline{K}\} \cup \{(0 : 1)\}.$$

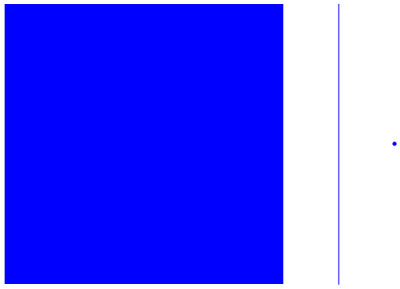
  Wegen

$$(1 : x) = (1 : x') \iff x = x' \quad \text{und} \quad (1 : x) \neq (0 : 1)$$

handelt es sich tatsächlich um ein Repräsentantensystem. Mengenmäßig entsteht $\mathbb{P}^1$ also, indem man zu $\mathbb{A}^1 \simeq \overline{K}$ einen Punkt hinzunimmt. Das folgende Bild ist nur mengenmäßig zu verstehen.

- **Ein Repräsentantensystem für $\mathbb{P}^2$.** Sei $(a : b : c) \in \mathbb{P}^2$.
  - **Fall $a \neq 0$:** Dann ist $(a : b : c) = (1 : \frac{b}{a} : \frac{c}{a})$.
  - **Fall $a = 0$, $b \neq 0$:** Dann ist $(a : b : c) = (0 : b : c) = (0 : 1 : \frac{c}{b})$.
  - **Fall $a = 0$, $b = 0$:** Da $c \neq 0$ gilt, folgt $(a : b : c) = (0 : 0 : c) = (0 : 0 : 1)$.

  Wir erhalten
  $$\mathbb{P}^2 = \{(1 : x : y) : x, y \in \overline{K}\} \cup \{(0 : 1 : z) : z \in \overline{K}\} \cup \{(0 : 0 : 1)\}.$$
  (Auch hier handelt es sich um ein Repräsentantensystem.) Mengenmäßig entsteht $\mathbb{P}^2$ also, indem man zu $\mathbb{A}^2 \simeq \overline{K}^2$ eine Gerade $\mathbb{A}^1 \simeq \overline{K}$ und einen Punkt hinzunimmt. Das folgende Bild soll diese mengenmäßige Zerlegung darstellen:



Überdeckung der projektiven Ebene $\mathbb{P}^2$ durch affine Ebenen $\mathbb{A}^2$: Wir definieren für $i = 0, 1, 2$
$$U_i = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_i \neq 0\} \text{ und } H_i = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_i = 0\},$$
sodass sich also eine disjunkte Zerlegung $\mathbb{P}^2 = U_i \cup H_i$ ergibt.
Wir definieren
$$\begin{aligned} \phi_0 &: \mathbb{A}^2 \to U_0, \qquad (x, y) \mapsto (1 : x : y), \\ \phi_1 &: \mathbb{A}^2 \to U_1, \qquad (u, v) \mapsto (u : 1 : v), \\ \phi_2 &: \mathbb{A}^2 \to U_2, \qquad (r, s) \mapsto (r : s : 1). \end{aligned}$$
Die Abbildungen ϕ_i sind bijektiv mit den Umkehrabbildungen
$$\begin{aligned} \phi_0^{-1} &: U_0 \to \mathbb{A}^2, \qquad (x_0 : x_1 : x_2) \mapsto (\frac{x_1}{x_0}, \frac{x_2}{x_0}), \\ \phi_1^{-1} &: U_1 \to \mathbb{A}^2, \qquad (x_0 : x_1 : x_2) \mapsto (\frac{x_0}{x_1}, \frac{x_2}{x_1}), \\ \phi_2^{-1} &: U_2 \to \mathbb{A}^2, \qquad (x_0 : x_1 : x_2) \mapsto (\frac{x_0}{x_2}, \frac{x_1}{x_2}). \end{aligned}$$
Wir können also U_i mit $\mathbb{A}^2$ identifizieren. Zur Unterscheidung verwenden wir in U_0 die affinen Koordinaten x, y, in U_1 die affinen Koordinaten u, v und in U_2 die affinen Koordinaten r, s.

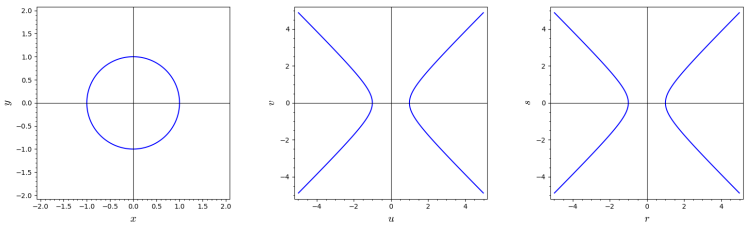
Natürlich gilt
$$\mathbb{P}^2 = U_0 \cup U_1 \cup U_2.$$

Beispiel: Wir betrachten (über $\mathbb{R}$)

$$X = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_1^2 + x_2^2 = x_0^2\}.$$

Es ist

$$\begin{aligned} X \cap U_0 &= \{(1 : x : y) : x^2 + y^2 = 1\}, \\ X \cap U_1 &= \{(u : 1 : v) : u^2 - v^2 = 1\}, \\ X \cap U_2 &= \{(r : s : 1) : r^2 - s^2 = 1\}. \end{aligned}$$



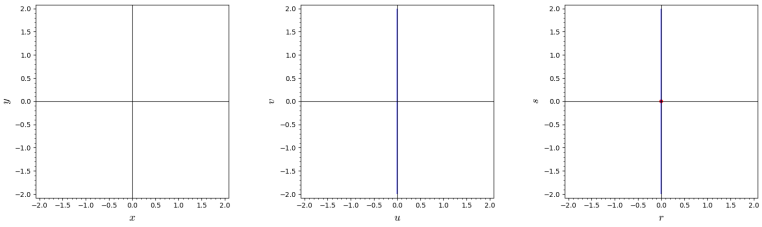
X schaut in U_0 wie ein Kreis $x^2 + y^2 = 1$, in U_1 und U_2 wie eine Hyperbel $x^2 - y^2 = 1$ aus. Kreis und Hyperbel sind also nur verschiedene affine Ansichten von $x_1^2 + x_2^2 = x_0^2$.

Beispiel: Wir betrachten in $\mathbb{P}^2$

$$H_0 = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_0 = 0\}.$$

Es ist

$$\begin{aligned} H_0 \cap U_0 &= \emptyset, \\ H_0 \cap U_1 &= \{(u : 1 : v) : u = 0\}, \\ H_0 \cap U_2 &= \{(r : s : 1) : r = 0\}. \end{aligned}$$



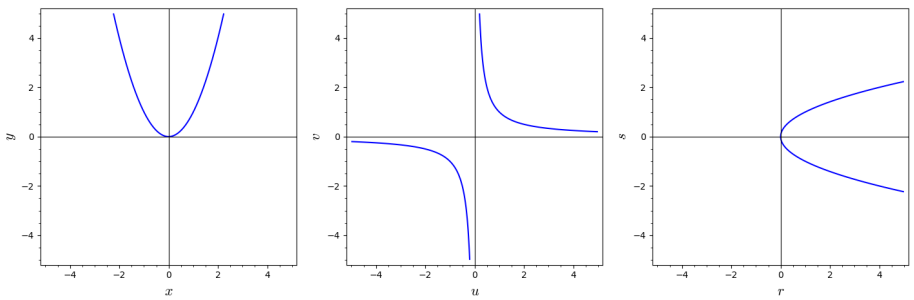
In U_0 ist kein Punkt von H_0 zu sehen. In U_1 sind fast alle Punkte von H_0 zu sehen, bis auf den Punkt $(0 : 0 : 1)$, der nur in U_2 mit den Koordinaten $(r, s) = (0, 0)$ zu sehen ist (und hier rot gezeichnet ist).

Beispiel: Wir betrachten (über $\mathbb{R}$)

$$X = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_0 x_2 - x_1^2 = 0\}.$$

Es ist

$$\begin{aligned} X \cap U_0 &= \{(1 : x : y) : y = x^2\}, \\ X \cap U_1 &= \{(u : 1 : v) : uv = 1\}, \\ X \cap U_2 &= \{(r : s : 1) : r = s^2\}. \end{aligned}$$



X schaut in U_0 wie eine Parabel, in U_1 wie eine Hyperbel, in U_2 wie eine Parabel aus. Hyperbel und Parabel sind also nur verschiedene affine Ansichten von $x_0x_2 - x_1^2 = 0$.

Überdeckung von $\mathbb{P}^n$ durch affine Räume $\mathbb{A}^n$: Wir definieren für $i = 0, 1, 2, \ldots, n$

$$\begin{aligned} U_i &= \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n : x_i \neq 0\}, \\ H_i &= \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n : x_i = 0\}, \end{aligned}$$

sodass sich eine disjunkte Zerlegung $\mathbb{P}^n = U_i \cup H_i$ ergibt. Wir definieren

$$\begin{aligned} \phi_0 : \mathbb{A}^n \to U_0, &\qquad (x_1, x_2, \ldots, x_n) \mapsto (1 : x_1 : x_2 : \cdots : x_n), \\ \phi_1 : \mathbb{A}^n \to U_1, &\qquad (x_1, x_2, \ldots, x_n) \mapsto (x_1 : 1 : x_2 : \cdots : x_n), \\ \vdots &\quad \vdots \\ \phi_n : \mathbb{A}^n \to U_n, &\qquad (x_1, x_2, \ldots, x_n) \mapsto (x_1 : x_2 : \cdots : x_n : 1). \end{aligned}$$

Die Abbildungen ϕ_i sind bijektiv mit den Umkehrabbildungen

$$\phi_i^{-1} : U_i \to \mathbb{A}^n, \quad (x_0 : x_1 : \cdots : x_n) \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}).$$

Wir können also U_i mit $\mathbb{A}^n$ identifizieren.

Überdeckung von $\mathbb{P}^1$ durch affine Geraden $\mathbb{A}^1$: Wir definieren für $i = 0, 1$

$$U_i = \{(x_0 : x_1) \in \mathbb{P}^1 : x_i \neq 0\} \text{ und } H_i = \{(x_0 : x_1) \in \mathbb{P}^1 : x_i = 0\},$$

sodass wir eine disjunkte Zerlegung $\mathbb{P}^1 = U_i \cup H_i$ haben. H_i ist jeweils nur ein Punkt:

$$H_0 = \{(0 : 1)\} \quad \text{und} \quad H_1 = \{(1 : 0)\}.$$

Wir definieren

$$\begin{aligned} \phi_0 : \mathbb{A}^1 \to U_0, &\qquad x \mapsto (1 : x), \\ \phi_1 : \mathbb{A}^1 \to U_1, &\qquad u \mapsto (u : 1). \end{aligned}$$

Die Abbildungen ϕ_i sind bijektiv mit den Umkehrabbildungen

$$\begin{aligned} \phi_0^{-1} : U_0 \to \mathbb{A}^1, &\qquad (x_0 : x_1) \mapsto \frac{x_1}{x_0}, \\ \phi_1^{-1} : U_1 \to \mathbb{A}^1, &\qquad (x_0 : x_1) \mapsto \frac{x_0}{x_1}. \end{aligned}$$

Wir können daher U_i mit $\mathbb{A}^1$ bzw. $\overline{K}$ identifizieren. Zur Unterscheidung verwenden wir in U_0 die affine Koordinate x, in U_1 die affine Koordinate u. Natürlich gilt $\mathbb{P}^1 = U_0 \cup U_1$.

Wir betrachten nochmals einen Punkt $P = (x_0 : x_1) \in \mathbb{P}^1$.

- **Fall $x_0 \neq 0$, $x_1 \neq 0$:** Dann ist

  $$P = (x_0 : x_1) = (1 : \frac{x_1}{x_0}) = (\frac{x_0}{x_1} : 1).$$

  Der Punkt hat also in U_0 die Koordinate $x = \frac{x_1}{x_0}$, in U_1 die Koordinate $u = \frac{x_0}{x_1}$. Insbesondere gilt $u = \frac{1}{x}$.
- **Fall $x_0 = 0$:** Dann ist $x_1 \neq 0$ und damit $P = (0 : 1)$. In U_0 ist der Punkt P nicht zu sehen, in U_1 hat der Punkt die Koordinate $u = 0$.
- **Fall $x_1 = 0$:** Dann ist $x_0 \neq 0$ und daher $P = (1 : 0)$. In U_0 hat der Punkt P die Koordinate $x = 0$, in U_1 ist der Punkt nicht zu sehen.

Einbettung von $\mathbb{A}^n$ in $\mathbb{P}^n$: Mit obiger Abbildung ϕ_0 identifiziert man oft $\mathbb{A}^n$ mit U_0, d.h. man denkt sich $\mathbb{A}^n$ als Teilmenge von $\mathbb{P}^n$:

$$\mathbb{A}^n \simeq U_0 \subseteq \mathbb{P}^n, \quad (x_1, \ldots, x_n) \simeq (1 : x_1 : \cdots : x_n).$$

Damit ist

$$\mathbb{P}^n \setminus \mathbb{A}^n = H_0 = \{(0 : x_1 : \cdots : x_n) \in \mathbb{P}^n\} \simeq \mathbb{P}^{n-1}.$$

H_0 wird auch die „unendlich ferne Hyperebene“, im Fall $n = 1$ der „unendlich ferne Punkt“, im Fall $n = 2$ die „unendlich ferne Gerade“ genannt.

Im Fall $\mathbb{P}^1$ schreibt man auch $\infty = (0:1)$ und hat dann

$$\mathbb{P}^1 = \{(1:x) : x \in \overline{K}\} \cup \{\infty\}.$$

(Der unendlich ferne Punkt ∞ hat die u-Koordinate 0.)

2. Projektive algebraische Mengen

Vorbemerkung: Wir wollen nun algebraische Teilmengen im $\mathbb{P}^n$ definieren als Nullstellenmenge von Polynomen, wie wir das auch bei den algebraischen Teilmengen von $\mathbb{A}^n$ gemacht haben.
Man kann aber Polynome $f \in \overline{K}[x_0, x_1, \ldots, x_n]$ nicht einfach als Funktionen auf $\mathbb{P}^n$ auffassen, indem man einen Repräsentanten eines Punkts in ein Polynom einsetzt, wie folgendes Beispiel zeigen soll:

Beispiel: Wir betrachten das Polynom $f = 1 + x_0$ und den Punkt

$$P = (1:2) \in \mathbb{P}^1.$$

Repräsentanten von P sind die Paare $(\lambda, 2\lambda)$ (mit $\lambda \neq 0$). Nun ist

$$f(\lambda, 2\lambda) = 1 + \lambda.$$

Also nimmt f auf verschiedenen Repräsentanten von P verschiedene Werte an. Daher kann man „$f(P)$“ auf diese Weise nicht definieren.
Um die Nullstellenmenge eines Polynoms f in $\mathbb{P}^n$ zu definieren, werden wir folgende Bedingung an das Polynom f stellen: Für alle Punkte $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n$ wollen wir haben, dass gilt

$$f(a_0, \ldots, a_n) = 0 \quad \Longleftrightarrow \quad f(\lambda a_0, \ldots, \lambda a_n) = 0 \text{ für alle } \lambda \in \overline{K}.$$

Dann liegt nämlich einer der beiden Fälle vor:

- $f(a_0, \ldots, a_n) = 0$ für alle $(a_0, \ldots, n)$ mit $P = (a_0 : \cdots : a_n)$. (Wir schreiben dafür auch $f(P) = 0$.)
- $f(a_0, \ldots, a_n) \neq 0$ für alle $(a_0, \ldots, n)$ mit $P = (a_0 : \cdots : a_n)$. (Wir schreiben dafür auch $f(P) \neq 0$.)

Diese Bedingung wird von den sogenannten homogenen Polynomen erfüllt.
Ein Polynom $f(x_0, x_1, \ldots, x_n) \in \overline{K}[x_0, x_1, \ldots, x_n]$ heißt **homogen vom Grad** d, falls gilt

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n) \text{ für alle } \lambda \in \overline{K}.$$

Äquivalent dazu ist, dass in f nur Monome vom Grad d auftreten, d.h. f hat die Form

$$f = \sum_{i_0 + \cdots + i_n = d} a_{i_0 \ldots i_n} x_0^{i_0} \ldots x_n^{i_n}.$$

Daher ist für $P \in \mathbb{P}^n$ die Aussage $f(P) = 0$ oder $f(P) \neq 0$ sinnvoll, d.h. unabhängig vom ausgewählten Repräsentanten für P.

Beispiele: In $\overline{K}[x_0, x_1, x_2]$ haben die homogenen Polynome vom Grad 1 die Gestalt

$$a_0 x_0 + a_1 x_1 + a_2 x_2,$$

die homogenen Polynome vom Grad 2 sehen so aus:

$$a_0 x_0^2 + a_1 x_0 x_1 + a_2 x_0 x_2 + a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2.$$

Satz (Eulersche Relation). *Ist $f \in \overline{K}[x_0, x_1, \ldots, x_n]$ ein homogenes Polynom vom Grad d, so gilt*

$$d \cdot f = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i} \cdot x_i.$$

Beweis: Seien $p_0, p_1, \ldots, p_n \in \overline{K}$ beliebig gegeben. Wir definieren

$$g(t) = f(tp_0, tp_1, \ldots, tp_n).$$

Die Kettenregel liefert

$$g'(t) = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(tp_0, \ldots, tp_n) \cdot p_i, \text{ also } g'(1) = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p_0, \ldots, p_n) \cdot p_i.$$

Da f homogen vom Grad d ist, gilt aber auch

$$g(t) = t^d f(p_0, \ldots, p_n).$$

Differenzieren liefert

$$g'(t) = dt^{d-1} f(p_0, \ldots, p_n) \text{ und } g'(1) = df(p_0, \ldots, p_n).$$

Vergleich der beiden Darstellungen für $g'(1)$ ergibt

$$d \cdot f(p_0, \ldots, p_n) = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(p_0, \ldots, p_n) \cdot p_i.$$

Da die Gleichung für alle $p_0, p_1, \ldots, p_n \in \overline{K}$ gilt, gilt sie auch für die Polynome. ■

DEFINITION. *Eine Teilmenge $X \subseteq \mathbb{P}^n$ heißt* **algebraische Teilmenge in** $\mathbb{P}^n$*, falls es homogene Polynome $f_1, \ldots, f_r \in \overline{K}[x_0, \ldots, x_n]$ gibt mit*

$$X = \{P \in \mathbb{P}^n : f_1(P) = \cdots = f_r(P) = 0\} = \{f_1 = \cdots = f_r = 0\}.$$

Man sagt, die algebraische Menge $X \subseteq \mathbb{P}^n$ ist über K definiert, falls es Polynome $g_1, \ldots, g_s \in K[x_0, \ldots, x_n]$ gibt mit $X = \{g_1 = \cdots = g_s = 0\}$. In diesem Fall heißt

$$X(K) = X \cap \mathbb{P}^n(K)$$

die Menge der K-rationalen Punkte von X.

Bemerkung: Wir haben den Begriff „algebraische Menge“ für Teilmengen von $\mathbb{A}^n$ und für Teilmengen von $\mathbb{P}^n$ definiert. Zur Unterscheidung sprechen wir deswegen auch manchmal von **affinen algebraischen** und **projektiven algebraischen** Mengen.
Beispiele:

- $\mathbb{P}^n = \{0 = 0\}$ und $\emptyset = \{x_0 = x_1 = \cdots = x_n = 0\}$ sind algebraische Teilmengen des $\mathbb{P}^n$.
- Ein Punkt $P = (p_0 : p_1 : \cdots : p_n) \in \mathbb{P}^n$ ist eine algebraische Teilmenge des $\mathbb{P}^n$, denn es gilt
$$\{P\} = \{p_j x_i - p_i x_j = 0 \text{ für alle } i, j\}.$$
- Sind $X = \{f_1 = \cdots = f_r = 0\}$ und $Y = \{g_1 = \cdots = g_s = 0\}$ algebraische Teilmengen des $\mathbb{P}^n$, so auch
$$X \cup Y = \{f_1 g_1 = \cdots = f_1 g_s = \cdots = f_r g_1 = \cdots = f_r g_s = 0\}$$
und
$$X \cap Y = \{f_1 = \cdots = f_r = g_1 = \cdots = g_s = 0\}.$$
- Man kann auch zeigen, dass beliebige Durchschnitte algebraischer Mengen des $\mathbb{P}^n$ wieder algebraisch sind.

Bemerkung: Die algebraischen Teilmengen des $\mathbb{P}^n$ erfüllen die Axiome für die abgeschlossenen Teilmengen einer Topologie. Man nennt diese Topologie die **Zariski-Topologie**.
Als konkretes geometrisches Objekt wollen wir uns zunächst die Geraden in $\mathbb{P}^2$ etwas genauer anschauen:

DEFINITION. *Eine* **Gerade** *in $\mathbb{P}^2$ ist eine Teilmenge der Gestalt*

$$G = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : a_0 x_0 + a_1 x_1 + a_2 x_2 = 0\}$$

mit $a_0, a_1, a_2 \in \overline{K}$ und $(a_0, a_1, a_2) \neq 0$.

Die „unendlich ferne Gerade“ $H_0 = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_0 = 0\}$ ist also die durch $x_0 = 0$ definierte Gerade.

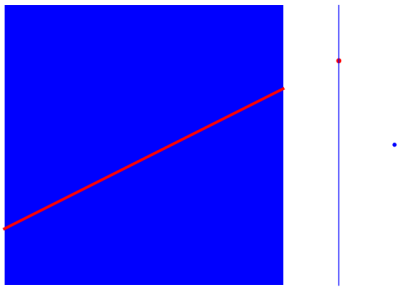
Es ist klar, dass für $\lambda \neq 0$ durch $a_0 x_0 + a_1 x_1 + a_2 x_2 = 0$ und $\lambda a_0 x_0 + \lambda a_1 x_1 + \lambda a_2 x_2 = 0$ die gleichen Geraden definiert werden.

Der affine Teil von Geraden im $\mathbb{P}^2$: Wir denken uns $\mathbb{A}^2 \simeq U_0 = \{(1 : x : y) : x, y \in \overline{K}\} \subseteq \mathbb{P}^2$. Es ist $\mathbb{P}^2 \setminus U_0 = H_0 = \{(0 : x_1 : x_2) \in \mathbb{P}^2\}$.
Sei G gegeben durch $a_0x_0 + a_1x_1 + a_2x_2 = 0$ (mit $(a_0, a_1, a_2) \neq 0$). Dann ist

$$\begin{aligned} G \cap U_0 &= \{(1 : x : y) \in \mathbb{P}^2 : a_0 + a_1x + a_2y = 0\}, \\ G \cap H_0 &= \{(0 : x_1 : x_2) \in \mathbb{P}^2 : a_1x_1 + a_2x_2 = 0\}. \end{aligned}$$

Wir unterscheiden zwei Fälle:

- Ist $(a_1, a_2) \neq (0, 0)$, so ist $G \cap U_0$ also die affine Gerade $a_0 + a_1x + a_2y = 0$ und $G \cap H_0 = \{(0 : a_2 : -a_1)\}$ besteht aus einem Punkt.



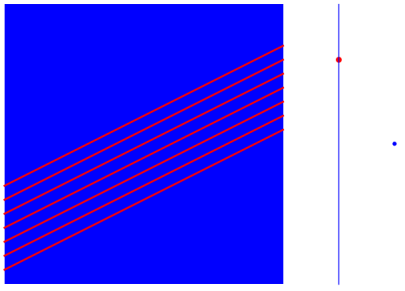
- Ist $(a_1, a_2) = (0, 0)$, so ist $G \cap U_0 = \emptyset$ und $G = H_0$.

Bis auf die unendlich ferne Gerade H_0 sieht man also alle Geraden von $\mathbb{P}^2$ als affine Geraden im endlichen Teil $\mathbb{A}^2$.
Man überlegt sich nun schnell, dass die Zuordnung

$$\{\text{Geraden in } \mathbb{P}^2\} \setminus \{H_0\} \to \{\text{Geraden in } \mathbb{A}^2\}, \quad G \mapsto G \cap U_0$$

eine Bijektion ist. (Der Geraden $a_0x_0 + a_1x_1 + a_2x_2 = 0$ im $\mathbb{P}^2$ wird die Gerade $a_0 + a_1x + a_2y = 0$ im $\mathbb{A}^2$ zugeordnet.)
Welche Punkte haben affine Geraden im Unendlichen? Nach der letzten Bemerkung können wir jede affine Gerade uns denken als $G \cap U_0$ bzw. $G \cap \mathbb{A}^2$ mit einer projektiven Geraden G. Was ist dann $G \cap H_0$?

- Die affine Gerade $y = ax + b$ ist der endliche Teil der projektiven Geraden $bx_0 + ax_1 - x_2 = 0$. Der Schnitt mit $H_0 = \{x_0 = 0\}$ ergibt den Punkt $(0 : 1 : a)$. (Variiert man b, so erhält man parallele Geraden, die sich im Unendlichen im Punkt $(0 : 1 : a)$ schneiden.)



- Die affine Gerade $x = c$ ist der endliche Teil der projektiven Geraden $cx_0 - x_1 = 0$. Der Schnitt mit H_0 ergibt den Punkt $(0 : 0 : 1)$. (Verschiedene Werte von c ergeben parallele Geraden im Endlichen.)

Wir sehen insbesondere: Schneiden sich zwei Geraden auf der unendlich fernen Geraden, so sind ihre affinen Teile parallele Geraden.
Weitere Betrachtungen zu Geraden in der projektiven Ebene $\mathbb{P}^2$:

- Zwei Geraden

$$\begin{aligned} G_1 &= \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}, \\ G_2 &= \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : b_0x_0 + b_1x_1 + b_2x_2 = 0\} \end{aligned}$$

können in folgenden Beziehungen stehen:
  – Sind (a_0, a_1, a_2) und (b_0, b_1, b_2) linear unabhängig, so gilt
$$G_1 \cap G_2 = \{(p_0 : p_1 : p_2)\},$$
wobei (p_0, p_1, p_2) durch
$$\begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$
bis auf eine multiplikative Konstante eindeutig bestimmt ist. (G_1 und G_2 schneiden sich in einem Punkt.)
  – Sind (a_0, a_1, a_2) und (b_0, b_1, b_2) linear abhängig, so gilt offensichtlich
$$G_1 = G_2.$$
(G_1 und G_2 sind identisch.)

- Seien $P = (p_0 : p_1 : p_2)$ und $Q = (q_0 : q_1 : q_2)$ zwei verschiedene Punkte in $\mathbb{P}^2$.
  – Es gibt genau eine Gerade G, die P und Q enthält, nämlich $G = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$, wobei (a_0, a_1, a_2) eine nichttriviale Lösung der Gleichung
$$\begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
ist. (Je zwei nichttriviale Lösungen unterscheiden sich nur um eine multiplikative Konstante.)
  – Alternativ kann man die G beschreibende lineare Gleichung auch in der Form
$$\begin{vmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \\ x_0 & x_1 & x_2 \end{vmatrix} = 0$$
angeben.
  – Man kann die Gerade durch P und Q auch in parametrisierter Form angeben:
$$G = \{(p_0u + q_0v : p_1u + q_1v : p_2u + q_2v) \in \mathbb{P}^2 : (u : v) \in \mathbb{P}^1\}.$$
- Da $a_0x_0 + a_1x_1 + a_2x_2 = 0$ und $b_0x_0 + b_1x_1 + b_2x_2 = 0$ genau dann die gleiche Gerade in $\mathbb{P}^2$ definieren, wenn gilt $(a_0 : a_1 : a_2) = (b_0 : b_1 : b_2)$, so ist klar, dass die Zuordnung
$$\mathbb{P}^2 \to \{\text{Geraden in } \mathbb{P}^2\}, \quad (a_0 : a_1 : a_2) \mapsto \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$$
eine Bijektion ist. Man sagt: Die Geraden in $\mathbb{P}^2$ bilden wieder einen $\mathbb{P}^2$.
- Drei Punkte $P = (p_0 : p_1 : p_2)$, $Q = (q_0 : q_1 : q_2)$, $R = (r_0 : r_1 : r_2)$ der projektiven Ebene $\mathbb{P}^2$ liegen genau dann auf einer Geraden, wenn gilt
$$\det \begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \\ r_0 & r_1 & r_2 \end{pmatrix} = 0.$$
Eine zugehörige Gerade G mit der Gleichung $a_0x_0 + a_1x_1 + a_2x_2 = 0$ ergibt sich dann aus der Bedingung
$$\begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \\ r_0 & r_1 & r_2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = 0.$$

Bemerkung: Ist $X \subseteq \mathbb{P}^n$ eine projektive algebraische Menge, gegeben durch
$$X = \{f_1(x_0, \ldots, x_n) = \cdots = f_r(x_0, \ldots, x_n) = 0\},$$
wo die f_i's homogene Polynome sind, so ist $X \cap \mathbb{A}^n$ eine affine algebraische Menge, gegeben durch die Gleichungen
$$X \cap \mathbb{A}^n = \{f_1(1, x_1, \ldots, x_n) = \cdots = f_r(1, x_1, \ldots, x_n) = 0\}.$$

Wichtiger ist die Umkehrung:

DEFINITION. *Ist $X \subseteq \mathbb{A}^n$ eine affine algebraische Menge, so denken wir uns X mit $X \subseteq \mathbb{A}^n \subset \mathbb{P}^n$ als Teilmenge des $\mathbb{P}^n$. Die kleinste projektive algebraische Menge, die X enthält, heißt der projektive Abschluss $\overline{X}$ von X. (In der Zariski-Topologie ist $\overline{X}$ der topologische Abschluss von X in $\mathbb{P}^n$.)*

Wie berechnet man den projektiven Abschluss?

Vorbemerkung: Um die rationalen Lösungen der Gleichung $f = 5x^2 + 19y^2 - 1 = 0$ zu bestimmen, kann man substituieren $x = \frac{X}{Z}, y = \frac{Y}{Z}$ und dann nach den ganzzahligen Lösungen der Gleichung $g = 5X^2 + 19Y^2 - Z^2 = 0$ suchen. ($(1, 2, 9)$ ist eine Lösung.) Dies entspricht dem Übergang vom Affinen zum Projektiven.

Homogenisierung von Polynomen: Sei $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \setminus \{0\}$ ein Polynom vom Grad d, d.h. man kann schreiben

$$f = \sum_{i_1+\cdots+i_n \leq d} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

wobei es ein Tupel $(j_1, \ldots, j_n)$ gibt mit

$$j_1 + \cdots + j_n = d \quad \text{und} \quad a_{j_1 \ldots j_n} \neq 0.$$

Beim Homogenisieren machen wir jedes Monom $x_1^{i_1} \ldots x_n^{i_n}$ durch eine neue Variable x_0 zu einem Monom vom Grad d:

$$x_1^{i_1} \ldots x_n^{i_n} \quad \longrightarrow \quad x_0^{d-i_1-\cdots-i_n} x_1^{i_1} \ldots x_n^{i_n}.$$

Das homogenisierte Polynom ist dann

$$\begin{aligned} f^* &= \sum_{i_1+\cdots+i_n \leq d} a_{i_1 \ldots i_n} x_0^{d-i_1-\cdots-i_n} x_1^{i_1} \ldots x_n^{i_n} = \\ &= \sum_{i_0+i_1+\cdots+i_n = d} a_{i_1 \ldots i_n} x_0^{i_0} x_1^{i_1} \ldots x_n^{i_n}. \end{aligned}$$

Insbesondere gilt dann $f^*(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Man kann die Homogenisierung auch etwas anders schreiben:

$$\begin{aligned} f^*(x_0, x_1, \ldots, x_n) &= \sum_{i_1+\cdots+i_n \leq d} a_{i_1 \ldots i_n} x_0^{d-i_1-\cdots-i_n} x_1^{i_1} \ldots x_n^{i_n} = \\ &= \sum_{i_1+\cdots+i_n \leq d} a_{i_1 \ldots i_n} x_0^d (\frac{x_1}{x_0})^{i_1} \ldots (\frac{x_n}{x_0})^{i_n} = \\ &= x_0^d \sum_{i_1+\cdots+i_n \leq d} a_{i_1 \ldots i_n} (\frac{x_1}{x_0})^{i_1} \ldots (\frac{x_n}{x_0})^{i_n} = \\ &= x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}). \end{aligned}$$

Beispiel: Das Polynom $f = x_1^3 + 5x_2x_3 - x_2^3 + 2$ hat Grad 3. Die Homogenisierung ist dann

$$f^* = x_1^3 + 5x_0x_2x_3 - x_2^3 + 2x_0^3.$$

Bemerkung: Bei der Homogenisierung von Polynomen $f(x, y)$ in zwei Variablen x, y werden wir meist x durch x_1 und y durch x_2 ersetzen. Dann erhält man

$$f^*(x_0, x_1, x_2) = x_0^d f(\frac{x_1}{x_0}, \frac{x_2}{x_0}).$$

Etwas ausführlicher: Aus

$$f = \sum_{j+k \leq d} a_{jk} x^j y^k$$

erhält man

$$f^* = \sum_{j+k \leq d} a_{jk} x_0^{d-j-k} x_1^j x_2^k = \sum_{i+j+k=d} a_{jk} x_0^i x_1^j x_2^k.$$

(Manchmal findet man auch die Homogenisierung mit einer neuen Variablen z.)

Beispiel: Aus $f = x^3 + ax + b - y^2$ erhält man

$$f^* = x_1^3 + ax_0^2x_1 + bx_0^3 - x_0x_2^2.$$

Bemerkung: Sei $X = \{f_1 = \cdots = f_r = 0\} \subseteq \mathbb{A}^n$ und f_i^* die Homogenisierung von f_i. Mit unserer Konvention gilt $\mathbb{A}^n \subseteq \mathbb{P}^n$ und damit

$$X \subseteq \{f_1^* = \cdots = f_r^* = 0\},$$

also

$$\overline{X} \subseteq \{f_1^* = \cdots = f_r^* = 0\}.$$

Leider muss im Allgemeinen hier keine Gleichheit gelten.

Beispiel: Es ist

$$\{(0,0)\} = \{x = 0, y - x^2 = 0\},$$

aber

$$\{x_1 = 0, x_0x_2 - x_1^2 = 0\} = \{(1:0:0), (0:1:0)\},$$

während der projektive Abschluss natürlich

$$\{x_1 = 0, x_2 = 0\} = \{(1:0:0)\}$$

ist.

Wenn aber die algebraische Menge nur durch ein Polynom definiert wird, ist die Sache einfacher. Wir geben den folgenden Satz ohne Beweis an.

SATZ. *Ist $X = \{f = 0\} \subseteq \mathbb{A}^n$ mit $f \in K[x_1, \ldots, x_n]$, und ist $f^* \in K[x_0, x_1, \ldots, x_n]$ die Homogenisierung von f, so ist der projektive Abschluss von X einfach*

$$\overline{X} = \{f^* = 0\}.$$

Wir werden projektive algebraische Mengen der Gestalt $\{g(x_0, x_1, \ldots, x_n) = 0\}$ oft einfach durch die affine Gleichung $g(1, x_1, \ldots, x_n) = 0$ angeben, weil dies einfacher aussieht. Die Punkte $X \cap H_0$ werden auch die unendlich fernen Punkte von X genannt.

Beispiel: Sei $X \subseteq \mathbb{P}^2$ gegeben durch $y = x^2$. Homogenisieren liefert $x_0x_2 = x_1^2$. Es gibt einen unendlich fernen Punkt, nämlich $(0:0:1)$. Betrachtet man X im affinen Teil $x_1 \neq 0$, so kann man setzen $(x_0 : x_1 : x_2) = (u : 1 : v)$ und man erhält die Gleichung $uv = 1$. Parabel und Hyperbel sind also nur verschiedene affine Ansichten der gleichen projektiven Kurve.

DEFINITION. *Eine projektive Transformation (oder ein projektiver Koordinatenwechsel) ist eine Abbildung $\phi : \mathbb{P}^n \to \mathbb{P}^n$, sodass eine Matrix $A \in \mathrm{GL}_{n+1}(\overline{K})$ existiert mit*

$$\phi(x_0 : \cdots : x_n) = (y_0 : \cdots : y_n) \iff A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix} \text{ für ein } \lambda \in \overline{K}^*.$$

ϕ ist offensichtlich bijektiv, ϕ^{-1} ist eine projektive Transformation, die durch die Matrix A^{-1} beschrieben wird.
Zwei Mengen $V, W \subseteq \mathbb{P}^n$ heißen projektiv äquivalent, wenn es eine projektive Transformation ϕ gibt mit $W = \phi(V)$. Die Mengen V, W heißen projektiv äquivalent über K, wenn die Matrix A in $\mathrm{GL}_{n+1}(K)$ gewählt werden kann.

LEMMA. *Seien $P, Q, R \in \mathbb{P}^2$ drei verschiedene Punkte der projektiven Ebene. Liegen P, Q, R nicht auf einer Geraden, so gibt es einen projektiven Koordinatenwechsel mit*

$$\phi(P) = (1:0:0), \quad \phi(Q) = (0:1:0), \quad \phi(R) = (0:0:1).$$

Sind $P, Q, R, S \in \mathbb{P}^2$ vier Punkte der projektiven Ebene, von denen keine drei auf einer Geraden liegen, so gibt es einen projektiven Koordinantenwechsel mit

$$\phi(P) = (1:0:0), \quad \phi(Q) = (0:1:0), \quad \phi(R) = (0:0:1), \quad \phi(S) = (1:1:1).$$

Beweis: Sei $P = (p_0 : p_1 : p_2)$, $Q = (q_0 : q_1 : q_2)$, $R = (r_0 : r_1 : r_2)$. Da P, Q, R nicht auf einer Geraden liegen, ist ψ mit

$$\psi \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} p_0 & q_0 & r_0 \\ p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

ein projektiver Koordinatenwechsel mit

$$\psi((1:0:0)) = P, \quad \psi((0:1:0)) = Q, \quad \psi((0:0:1)) = R.$$

Mit $\phi = \psi^{-1}$ folgt dann die erste Aussage.
Für die zweite Behauptung können wir nun o.E.

$$P = (1:0:0), \quad Q = (0:1:0), \quad R = (0:0:1), \quad S = (s_0 : s_1 : s_2)$$

annehmen. P und Q liegen auf der Geraden $x_2 = 0$, P und R auf der Geraden $x_1 = 0$, Q und R auf der Geraden $x_0 = 0$. Da S auf keiner der Geraden liegen soll, ist $s_0, s_1, s_2 \neq 0$. Dann ist

$$\rho \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} s_0 & 0 & 0 \\ 0 & s_1 & 0 \\ 0 & 0 & s_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

ein projektiver Koordinatenwechsel mit

$$\rho((1:0:0)) = (1:0:0), \quad \rho((0:1:0)) = (0:1:0),$$

$$\rho((0:0:1)) = (0:0:1), \quad \rho((1:1:1)) = S,$$

sodass ρ^{-1} ein geeigneter Koordinantenwechsel ist. ■

3. Ebene projektive Kurven

DEFINITION. *Eine ebene projektive Kurve C über K vom Grad $d \geq 1$ wird durch ein homogenes Polynom $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ vom Grad d gegeben. (Man sagt auch, dass C durch die Gleichung $f(x_0, x_1, x_2) = 0$ definiert wird.) Das zugehörige geometrische Objekt ist die Nullstellenmenge*

$$C(\overline{K}) = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : f(x_0, x_1, x_2) = 0\}.$$

Die Menge

$$C(K) = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(K) : f(x_0, x_1, x_2) = 0\}$$

heißt die Menge der K-rationalen Punkte von C. Etwas allgemeiner betrachtet man für einen Oberkörper L von K die Menge der L-rationalen Punkte von C:

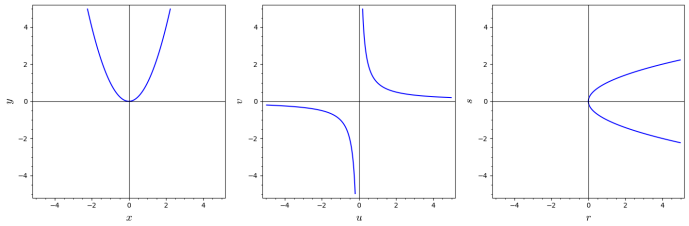
$$C(L) = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(L) : f(x_0, x_1, x_2) = 0\}.$$

Ist $c \in K^*$, so unterscheidet man nicht zwischen der durch $f(x_0, x_1, x_2) = 0$ und der durch $cf(x_0, x_1, x_2) = 0$ definierten Kurve.
Die Kurve C heißt irreduzibel über K, wenn $f(x_0, x_1, x_2)$ als Polynom über K irreduzibel ist, C heißt absolut irreduzibel, wenn $f(x_0, x_1, x_2)$ als Polynom über $\overline{K}$ irreduzibel ist.

Beispiele:

- Eine Gerade in $\mathbb{P}^2$, gegeben als $G = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$ können wir mit einer projektiven ebenen Kurve vom Grad 1, gegeben durch das Polynom $a_0x_0+a_1x_1+a_2x_2$, identifizieren.
- Ebene projektive Kurven vom Grad 2 nennt man Quadriken, Kurven vom Grad 3 heißen Kubiken.
- Wir betrachten die durch $f(x_0, x_1, x_2) = x_0x_2 - x_1^2$ definierte Quadrik Q. Wir haben bereits früher gesehen, wie die Quadrik Q in den affinen Teilen U_i aussieht:

$$\begin{aligned} Q(\overline{K}) \cap U_0 &= Q(\overline{K}) \cap \{(1 : x : y) : (x, y) \in \mathbb{A}^2\} = \{(1 : x : y) : y = x^2\}, \\ Q(\overline{K}) \cap U_1 &= Q(\overline{K}) \cap \{(u : 1 : v) : (u, v) \in \mathbb{A}^2\} = \{(u : 1 : v) : uv = 1\}, \\ Q(\overline{K}) \cap U_2 &= Q(\overline{K}) \cap \{(r : s : 1) : (r, s) \in \mathbb{A}^2\} = \{(r : s : 1) : r = s^2\}. \end{aligned}$$



Die projektive Quadrik sieht also in den affinen Teilen wie eine Parabel oder wie eine Hyperbel aus.

Sei die ebene projektive Kurve C gegeben durch das homogene Polynom $f(x_0, x_1, x_2)$. Mit der Identifikation $\mathbb{A}^2 \simeq U_0 = \{(1 : x : y)\} \subseteq \mathbb{P}^2$ erhalten wir

$$\begin{aligned} C(\overline{K}) \cap \mathbb{A}^2 &= \{(1 : x : y) \in \mathbb{P}^2 : f(1, x, y) = 0\} \simeq \\ &\simeq \{(x, y) \in \mathbb{A}^2 : f(1, x, y) = 0\} \quad \text{und} \\ C(\overline{K}) \cap H_0 &= \{(0 : z_1 : z_2) : f(0, z_1, z_2) = 0\}. \end{aligned}$$

Ist $f(1, x, y)$ ein nichtkonstantes Polynom, so entspricht der affine Teil von C also der affinen Kurve $f(1, x, y) = 0$. Ist $f(1, x, y)$ konstant, so ist $f = cx_0^d$ und mengenmäßig $C(\overline{K}) = H_0$.

DEFINITION. *Sei C eine affine ebene Kurve gegeben durch ein Polynom $f(x, y) \in K[x, y]$ vom Grad d. Ist dann*

$$f^*(x_0, x_1, x_2) = x_0^d f(\frac{x_1}{x_0}, \frac{x_2}{x_0})$$

die Homogenisierung von f, so heißt die durch $f^*(x_0, x_1, x_2)$ definierte projektive ebene Kurve der projektive Abschluss $\overline{C}$ von C.

Beispiel: Wir betrachten die Parabel C mit der Gleichung $f = y - x^2 = 0$ in $\mathbb{A}^2$. Die Homogenisierung von $f(x, y)$ ist $f^*(x_0, x_1, x_2) = x_0^2 f(\frac{x_1}{x_0}, \frac{x_2}{x_0}) = x_0 x_2 - x_1^2$. Der projektive Abschluss von C ist also $\overline{C}$, gegeben durch das homogene Polynom $f^* = x_0 x_2 - x_1^2$.

Überlegung: Sei eine ebene affine Kurve C gegeben durch das Polynom $f(x, y) \in K[x, y]$. Wir schreiben

$$f(x, y) = \sum_{\ell=0}^{d} f_\ell(x, y), \quad f_\ell(x, y) \text{ homogen vom Grad } \ell, \quad f_d(x, y) \neq 0.$$

Dann definiert die Homogenisierung

$$f^*(x_0, x_1, x_2) = \sum_{\ell=0}^{d} x_0^{d-\ell} f_\ell(x_1, x_2) = x_0^d f_0(x_1, x_2) + x_0^{d-1} f_1(x_1, x_2) + \cdots + x_0 f_{d-1}(x_1, x_2) + f_d(x_1, x_2)$$

den projektiven Abschluss $\overline{C}$ von C. Faktorisieren wir

$$f_d(x_1, x_2) = \prod_{i=1}^{d} (\lambda_i x_1 - \mu_i x_2),$$

so gilt

$$\begin{aligned} \overline{C}(\overline{K}) \cap \mathbb{A}^2 &= \{(x, y) \in \mathbb{A}^2 : f^*(1, x, y) = 0\} = \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\} = C(\overline{K}), \\ \overline{C}(\overline{K}) \cap H_0 &= \{(0 : z_1 : z_2) \in \mathbb{P}^2 : f^*(0, z_1, z_2) = 0\} = \{(0 : z_1 : z_2) \in \mathbb{P}^2 : f_d(z_1, z_2) = 0\} = \\ &= \{(0 : \mu_1 : \lambda_1), \ldots, (0 : \mu_d : \lambda_d)\}, \end{aligned}$$

wobei nicht alle Punkte $(0 : \mu_i : \lambda_i)$ notwendig verschieden sind. Wir nennen die Punkte von $\overline{C}(\overline{K}) \cap H_0$ auch die Punkte im Unendlichen der Kurve C.

Beispiel: Wir betrachten nochmals die affine Kurve C mit der Gleichung $y = x^2$, die also durch das Polynom $f(x, y) = y - x^2$ gegeben wird. Die Homogenisierung ist $f^*(x_0, x_1, x_2) = x_0 x_2 - x_1^2$. Der projektive Abschluss von C wird also durch $x_0 x_2 - x_1^2 = 0$ gegeben. Wegen

$$\overline{C}(\overline{K}) \cap H_0 = \{(0 : 0 : 1)\}$$

hat C nur einen Punkt im Unendlichen, nämlich $(0 : 0 : 1)$.

Lokale Betrachtung: Sei die projektve ebene Kurve C vom Grad d gegeben durch das Polynom $F(x_0, x_1, x_2)$. Wir schreiben

$$F(x_0, x_1, x_2) = \sum_{\ell=0}^{d} x_0^{d-\ell} f_\ell(x_1, x_2) \quad \text{und} \quad f(x, y) = F(1, x, y) = \sum_{\ell=0}^{d} f_\ell(x, y)$$

und erhalten

$$\begin{aligned}
\frac{\partial F}{\partial x_1}(1, x, y) &= \frac{\partial f}{\partial x}(x, y), \\
\frac{\partial F}{\partial x_2}(1, x, y) &= \frac{\partial f}{\partial y}(x, y), \\
\frac{\partial F}{\partial x_0}(1, x, y) &= dF(1, x, y) - x\frac{\partial F}{\partial x_1}(1, x, y) - y\frac{\partial F}{\partial x_2}(1, x, y) = df(x, y) - x\frac{\partial f}{\partial x}(x, y) - y\frac{\partial f}{\partial y}(x, y).
\end{aligned}$$

Sei weiter $P = (p_0 : p_1 : p_2) \in C(\overline{K})$ ein Punkt der projektiven Kurve.
Wir betrachten den Fall $p_0 \neq 0$, d.h. $P = (1 : \frac{p_1}{p_0} : \frac{p_2}{p_0})$. Wegen $F(P) = F(p_0, p_1, p_2) = p_0^d f(\frac{p_1}{p_0}, \frac{p_2}{p_0}) = 0$ gilt

$$\frac{\partial F}{\partial x_0}(P) = \frac{\partial F}{\partial x_1}(P) = \frac{\partial F}{\partial x_2}(P) = 0 \quad \Longleftrightarrow \quad \frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) = \frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) = 0$$

und

$$\begin{aligned}
& \frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0})(x - \frac{p_1}{p_0}) + \frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0})(y - \frac{p_2}{p_0}) = \\
= \; & x\frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) + y\frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) - \left(\frac{p_1}{p_0}\frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) + \frac{p_2}{p_0}\frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0})\right) = \\
= \; & x\frac{\partial F}{\partial x_1}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) + y\frac{\partial F}{\partial x_2}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) - \left(dF(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) - \frac{\partial F}{\partial x_0}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0})\right) = \\
= \; & \frac{\partial F}{\partial x_0}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) + x\frac{\partial F}{\partial x_1}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) + y\frac{\partial F}{\partial x_2}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) = \\
= \; & \frac{1}{p_0^{d-1}}\left(\frac{\partial F}{\partial x_0}(p_0, p_1, p_2) + x\frac{\partial F}{\partial x_1}(p_0, p_1, p_2) + y\frac{\partial F}{\partial x_2}(p_0, p_1, p_2)\right)
\end{aligned}$$

hat (bis auf eine Konstante) die Homogenisierung (vom Grad 1)

$$x_0\frac{\partial F}{\partial x_0}(p_0, p_1, p_2) + x_1\frac{\partial F}{\partial x_1}(p_0, p_1, p_2) + x_2\frac{\partial F}{\partial x_2}(p_0, p_1, p_2).$$

Daher gilt: P ist auf dem affinen Teil der Kurve genau dann singulär, wenn gilt

$$\frac{\partial F}{\partial x_0}(P) = \frac{\partial F}{\partial x_1}(P) = \frac{\partial F}{\partial x_2}(P) = 0.$$

Ist P ein glatter Punkt, so ist der projektive Abschluss der Tangente die Gerade

$$\frac{\partial F}{\partial x_0}(P)x_0 + \frac{\partial F}{\partial x_1}(P)x_1 + \frac{\partial F}{\partial x_2}(P)x_2 = 0.$$

Man definiert nun:

DEFINITION. *Ist die projektive ebene Kurve C gegeben durch das Polynom $f(x_0, x_1, x_2)$, so heißt $P \in C(\overline{K})$ ein singulärer Punkt, wenn gilt*

$$\frac{\partial f}{\partial x_0}(P) = \frac{\partial f}{\partial x_1}(P) = \frac{\partial f}{\partial x_2}(P) = 0.$$

Im andern Fall heißt P nichtsingulärer oder glatter Punkt, die Gerade

$$\frac{\partial f}{\partial x_0}(P)x_0 + \frac{\partial f}{\partial x_1}(P)x_1 + \frac{\partial f}{\partial x_2}(P)x_2 = 0$$

heißt die Tangente an C in P.

Mit der vorangegangenen lokalen Betrachtung sieht man, dass man Singularitäten in affinen Teilen untersuchen kann. Natürlich muss man sich überlegen, dass diese Begriffe mit Koordinatenwechsel verträglich sind.

Beispiel: Der projektive Abschluss der durch $y^2 = x^3 - 2x$ definierten Kurve ist $x_0x_2^2 = x_1^3 - 2x_0^2x_1$, wird also beschrieben durch das Polynom

$$f = -2x_0^2x_1 - x_0x_2^2 + x_1^3.$$

Der Punkt $(2,2) \simeq (1:2:2)$ liegt auf der Kurve. Mit

$$\frac{\partial f}{\partial x_0} = -4x_0x_1 - x_2^2, \quad \frac{\partial f}{\partial x_1} = -2x_0^2 + 3x_1^2, \quad \frac{\partial f}{\partial x_2} = -2x_0x_2$$

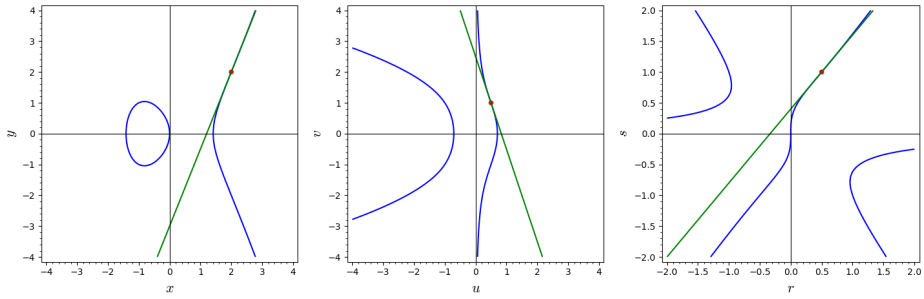
erhalten wir

$$\frac{\partial f}{\partial x_0}(1,2,2) = -12, \quad \frac{\partial f}{\partial x_1}(1,2,2) = 10, \quad \frac{\partial f}{\partial x_2}(1,2,2) = -4.$$

Man sieht, dass $(1:2:2)$ nichtsingulär ist und die Tangente

$$-12x_0 + 10x_1 - 4x_2 = 0, \quad \text{also} \quad 6x_0 - 5x_1 + 2x_2 = 0$$

besitzt. Die folgenden Bilder zeigen die Situation in den drei affinen Teilen U_0, U_1, U_2:



Schnitte von Kurven und Geraden: Wir wollen jetzt noch Schnitte von Kurven mit Geraden in $\mathbb{P}^2$ betrachten. Die Schnittvielfachkeit $(C \cdot G)_P$ in einem Punkt wird lokal definiert, indem man den Punkt in einem affinen Teil anschaut.

Wir geben eine algorithmische Darstellung der Berechnung der Schnittmultiplizität:

Die Kurve C sei durch das Polynom $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ definiert, die Gerade G sei durch eine Parametrisierung gegeben:

$$G = \{(p_0u + q_0v : p_1u + q_1v : p_2u + q_2v) : (u : v) \in \mathbb{P}^1\}.$$

(Die Punkte $(p_0 : p_1 : p_2)$ und $(q_0 : q_1 : q_2)$ liegen auf der Kurve.)

- Wir bilden das homogene Polynom

$$g(u, v) = f(p_0u + q_0v, p_1u + q_1v, p_2u + q_2v) \in K[u, v].$$

- Ist das Polynom $g(u, v) = 0$, so gilt $G(\overline{K}) \subseteq C(\overline{K})$ und das Polynom $f(x_0, x_1, x_2)$ spaltet über $\overline{K}$ einen Linearfaktor ab.
- Ist $g(u, v) \neq 0$, so erhält man über dem algebraischen Abschluss $\overline{K}$ eine Zerlegung

$$g(u, v) = cu^{n_0} \prod_{i=1}^{r} (v - \alpha_i u)^{n_i}$$

mit $c \in K^*$, paarweise verschiedenen $\alpha_i \in \overline{K}$, $n_0 \geq 0$, $r \geq 0$, $n_1 \geq 1, \ldots, n_r \geq 1$.

  - Ist $n_0 \geq 1$, so ist $Q = (q_0 : q_1 : q_2)$ ein Schnittpunkt mit Schnittmultiplizität $(C \cdot G)_Q = n_0$.
  - Für $i = 1, \ldots, r$ ist $P_i = (p_0 + \alpha_i q_0 : p_1 + \alpha_i q_1 : p_2 + \alpha_i q_2)$ ein Schnittpunkt mit Schnittmultiplizität $(C \cdot G)_{P_i} = n_i$.

Da das Polynom g Grad d hat, gilt $n_0 + n_1 + \cdots + n_r = d$, und damit

$$\sum_{P \in C(\overline{K}) \cap G(\overline{K})} (C \cdot G)_P = d.$$

Wir formulieren dieses wichtige Ergebnis nochmals als Satz:

SATZ. *Sei G eine Gerade, C eine Kurve vom Grad d in $\mathbb{P}^2$ mit $G(\overline{K}) \not\subseteq C(\overline{K})$. Dann gilt*

$$\sum_{P \in C(\overline{K}) \cap G(\overline{K})} (C \cdot G)_P = d,$$

d.h. C schneidet G in genau d Punkten, wenn man mit Multiplizitäten zählt.

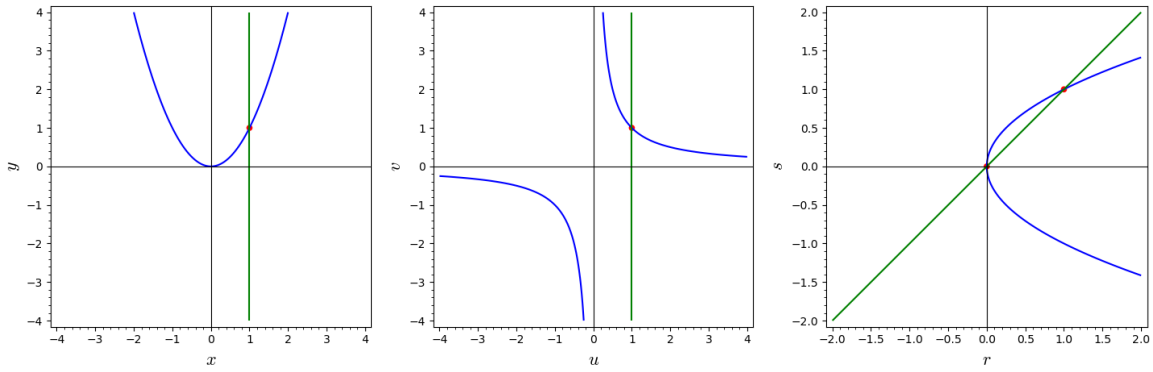
Beispiel: Wir betrachten die ebene Kurve C mit der affinen Gleichung $y = x^2$ bzw. der projektiven Gleichung $f = x_0x_2 - x_1^2 = 0$.
Wir wollen den Schnitt mit den Geraden G_c der Form $x = c$ bzw. $x_1 = cx_0$ bestimmen. Es ist

$$\begin{aligned} G_c &= \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_1 = cx_0\} = \{(x_0 : cx_0 : x_2) \in \mathbb{P}^2\} = \\ &= \{(u : cu : v) : (u : v) \in \mathbb{P}^1\}. \end{aligned}$$

Wir setzen die letzte Parametrisierung in f ein:

$$f(u, cu, v) = uv - c^2u^2 = u(v - c^2u).$$

Für $(u : v) = (0 : 1)$ erhält man den Schnittpunkt $(0 : 0 : 1)$ mit der Schnittmultiplizität 1, für $(u : v) = (1 : c^2)$ erhält man den Schnittpunkt $(1 : c : c^2)$, ebenfalls mit Schnittmultiplizität 1. Die Bilder zeigen die Situation in den drei affinen Teilen U_0, U_1, U_2:



Bemerkung: Ist C eine absolut irreduzible ebene projektive Kurve vom Grad $d \geq 2$, so schneidet jede Gerade die Kurve in genau d Punkten, wenn man mit Vielfachheiten zählt.

Beispiel: Sei Q eine absolut irreduzible projektive ebene Quadrik. Jede Tangente schneidet die Quadrik genau in einem Punkt, und zwar mit Vielfachheit 2. Insbesondere besitzt Q keine Wendepunkte.

Bemerkung: Der Satz ist ein Spezialfall des Satzes von Bézout, der besagt, dass sich ebene projektive Kurven C und D in genau $\text{grad}(C) \cdot \text{grad}(D)$ Punkten schneiden, wenn man mit Multiplizitäten zählt und wenn es nur endlich viele Schnittpunkte gibt.
Beispiel: Wir betrachten wieder den projektiven Abschluss der durch $y^2 = x^3 - 2x$ gegeben Kurve, der durch

$$f = -2x_0^2x_1 - x_0x_2^2 + x_1^3$$

beschrieben wird. Die Tangente im Punkt $P = (1 : 2 : 2)$ wird durch $6x_0 - 5x_1 + 2x_2$ beschrieben, lässt sich also durch die Gleichung

$$x_2 = -3x_0 + \frac{5}{2}x_1$$

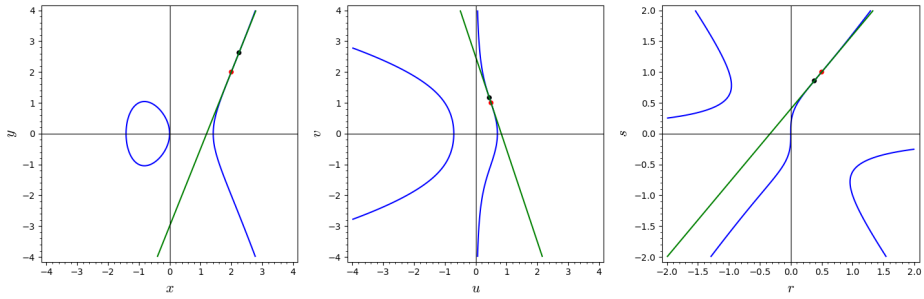
beschreiben. Um den Schnitt der Tangente mit der Kurve zu bestimmen, verwenden wir die letzte Darstellung (mit den Parametern x_0, x_1), wir setzen x_2 in f ein:

$$f(x_0, x_1, -3x_0 + \frac{5}{2}x_1) = -9x_0^3 + 13x_0^2x_1 - \frac{25}{4}x_0x_1^2 + x_1^3 = (x_1 - 2x_0)^2(x_1 - \frac{9}{4}x_0).$$

$(x_0 : x_1) = (1 : 2)$ liefert den Punkt $P = (1 : 2 : 2)$ mit Schnittmultiplizität 2, $(x_0 : x_1) = (1 : \frac{9}{4})$ liefert den neuen Punkt

$$Q = (1 : \frac{9}{4} : \frac{21}{8}) = (\frac{4}{9} : 1 : \frac{7}{6}) = (\frac{8}{21} : \frac{6}{7} : 1)$$

mit Schnittmultiplizität 1.



Die Tangente schneidet die Kurve in drei Punkten, wenn man mit Vielfachheiten zählt. Obwohl die Tangente ursprünglich wie eine Wendetangente aussah, ist es doch keine.

DEFINITION. *Ein nichtsingulärer Punkt P einer projektiven ebenen Kurve C heißt* **Wendepunkt**, *falls die Tangente T in P die Kurve mit Multiplizität ≥ 3 in P schneidet, d.h. $(C \cdot T)_P \geq 3$. Die Tangente wird dann auch eine* **Wendetangente** *von C genannt.*

Dass ein Punkt ein Wendepunkt ist, ist eine lokale Eigenschaft, d.h. kann in den affinen Teilen untersucht werden. Für die globale Beschreibung von Wendepunkten ist folgende Definition wichtig:

DEFINITION. *Sei C eine projektive ebene Kurve vom Grad $d \geq 3$, gegeben durch ein homogenes Polynom $f(x_0, x_1, x_2)$ vom Grad d. Dann heißt das Polynom*

$$H_f = \det\left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right) = \det\begin{pmatrix} \frac{\partial^2 f}{\partial x_0^2} & \frac{\partial^2 f}{\partial x_0 \partial x_1} & \frac{\partial^2 f}{\partial x_0 \partial x_2} \\ \frac{\partial^2 f}{\partial x_1 \partial x_0} & \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} \\ \frac{\partial^2 f}{\partial x_2 \partial x_0} & \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial x_2^2} \end{pmatrix}$$

die **Hessesche** *von f. H_f ist homogen vom Grad $3(d-2)$. Ist $H_f \neq 0$, so heißt die durch $H_f = 0$ definierte Kurve die* **Hessesche Kurve** *(oder einfach die* **Hessesche***) H_C zu C.*

Bemerkungen:

- Hat der Grundkörper K die Charakteristik p, ist d der Grad des homogenen Polynoms $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ und gilt in K die Gleichheit $d = 1$, d.h. $p \mid d-1$, so ist $H(f) = 0$ (als Polynom).
- Im Fall der Charakteristik 0 hat Hesse 1851 Folgendes behauptet, das 1876 von Gordan und Noether bewiesen wurde: H_f ist genau dann 0, wenn $f = 0$ aus lauter Geraden besteht, die durch einen Punkt gehen.

Beispiele:

- Für $f = x_0^d + x_1^d + x_2^d$ (mit $d \geq 3$) ergibt sich aus
$$\frac{\partial f}{\partial x_0} = dx_0^{d-1}, \quad \frac{\partial f}{\partial x_1} = dx_1^{d-1}, \quad \frac{\partial f}{\partial x_2} = dx_2^{d-1}$$
für die Hessesche zu f
$$H_f = \begin{vmatrix} d(d-1)x_0^{d-2} & 0 & 0 \\ 0 & d(d-1)x_1^{d-2} & 0 \\ 0 & 0 & d(d-1)x_2^{d-2} \end{vmatrix} = d^3(d-1)^3 x_0^{d-2} x_1^{d-2} x_2^{d-2}.$$
- Für $f = x_0 x_1 x_2$ ist
$$\frac{\partial f}{\partial x_0} = x_1 x_2, \quad \frac{\partial f}{\partial x_1} = x_0 x_2, \quad \frac{\partial f}{\partial x_2} = x_0 x_1,$$
und damit
$$H_f = \begin{vmatrix} 0 & x_2 & x_1 \\ x_2 & 0 & x_0 \\ x_1 & x_0 & 0 \end{vmatrix} = 2x_0 x_1 x_2.$$

- Für $f = x_1x_2(x_1 + x_2)$ ist $\frac{\partial f}{\partial x_0} = 0$, was sofort $H_f = 0$ liefert. ($f = 0$ besteht aus drei Geraden, die alle durch den Punkt $(1 : 0 : 0)$ gehen.)

LEMMA. *Geht eine projektive ebene Kurve C bei einem Koordinatenwechsel in die Kurve C' über, so die Hessesche H_C von C in die Hessesche $H_{C'}$ von C'.*

Beweis: Die Kurve C werde definiert durch das homogene Polynom $f(x_0, x_1, x_2)$. Bei einem Koordinatenwechsel werden durch

$$x_0 = a_{00}y_0 + a_{01}y_1 + a_{02}y_2, \quad x_1 = a_{10}y_0 + a_{11}y_1 + a_{12}y_2, \quad x_2 = a_{20}y_0 + a_{21}y_1 + a_{22}y_2$$

neue Variable y_0, y_1, y_2 eingeführt. Definiert man

$$g(y_0, y_1, y_2) = f(a_{00}y_0 + a_{01}y_1 + a_{02}y_2, a_{10}y_0 + a_{11}y_1 + a_{12}y_2, a_{20}y_0 + a_{21}y_1 + a_{22}y_2),$$

so wird C' gegeben durch das Polynom g. Nun ist

$$\frac{\partial g}{\partial y_j} = \frac{\partial f}{\partial x_0}(\dots)a_{0j} + \frac{\partial f}{\partial x_1}(\dots)a_{1j} + \frac{\partial f}{\partial x_2}(\dots)a_{2j}$$

und

$$\begin{aligned}
\frac{\partial}{\partial y_i}\left(\frac{\partial g}{\partial y_j}\right) &= \left(\frac{\partial^2 f}{\partial x_0^2}(\dots)a_{0i} + \frac{\partial^2 f}{\partial x_1\partial x_0}(\dots)a_{1i} + \frac{\partial^2 f}{\partial x_2\partial x_0}(\dots)a_{2i}\right)a_{0j} + \dots = \\
&= \left(\sum_{k=0}^{2}\frac{\partial^2 f}{\partial x_k\partial x_0}(\dots)a_{ki}\right)a_{0j} + \dots = \\
&= \sum_{l=0}^{2}\left(\sum_{k=0}^{2}\frac{\partial^2 f}{\partial x_k\partial x_l}(\dots)a_{ki}\right)a_{lj} \overset{b_{ik}=a_{ki}}{=} \sum_{0\le k,l\le 2} b_{ik}\frac{\partial^2 f}{\partial x_k\partial x_l}(\dots)a_{lj},
\end{aligned}$$

sodass für die Matrizen $(M_f = (\frac{\partial^2 f}{\partial x_i\partial x_j}))$ folgt

$$\left(\frac{\partial^2 g}{\partial y_i\partial y_j}\right)(y_0, y_1, y_2) = (b_{ik})_{i,k} \cdot \left(\frac{\partial^2 f}{\partial x_k\partial x_l}(a_{00}y_0 + a_{01}y_1 + \dots)\right)_{k,l} \cdot (a_{lj})_{l,j}$$

also

$$M_g(y_0, y_1, y_2) = A^t \cdot M_f(a_{00}y_0 + a_{01}y_1 + \dots) \cdot A.$$

Determinantenbildung liefert

$$H_g(y_0, y_1, y_2) = (\det A)^2 \cdot H_f(a_{00}y_0 + a_{01}y_1 + \dots),$$

was die Behauptung beweist. ■

Für die Wendepunkte erhalten wir folgenden Satz:

SATZ. *(Die Charakteristik von K sei 0.) Sei C eine projektive ebene Kurve vom Grad $d \ge 3$, die nicht nur aus Geraden besteht, die alle durch einen Punkt gehen. Dann gilt:*

$$P \in C(\overline{K}) \cap H_C(\overline{K}) \quad \Longleftrightarrow \quad P \text{ singulär oder Wendepunkt.}$$

Die singulären Punkte und die Wendepunkte von C sind also genau die Punkte, in denen sich die Kurve C und die Hessesche H_C schneiden.

Beweis: Die Kurve C werde durch das Polynom $f(x_0, x_1, x_2)$ beschrieben. Sei $P \in C(\overline{K})$. Das vorangegangene Lemma erlaubt uns, einen Koordinatenwechsel zu machen, sodass $P = (1 : 0 : 0)$ gilt. Dann ist $f(1, 0, 0) = 0$. Wir wollen $H_f(1, 0, 0)$ bestimmen und berechnen dazu zunächst die Hesse-Matrix

$$\begin{pmatrix}
\frac{\partial^2 f}{\partial x_0^2} & \frac{\partial^2 f}{\partial x_0\partial x_1} & \frac{\partial^2 f}{\partial x_0\partial x_2} \\
\frac{\partial^2 f}{\partial x_1\partial x_0} & \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1\partial x_2} \\
\frac{\partial^2 f}{\partial x_2\partial x_0} & \frac{\partial^2 f}{\partial x_2\partial x_1} & \frac{\partial^2 f}{\partial x_2^2}
\end{pmatrix}$$

in $(1, 0, 0)$. Wir schreiben f in der Form

$$f(x_0, x_1, x_2) = \sum_{\ell=1}^{d} x_0^{d-\ell} f_\ell(x_1, x_2) = x_0^{d-1}f_1(x_1, x_2) + \dots + x_0 f_{d-1}(x_1, x_2) + f_d(x_1, x_2),$$

wobei die Polynome $f_\ell(x_1, x_2)$ homogen vom Grad ℓ sind.
Wir bilden die Ableitungen:

$$\begin{aligned}
\frac{\partial f}{\partial x_0} &= \sum_{\ell=1}^{d-1}(d-\ell)x_0^{d-\ell-1}f_\ell(x_1,x_2) = (d-1)x_0^{d-2}f_1(x_1,x_2) + \cdots + f_{d-1}(x_1,x_2),\\
\frac{\partial f}{\partial x_1} &= \sum_{\ell=1}^{d} x_0^{d-\ell}\frac{\partial f_\ell}{\partial x_1}(x_1,x_2) = x_0^{d-1}\frac{\partial f_1}{\partial x_1} + x_0^{d-2}\frac{\partial f_2}{\partial x_1}(x_1,x_2) + x_0^{d-3}\frac{\partial f_3}{\partial x_1}(x_1,x_2) + \ldots\\
\frac{\partial f}{\partial x_2} &= \sum_{\ell=1}^{d} x_0^{d-\ell}\frac{\partial f_\ell}{\partial x_2}(x_1,x_2) = x_0^{d-1}\frac{\partial f_1}{\partial x_2} + x_0^{d-2}\frac{\partial f_2}{\partial x_2}(x_1,x_2) + x_0^{d-3}\frac{\partial f_3}{\partial x_2}(x_1,x_2) + \ldots
\end{aligned}$$

Für die zweiten Ableitungen erhalten wir

$$\begin{aligned}
\frac{\partial^2 f}{\partial x_0^2} &= \sum_{\ell=1}^{d-2}(d-\ell)(d-\ell-1)x_0^{d-\ell-2}f_\ell(x_1,x_2) = (d-1)(d-2)x_0^{d-3}f_1(x_1,x_2) + \ldots,\\
\frac{\partial^2 f}{\partial x_0^2}(1,0,0) &= 0,\\
\frac{\partial^2 f}{\partial x_0\partial x_1} &= \sum_{\ell=1}^{d-1}(d-\ell)x_0^{d-\ell-1}\frac{\partial f_\ell}{\partial x_1}(x_1,x_2) = (d-1)x_0^{d-2}\frac{\partial f_1}{\partial x_1} + (d-2)x_0^{d-3}\frac{\partial f_2}{\partial x_1}(x_1,x_2) + \ldots,\\
\frac{\partial^2 f}{\partial x_0\partial x_1}(1,0,0) &= (d-1)\frac{\partial f_1}{\partial x_1},\\
\frac{\partial^2 f}{\partial x_0\partial x_2} &= \sum_{\ell=1}^{d-1}(d-\ell)x_0^{d-\ell-1}\frac{\partial f_\ell}{\partial x_2}(x_1,x_2) = (d-1)x_0^{d-2}\frac{\partial f_1}{\partial x_2} + (d-2)x_0^{d-3}\frac{\partial f_2}{\partial x_2}(x_1,x_2) + \ldots,\\
\frac{\partial^2 f}{\partial x_0\partial x_2}(1,0,0) &= (d-1)\frac{\partial f_1}{\partial x_2},\\
\frac{\partial^2 f}{\partial x_1^2} &= \sum_{\ell=2}^{d} x_0^{d-\ell}\frac{\partial^2 f_\ell}{\partial x_1^2}(x_1,x_2) = x_0^{d-2}\frac{\partial^2 f_2}{\partial x_1^2} + x_0^{d-3}\frac{\partial^2 f_3}{\partial x_1^2}(x_1,x_2) + \ldots,\\
\frac{\partial^2 f}{\partial x_1^2}(1,0,0) &= \frac{\partial^2 f_2}{\partial x_1^2},\\
\frac{\partial^2 f}{\partial x_1\partial x_2} &= \sum_{\ell=2}^{d} x_0^{d-\ell}\frac{\partial^2 f_\ell}{\partial x_1\partial x_2}(x_1,x_2) = x_0^{d-2}\frac{\partial^2 f_2}{\partial x_1\partial x_2} + x_0^{d-3}\frac{\partial^2 f_3}{\partial x_1\partial x_2}(x_1,x_2) + \ldots,\\
\frac{\partial^2 f}{\partial x_1\partial x_2}(1,0,0) &= \frac{\partial^2 f_2}{\partial x_1\partial x_2},\\
\frac{\partial^2 f}{\partial x_2^2} &= \sum_{\ell=2}^{d} x_0^{d-\ell}\frac{\partial^2 f_\ell}{\partial x_2^2}(x_1,x_2) = x_0^{d-2}\frac{\partial^2 f_2}{\partial x_2^2} + x_0^{d-3}\frac{\partial^2 f_3}{\partial x_2^2}(x_1,x_2) + \ldots,\\
\frac{\partial^2 f}{\partial x_2^2}(1,0,0) &= \frac{\partial^2 f_2}{\partial x_2^2}.
\end{aligned}$$

Wir erhalten die Matrix

$$\begin{pmatrix}
0 & (d-1)\frac{\partial f_1}{\partial x_1} & (d-1)\frac{\partial f_1}{\partial x_2}\\
(d-1)\frac{\partial f_1}{\partial x_1} & \frac{\partial^2 f_2}{\partial x_1^2} & \frac{\partial^2 f_2}{\partial x_1\partial x_2}\\
(d-1)\frac{\partial f_1}{\partial x_2} & \frac{\partial^2 f_2}{\partial x_1\partial x_2} & \frac{\partial^2 f_2}{\partial x_2^2}
\end{pmatrix}.$$

Wir führen nochmals einen Koordinatenwechsel durch, sodass wir

$$f_1(x_1, x_2) = Ax_1$$

annehmen können. (Im Fall eines singulären Punkts ist $A = 0$.) Außerdem sei

$$f_2(x_1, x_2) = Bx_1^2 + Cx_1x_2 + Dx_2^2.$$

Dann ist

$$\frac{\partial f_1}{\partial x_1} = A, \quad \frac{\partial f_1}{\partial x_2} = 0.$$

Weiter gilt

$$\frac{\partial f_2}{\partial x_1} = 2Bx_1 + Cx_2, \quad \frac{\partial f_2}{\partial x_2} = Cx_1 + 2Dx_2,$$

und damit

$$\frac{\partial^2 f_2}{\partial x_1^2} = 2B, \quad \frac{\partial^2 f_2}{\partial x_1 \partial x_2} = C, \quad \frac{\partial^2 f_2}{\partial x_2^2} = 2D.$$

Unsere Matrix wird zu

$$\begin{pmatrix} 0 & (d-1)A & 0 \\ (d-1)A & 2B & C \\ 0 & C & 2D \end{pmatrix}$$

und hat die Determinante

$$H_f(1,0,0) = -2(d-1)^2 A^2 D.$$

Nochmals:

$$H_f(1,0,0) = -2(d-1)^2 A^2 D.$$

Es gilt also in Charakteristik 0

$$H_f(1,0,0) = 0 \quad \Longleftrightarrow \quad A = 0 \text{ oder } D = 0.$$

- **Fall** $A = 0$**:** In diesem Fall ist die Kurve singulär im Punkt $(1:0:0)$.
- **Fall** $A \neq 0$**:** Die Kurve ist nichtsingulär in $(1:0:0)$.
  Wie schaut die Taylorentwicklung affin aus?

  $$f(1,x,y) = Ax + Bx^2 + Cxy + Dy^2 + \dots$$

  Wir können o.E. $A = 1$ annehmen:

  $$f(1,x,y) = x + Bx^2 + Cxy + Dy^2 + \dots$$

  Die Tangente T wird durch $x = 0$ beschrieben:

  $$T = \{(x,y) : x = 0\} = \{(0,t) : t \in \overline{K}\}.$$

  Um die Schnittvielfachheit zu bestimmen, setzen wir die Parametrisierung $x = 0$, $y = t$ in die $f(1,x,y)$ ein:

  $$f(1,0,t) = Dt^2 + \dots = t^2(D + \dots).$$

  - **Fall** $D \neq 0$**:** Dann ist die Schnittmultiplizität 2, die Tangente ist keine Wendetangente. Es gilt $H_f(1,0,0) \neq 0$.
  - **Fall** $D = 0$**:** Dann ist die Schnittmultiplizität ≥ 3, die Tangente ist eine Wendetangente, $(1:0:0)$ ein Wendepunkt und $H_f(1,0,0) = 0$.

Damit ist der Satz bewiesen. ■

Beispiel: Sei C der projektive Abschluss der durch $y^2 = x^3 - 2x$ definierten affinen Kurve. C wird durch das Polynom

$$f = -2x_0^2 x_1 - x_0 x_2^2 + x_1^3$$

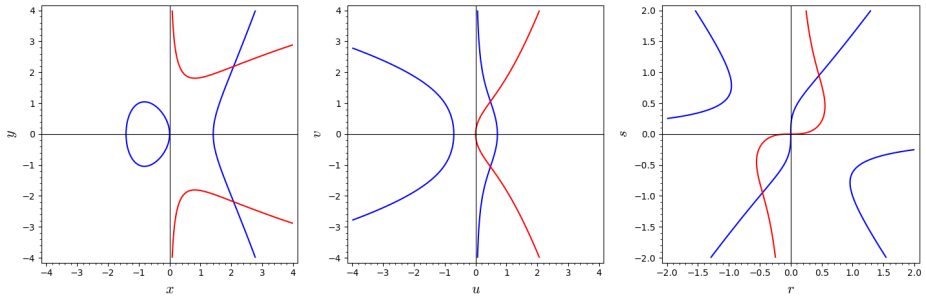
beschrieben. Es ist

$$\frac{\partial f}{\partial x_0} = -4x_0x_1 - x_2^2, \quad \frac{\partial f}{\partial x_1} = -2x_0^2 + 3x_1^2, \quad \frac{\partial f}{\partial x_2} = -2x_0x_2.$$

Daher wird die zugehörige Hessesche Kurve definiert durch das Polynom

$$H = \begin{vmatrix} -4x_1 & -4x_0 & -2x_2 \\ -4x_0 & 6x_1 & 0 \\ -2x_2 & 0 & -2x_0 \end{vmatrix} = 32x_0^3 + 48x_0x_1^2 - 24x_1x_2^2.$$

Man sieht, dass $(0:0:1)$ auf der Kurve und der Hesseschen Kurve liegt. Daher ist $(0:0:1)$ ein Wendepunkt. ($\frac{\partial f}{\partial x_0}(0,0,1) = -1 \neq 0$, weswegen $(0:0:1)$ keine Singularität ist.) In den Bildern ist die Kurve blau, die Hessesche Kurve rot gezeichnet.



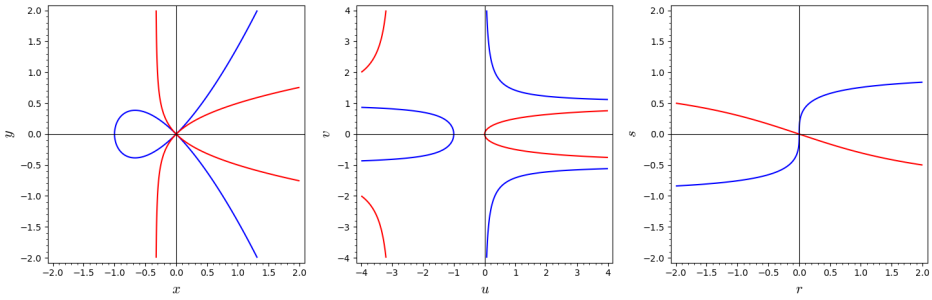
Beispiel: Der projektive Abschluss der Kurve $y^2 = x^2 + x^3$ wird beschrieben durch das Polynom

$$f = x_0x_1^2 - x_0x_2^2 + x_1^3.$$

Die Kurve hat in $(1:0:0)$ eine Singularität. (Dies ist die einzige Singularität der Kurve.) Die Hessesche wird beschrieben durch

$$H = 8x_0x_1^2 - 8x_0x_2^2 - 24x_1x_2^2.$$

Die Hessesche geht also durch die Singularität $(1:0:0)$ der Kurve.
Außerdem sieht man, dass $(0:0:1)$ ein Wendepunkt ist, da der Punkt im Durchschnitt von Kurve und Hessescher liegt.



Wir wollen nun den Durchschnitt von Kurve und Hessescher, also $f = H = 0$ bestimmen.
Wir wollen den Durchschnitt der durch

$$f = x_0x_1^2 - x_0x_2^2 + x_1^3 \quad \text{und} \quad H = 8x_0x_1^2 - 8x_0x_2^2 - 24x_1x_2^2$$

definierten Kurven bestimmen.

- **Punkte im Unendlichen:** Es ist

  $$f(0,x_1,x_2) = x_1^3 \quad \text{und} \quad H(0,x_1,x_2) = -24x_1x_2^2.$$

  Man sieht sofort, dass $(0:0:1)$ der einzige Punkt im Durchschnitt ist.
- **Punkte im Endlichen:** Wir verwenden affine Koordinaten x, y, betrachten also

  $$f(1,x,y) = x^3 + x^2 - y^2 \quad \text{und} \quad H(1,x,y) = -24xy^2 + 8x^2 - 8y^2.$$

  Resultantenbildung liefert

  $$R_x(f(1,x,y), H(1,x,y))(y) = -13824y^6(y^2 + \frac{16}{27})$$

  und

  $$R_y(f(1,x,y), H(1,x,y))(x) = 576x^6(x + \frac{4}{3})^2.$$

  Die Punkte im Durchschnitt müssen also x-Koordinate 0 oder $-\frac{4}{3}$ haben. Wir setzen dies in f und H ein:

  $$f(1,0,y) = -y^2, \quad H(1,0,y) = -8y^2.$$

Dies liefert den Schnittpunkt $(x, y) = (0, 0)$ bzw. $(1 : 0 : 0)$, der eine Singularität von $f = 0$ ist. Nun setzen wir $x = -\frac{4}{3}$ ein:

$$f(1, -\frac{4}{3}, y) = -(y^2 + \frac{16}{27}) \quad \text{und} \quad H(1, -\frac{4}{3}, y) = 24(y^2 + \frac{16}{27}).$$

Wir erhalten also die beiden Schnittpunkte

$$(-\frac{4}{3}, \pm\sqrt{-\frac{16}{27}}).$$

Diese Punkte sind über $\mathbb{C}$ definierte Wendepunkte der Kurve, die reell nicht sichtbar sind.

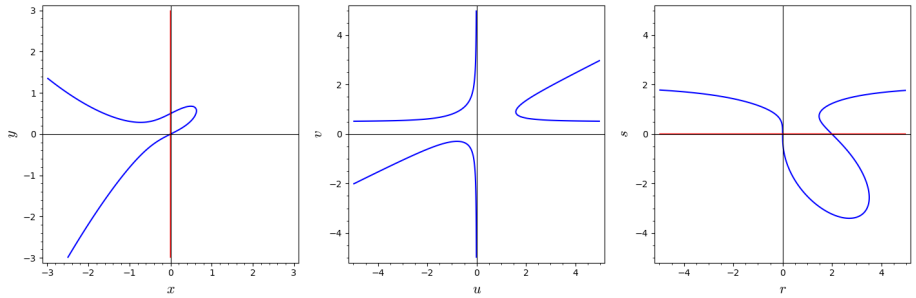
Beispiel: Wir betrachten die ebene projektive Kurve, die durch das Polynom

$$f = x_1^3 + x_0x_1^2 - 4x_0x_1x_2 + 4x_0x_2^2 + x_0^2x_1 - 2x_0^2x_2$$

definiert wird. Die zugehörige Hessesche ist

$$\begin{aligned} H_f &= -96x_0^2x_1 - 96x_0x_1^2 + 192x_0x_1x_2 - 96x_1^3 + 384x_1^2x_2 - 384x_1x_2^2 = \\ &= -96 \cdot x_1 \cdot \left(x_0^2 + x_0x_1 - 2x_0x_2 + x_1^2 - 4x_1x_2 + 4x_2^2\right). \end{aligned}$$

Die Gerade $x_1 = 0$ schneidet die Kurve wegen $f(x_0, 0, x_2) = 4x_0x_2^2 - 2x_0^2x_2 = 2x_0x_2(2x_2 - x_0)$ in den Punkten $(1 : 0 : 0)$, $(1 : 0 : \frac{1}{2})$, $(0 : 0 : 1)$.



Warum scheint bei der Hesseschen nur die Gerade $x_1 = 0$ sichtbar zu sein?
Sei

$$g = x_0^2 + x_0x_1 - 2x_0x_2 + x_1^2 - 4x_1x_2 + 4x_2^2.$$

Man findet, dass $g = 0$ genau eine Singularität hat, und zwar in $(0 : 2 : 1)$. Im affinen Teil U_2 mit den affinen Koordinaten r, s hat die Singularität also die Koordinaten $(r, s) = (0, 2)$. Führt man affine Koordinaten r, t ein durch $(x_0, x_1, x_2) = (r, 2 + t, 1)$, so erhält man

$$g(r, 2 + t, 1) = r^2 + rt + t^2.$$

Zwar ist dieses Polynom über $\mathbb{R}$ irreduzibel, über $\mathbb{C}$ zerfällt es aber:

$$g(r, 2 + t, 1) = (r - \frac{-1 + \sqrt{-3}}{2}t)(r - \frac{-1 - \sqrt{-3}}{2}t).$$

Der einzige $\mathbb{R}$-rationale Punkt von $g = 0$ ist also $(0 : 2 : 1)$.
Wir betrachten noch Beispiele von Hesseschen Polynomen zu gegebenen homogenen Polynomen $f(x_0, x_1, x_2)$. Für ein allgemeines quadratisches Polynom

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

ist

$$H_f = 8a_0a_3a_5 - 2a_0a_4^2 - 2a_1^2a_5 + 2a_1a_2a_4 - 2a_2^2a_3$$

einfach eine Zahl. Für ein allgemeines kubisches Polynom

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_3x_0x_1^2 + a_6x_1^3 + a_2x_0^2x_2 + a_4x_0x_1x_2 + a_7x_1^2x_2 + a_5x_0x_2^2 + a_8x_1x_2^2 + a_9x_2^3$$

ist

$$\begin{aligned}
H_f \quad = \quad & \left(24a_0a_3a_5 - 6a_0a_4^2 - 8a_1^2a_5 + 8a_1a_2a_4 - 8a_2^2a_3\right)x_0^3 + \\
& + \left(24a_0a_3a_8 - 24a_0a_4a_7 + 72a_0a_5a_6 - 8a_1^2a_8 + 16a_1a_2a_7 - 8a_1a_3a_5 + 2a_1a_4^2 - 24a_2^2a_6\right)x_0^2x_1 + \\
& + \left(72a_0a_6a_8 - 24a_0a_7^2 - 8a_1a_3a_8 + 24a_1a_5a_6 + 16a_2a_3a_7 - 24a_2a_4a_6 - 8a_3^2a_5 + 2a_3a_4^2\right)x_0x_1^2 + \\
& + \left(24a_1a_6a_8 - 8a_1a_7^2 - 8a_3^2a_8 + 8a_3a_4a_7 - 6a_4^2a_6\right)x_1^3 + \\
& + \left(72a_0a_3a_9 - 24a_0a_4a_8 + 24a_0a_5a_7 - 24a_1^2a_9 + 16a_1a_2a_8 - 8a_2^2a_7 - 8a_2a_3a_5 + 2a_2a_4^2\right)x_0^2x_2 + \\
& + \left(216a_0a_6a_9 - 24a_0a_7a_8 - 24a_1a_3a_9 - 8a_1a_4a_8 + 24a_1a_5a_7 + 24a_2a_3a_8 - 8a_2a_4a_7 - 24a_2a_5a_6 - 8a_3a_4a_5 + 2a_4^3\right)x_0x_1x_2 + \\
& + \left(72a_1a_6a_9 - 8a_1a_7a_8 + 24a_2a_6a_8 - 8a_2a_7^2 - 24a_3^2a_9 + 16a_3a_5a_7 + 2a_4^2a_7 - 24a_4a_5a_6\right)x_1^2x_2 + \\
& + \left(72a_0a_7a_9 - 24a_0a_8^2 - 24a_1a_4a_9 + 16a_1a_5a_8 + 24a_2a_3a_9 - 8a_2a_5a_7 - 8a_3a_5^2 + 2a_4^2a_5\right)x_0x_2^2 + \\
& + \left(24a_1a_7a_9 - 8a_1a_8^2 + 72a_2a_6a_9 - 8a_2a_7a_8 - 24a_3a_4a_9 + 16a_3a_5a_8 + 2a_4^2a_8 - 24a_5^2a_6\right)x_1x_2^2 + \\
& + \left(24a_2a_7a_9 - 8a_2a_8^2 - 6a_4^2a_9 + 8a_4a_5a_8 - 8a_5^2a_7\right)x_2^3
\end{aligned}$$

wieder ein kubisches Polynom.

KAPITEL 4

Ebene projektive Quadriken

Wir betrachten im Folgenden über einem Körper K definierte projektive ebene Kurven C vom Grad 2. Sie werden definiert durch homogene Polynome

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0, x_1, x_2] \setminus \{0\}.$$

Diese Kurven werden (projektive) **ebene Quadriken** oder **Kegelschnitte** genannt. Da die Gleichung der Kurve nur bis auf eine Konstante eindeutig bestimmt ist, erhalten wir eine Bijektion

$$\mathbb{P}^5 \to \{\text{Ebene Quadriken}\}, \quad (a_0 : a_1 : a_2 : a_3 : a_4 : a_5) \mapsto \{f = 0\}.$$

Wir sagen, die ebenen Quadriken bilden einen $\mathbb{P}^5$.

1. Reduzibilität und Singularität

Wir beginnen mit einem Lemma zur Zerlegung homogener Polynome.

LEMMA. *Seien $f, g \in K[x_0, x_1, \ldots, x_n] \setminus \{0\}$. Dann gilt:*

$$fg \text{ homogen} \quad \Longleftrightarrow \quad f \text{ und } g \text{ homogen.}$$

(Ein Produkt von Polynomen ist genau dann homogen, wenn jeder der Faktoren homogen ist.)

Beweis:

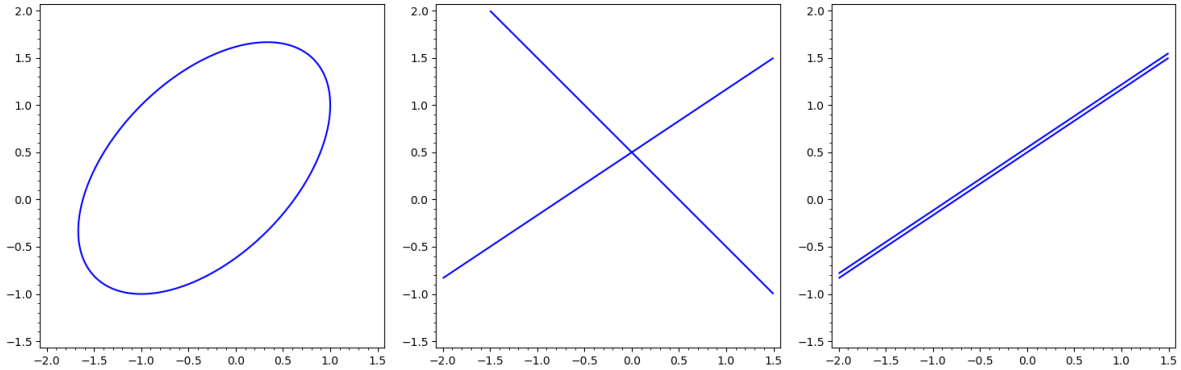
- $\Longleftarrow$ Ist f homogen vom Grad d, g homogen vom Grad e, so können wir schreiben
$$f = \sum_{i_0+\cdots+i_n=d} a_{i_0,\ldots,i_n} x_0^{i_0} \ldots x_n^{i_n} \quad \text{und} \quad g = \sum_{j_0+\cdots+j_n=e} b_{j_0,\ldots,j_n} x_0^{j_0} \ldots x_n^{j_n},$$
woraus
$$fg = \sum_{\substack{i_0+\cdots+i_n=d \\ j_0+\cdots+j_n=e}} a_{i_0,\ldots,i_n} b_{j_0,\ldots,j_n} x_0^{i_0+j_1} \ldots x_n^{i_n+j_n}$$
folgt. Alle in dieser Darstellung von fg auftretenden Monome haben Grad $d+e$, weswegen fg homogen vom Grad $d+e$ ist.
- $\Longrightarrow$ Wir zerlegen f und g in homogene Bestandteile:
$$f = \sum_{k_0 \le k \le k_1} f_k, \quad g = \sum_{l_0 \le l \le l_1} g_l,$$
wobei f_k homogen vom Grad k, g_l homogen vom Grad l sein und außerdem $f_{k_0} \neq 0$, $f_{k_1} \neq 0$, $g_{l_0} \neq 0$, $g_{l_1} \neq 0$ gelten soll. Nach dem ersten Teil ist f_kg_l homogen vom Grad $k+l$. Dann ist
$$fg = \sum_{m \ge 0} \left(\sum_{k+l=m} f_k g_l \right) = \sum_{k_0+l_0 \le m \le k_1+l_1} \left(\sum_{k+l=m} f_k g_l \right).$$
Der homogene Anteil von fg vom Grad k_0+l_0 ist $f_{k_0}g_{l_0} \neq 0$, der vom Grad k_1+l_1 ist $f_{k_1}g_{l_1} \neq 0$. Da aber fg homogen sein soll, müssen diese Anteile übereinstimmen, d.h. es muss gelten $k_0+l_0 = k_1+l_1$, woraus wegen $k_0 \le k_1$ und $l_0 \le l_1$ sofort $k_0 = k_1$ und $l_0 = l_1$ folgt. Also ist f homogen vom Grad k_0 und g homogen vom Grad l_0. Dies beweist die Behauptung. ■

Ist nun $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2] \setminus \{0\}$ homogen vom Grad 2, so gibt es folgende Möglichkeiten für die Zerlegung von f in $\overline{K}[x_0, x_1, x_2]$:

- **Fall 1:** f ist irreduzibel über $\overline{K}$.

- **Fall 2:** f ist reduzibel über $\overline{K}$, es gibt also homogene Polynome $\ell_1, \ell_2 \in \overline{K}[x_0, x_1, x_2]$ vom Grad 1 mit
$$f = \ell_1 \ell_2.$$
Man kann zwei Fälle unterscheiden:
  - **Fall 2.1:** ℓ_1 und ℓ_2 sind linear unabhängig (über $\overline{K}$). Dann sind $\{\ell_1 = 0\}$ und $\{\ell_2 = 0\}$ zwei verschiedene Geraden, die sich in einem Punkt schneiden. $\{f = 0\}$ besteht aus zwei sich schneidenden Geraden:
$$\{f = 0\} = \{\ell_1 = 0\} \cup \{\ell_2 = 0\} \quad \text{mit} \quad \#\{\ell_1 = 0\} \cap \{\ell_2 = 0\} = 1.$$
  - **Fall 2.2:** ℓ_1 und ℓ_2 sind linear abhängig (über $\overline{K}$)).
Dann gibt es eine Zahl $c \in \overline{K}^*$ mit $\ell_2 = c\,\ell_1$, also $f = c\ell_1^2$. Geometrisch gilt $\{f = 0\} = \{\ell_1 = 0\}$, $f = 0$ besteht also nur aus der Geraden $\ell_1 = 0$. Wegen des Exponenten 2 in der Zerlegung $f = c\ell_1^2$ sagt man manchmal auch, $f = 0$ ist eine **Doppelgerade**.

Die Bilder sollen die Fälle 1, 2.1 und 2.2 illustrieren.



Das folgende Lemma stellt eine Verbindung zwischen Reduzibilität und Singularität her.

LEMMA. *Die projektive ebene Quadrik C sei gegeben durch das homogene Polynom $f \in K[x_0, x_1, x_2]$ vom Grad 2.*

- *Ist f reduzibel über $\overline{K}$, d.h. $f = \ell_1\ell_2$ mit Linearformen $\ell_1, \ell_2 \in \overline{K}[x_0, x_1, x_2]$, so sind die Singularitäten genau die Punkte des Durchschnitts $\{\ell_1 = \ell_2 = 0\}$.*
  - *Sind ℓ_1, ℓ_2 linear unabhängig (über $\overline{K}$), so hat C genau den Schnittpunkt der beiden Geraden $\ell_1 = 0$ und $\ell_2 = 0$ als Singularität.*
  - *Sind ℓ_1, ℓ_2 linear abhängig (über $\overline{K}$), so sind alle Punkte von C Singularitäten.*
- *Ist C singulär und $P \in C(\overline{K})$ eine Singularität von C, so zerfällt C in zwei Geraden, die durch den Punkt P gehen.*

Beweis:

- Mit $f = \ell_1\ell_2$ gilt
$$\frac{\partial f}{\partial x_i}(x_0, x_1, x_2) = \frac{\partial \ell_1}{\partial x_i} \cdot \ell_2(x_0, x_1, x_2) + \frac{\partial \ell_2}{\partial x_i} \cdot \ell_1(x_0, x_1, x_2).$$
Sei $P = (p_0 : p_1 : p_2) \in C(\overline{K})$ ein beliebiger Kurvenpunkt, wobei wir aus Symmetriegründen o.E. $\ell_1(p_0, p_1, p_2) = 0$ annehmen können.
Sei weiter $\ell_1(x_0, x_1, x_2) = b_0x_0 + b_1x_1 + b_2x_2$. Dann gilt:
$$\begin{aligned} P \text{ Singularität von } C &\iff \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0 \text{ für } i = 0, 1, 2 \iff \\ &\iff b_i\ell_2(p_0, p_1, p_2) = 0 \text{ für } i = 0, 1, 2 \iff \\ &\iff \ell_2(p_0, p_1, p_2) = 0. \end{aligned}$$
Genau die Punkte des Durchschnitts $\{\ell_1 = 0\} \cap \{\ell_2 = 0\}$ sind also die Singularitäten von C. Dies beweist den ersten Teil des Lemmas.

- Sei nun $P \in C(\overline{K})$ ein singulärer Punkt von C. Nach Koordinatenwechsel können wir o.E. $P = (1:0:0)$ annehmen. Wir schreiben

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

und erhalten

$$\frac{\partial f}{\partial x_0} = 2a_0x_0 + a_1x_1 + a_2x_2, \quad \frac{\partial f}{\partial x_1} = a_1x_0 + 2a_3x_1 + a_4x_2, \quad \frac{\partial f}{\partial x_2} = a_2x_0 + a_4x_1 + 2a_5x_2.$$

Nun ist

$$f(1,0,0) = a_0, \quad \frac{\partial f}{\partial x_0}(1,0,0) = 2a_0, \quad \frac{\partial f}{\partial x_1}(1,0,0) = a_1, \quad \frac{\partial f}{\partial x_2}(1,0,0) = a_2.$$

Da $(1:0:0)$ ein singulärer Kurvenpunkt sein soll, ist $a_0 = a_1 = a_2 = 0$, also

$$f = a_3x_1^2 + a_4x_1x_2 + a_5x_2^2.$$

Nun ist f ein homogenes Polynom in den zwei Variablen x_1, x_2, das dann nach einem früheren Lemma über $\overline{K}$ in Linearfaktoren zerfällt:

$$f = a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = (b_1x_1 + b_2x_2)(c_1x_1 + c_2x_2).$$

Daraus folgt die Behauptung. ■

Wir betrachten jetzt die Frage nach Reduzibilität und Singularität nochmals von einem anderen Blickwinkel aus. Zu

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

bilden wir die Ableitungen

$$\begin{aligned} \frac{\partial f}{\partial x_0} &= 2a_0x_0 + a_1x_1 + a_2x_2, \\ \frac{\partial f}{\partial x_1} &= a_1x_0 + 2a_3x_1 + a_4x_2, \\ \frac{\partial f}{\partial x_2} &= a_2x_0 + a_4x_1 + 2a_5x_2. \end{aligned}$$

Dies können wir auch so schreiben:

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = A_f \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \text{ mit } A_f = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}.$$

Die Matrix A_f ist genau die Hesse-Matrix $(\frac{\partial^2 f}{\partial x_i \partial x_j})_{0 \le i,j \le 2}$ von f. Die Determinante ist das zu f gehörige Hesse-Polynom, das in diesem Fall konstant ist:

$$H_f = \det(A_f) = 2 \cdot \left(4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5\right).$$

In Charakteristik 2 ist also $H_f = 0$. Dies deutet schon darauf hin, dass sich die Charakteristik 2 anders verhält als Charakteristik $\neq 2$.
Wir beschäftigen uns zunächst mit dem Fall $\mathrm{char}(K) \neq 2$.

LEMMA. *($\mathrm{char}(K) \neq 2$) Sei C eine projektive ebene Quadrik, die durch das Polynom f definiert wird. Dann gilt für $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2$:*

$$P = (p_0 : p_1 : p_2) \text{ ist singulärer Punkt von } C \iff \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} \in \mathrm{Kern}(A_f).$$

Beweis: Für $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2$ gilt mit $\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = A_f \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$

$$\frac{\partial f}{\partial x_0}(P) = \frac{\partial f}{\partial x_1}(P) = \frac{\partial f}{\partial x_2}(P) = 0 \quad \iff \quad \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} \in \mathrm{Kern}(A_f).$$

Daher ist die Implikation $\Longrightarrow$ im obigen Lemma klar. Ist umgekehrt $\begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} \in \mathrm{Kern}(A_f)$, so folgt

$$\frac{\partial f}{\partial x_0}(P) = \frac{\partial f}{\partial x_1}(P) = \frac{\partial f}{\partial x_2}(P) = 0.$$

Die Euler-Relation liefert

$$2 \cdot f(p_0, p_1, p_2) = p_0 \frac{\partial f}{\partial x_0}(p_0, p_1, p_2) + p_1 \frac{\partial f}{\partial x_1}(p_0, p_1, p_2) + p_2 \frac{\partial f}{\partial x_2}(p_0, p_1, p_2) = 0,$$

also wegen $\mathrm{char}(K) \neq 2$ dann $f(P) = 0$, d.h. $P \in C(\overline{K})$, sodass P ein singulärer Punkt von C ist. ■

Es gilt $\dim \mathrm{Kern}(A_f) = 3 - \mathrm{Rang}(A_f)$. Wir unterscheiden nun die Fälle $\mathrm{Rang}(A_f) = 1, 2, 3$.

SATZ. *($\mathrm{char}(K) \neq 2$) Für eine über K durch das Polynom*

$$f = a_0 x_0^2 + a_1 x_0 x_1 + a_2 x_0 x_2 + a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2$$

definierte projektive ebene Quadrik gilt:

- *Im Fall* $\mathrm{Rang}(A_f) = 1$ *gibt es* $c, b_0, b_1, b_2 \in K$ *mit*

  $$f(x_0, x_1, x_2) = c(b_0 x_0 + b_1 x_1 + b_2 x_2)^2.$$

  Genauer:
  - *Gilt* $a_0 \neq 0$*, so ist*

    $$f = \frac{1}{4a_0} \cdot (2a_0 x_0 + a_1 x_1 + a_2 x_2)^2 .$$

  - *Gilt* $a_0 = 0$ *und* $a_3 \neq 0$*, so ist* $a_1 = a_2 = 0$ *und*

    $$f = \frac{1}{4a_3} \cdot (2a_3 x_1 + a_4 x_2)^2 .$$

  - *Gilt* $a_0 = 0$ *und* $a_3 = 0$*, so gilt* $a_1 = 0$*,* $a_2 = 0$*,* $a_4 = 0$*,* $a_5 \neq 0$ *und*

    $$f = a_5 x_2^2.$$

- *Gibt es* $c, b_0, b_1, b_2 \in \overline{K}$ *mit*

  $$f(x_0, x_1, x_2) = c(b_0 x_0 + b_1 x_1 + b_2 x_2)^2,$$

  so gilt $\mathrm{Rang}(A_f) = 1$.

Beweis:

- $\mathrm{Rang}(A_f) = 1$ impliziert, dass alle 2×2-Untermatrizen von

  $$A_f = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}$$

  Determinante 0 haben. Dies sind die 9 Untermatrizen:

  $$\begin{pmatrix} 2a_0 & a_1 \\ a_1 & 2a_3 \end{pmatrix}, \begin{pmatrix} 2a_0 & a_2 \\ a_1 & a_4 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 \\ 2a_3 & a_4 \end{pmatrix}, \begin{pmatrix} 2a_0 & a_1 \\ a_2 & a_4 \end{pmatrix}, \begin{pmatrix} 2a_0 & a_2 \\ a_2 & 2a_5 \end{pmatrix},$$
  $$\begin{pmatrix} a_1 & a_2 \\ a_4 & 2a_5 \end{pmatrix}, \begin{pmatrix} a_1 & 2a_3 \\ a_2 & a_4 \end{pmatrix}, \begin{pmatrix} a_1 & a_4 \\ a_2 & 2a_5 \end{pmatrix}, \begin{pmatrix} 2a_3 & a_4 \\ a_4 & 2a_5 \end{pmatrix}.$$

Daraus ergeben sich die Gleichungen

$$4a_0a_3 = a_1^2, \quad 2a_0a_4 = a_1a_2, \quad a_1a_4 = 2a_2a_3,$$
$$4a_0a_5 = a_2^2, \quad 2a_1a_5 = a_2a_4, \quad 4a_3a_5 = a_4^2.$$

(Einige Untermatrizen liefern die gleiche Gleichung.)

- Hier sind nochmals die Gleichungen:

$4a_0a_3 = a_1^2, \quad 2a_0a_4 = a_1a_2, \quad a_1a_4 = 2a_2a_3, \quad 4a_0a_5 = a_2^2, \quad 2a_1a_5 = a_2a_4, \quad 4a_3a_5 = a_4^2.$

  - **Fall $a_0 \neq 0$:** Dann erhalten wir aus den letzten Gleichungen

$$a_3 = \frac{a_1^2}{4a_0}, \quad a_4 = \frac{a_1a_2}{2a_0}, \quad a_5 = \frac{a_2^2}{4a_0}.$$

    Es folgt

$$\begin{aligned} f &= a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = \\ &= a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + \frac{a_1^2}{4a_0}x_1^2 + \frac{a_1a_2}{2a_0}x_1x_2 + \frac{a_2^2}{4a_0}x_2^2 = \\ &= \frac{1}{4a_0} \cdot \left(4a_0^2x_0^2 + 4a_0a_1x_0x_1 + 4a_0a_2x_0x_2 + a_1^2x_1^2 + 2a_1a_2x_1x_2 + a_2^2x_2^2\right) = \\ &= \frac{1}{4a_0} \cdot (2a_0x_0 + a_1x_1 + a_2x_2)^2 . \end{aligned}$$

  - **Fall $a_0 = 0$:** Aus obigen Gleichungen folgt dann auch

$$a_1 = 0, \quad a_2 = 0.$$

    Es bleibt die Gleichung

$$4a_3a_5 = a_4^2.$$

    * **Fall $a_0 = 0$, $a_3 \neq 0$:** Dann ist

$$a_1 = 0, \quad a_2 = 0, \quad a_5 = \frac{a_4^2}{4a_3}$$

      und

$$\begin{aligned} f &= a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = a_3x_1^2 + a_4x_1x_2 + \frac{a_4^2}{4a_3}x_2^2 = \\ &= \frac{1}{4a_3} \cdot \left(4a_3^2x_1^2 + 4a_3a_4x_1x_2 + a_4^2x_2^2\right) = \frac{1}{4a_3} \cdot (2a_3x_1 + a_4x_2)^2 . \end{aligned}$$

    * **Fall $a_0 = 0$, $a_3 = 0$:** Dann gilt

$$a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = 0,$$

      und damit

$$f = a_5x_2^2.$$

- Wir können o.E. $c = 1$, also $f = (b_0x_0 + b_1x_1 + b_2x_2)^2$ annehmen.

  Wegen

$$f = b_0^2x_0^2 + 2b_0b_1x_0x_1 + 2b_0b_2x_0x_2 + b_1^2x_1^2 + 2b_1b_2x_1x_2 + b_2^2x_2^2$$

  gilt

$$a_0 = b_0^2, \quad a_1 = 2b_0b_1, \quad a_2 = 2b_0b_2, \quad a_3 = b_1^2, \quad a_4 = 2b_1b_2, \quad a_5 = b_2^2.$$

Dann ist

$$A_f = \begin{pmatrix} 2b_0^2 & 2b_0b_1 & 2b_0b_2 \\ 2b_1b_0 & 2b_1^2 & 2b_1b_2 \\ 2b_2b_0 & 2b_2b_1 & 2b_2^2 \end{pmatrix} = 2 \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \begin{pmatrix} b_0 & b_1 & b_2 \end{pmatrix}.$$

Alle Zeilen der Matrix A_f sind Vielfache des Vektors (b_0, b_1, b_2),
weswegen $\mathrm{Rang}(A_f) = 1$ gilt. Dies beweist die Behauptung. ■

Im Fall $\mathrm{Rang}(A_f) = 1$ kann man also aus sofort die Faktorisierung von f angeben. Bei $\mathrm{Rang}(A_f) = 2$ ist dies nicht mehr der Fall.

SATZ. *($\mathrm{char}(K) \neq 2$) Für einen über K durch das Polynom*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

definierten ebenen Kegelschnitt sind folgende Aussagen äquivalent:

- $\mathrm{Rang}(A_f) = 2$.
- *C hat genau eine Singularität.*
- *Es gibt linear unabhängige Linearformen $\ell_1, \ell_2 \in \overline{K}[x_0, x_1, x_2]$ mit $f = \ell_1\ell_2$.*

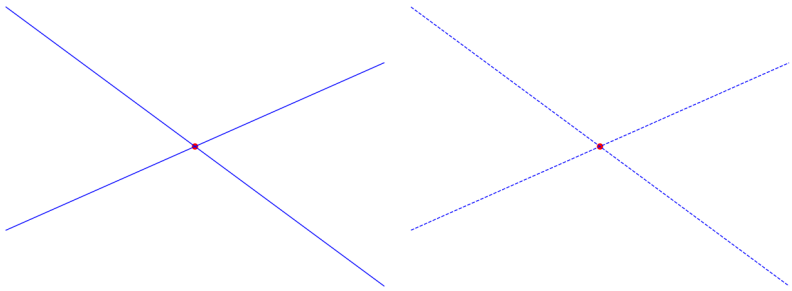
Der singuläre Punkt ist in diesem Fall $(p_0 : p_1 : p_2)$ mit $\mathrm{Kern}(A_f) = K \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$. *Insbesondere ist $(p_0 : p_1 : p_2) \in C(K)$.*

Beweis: $\mathrm{Rang}(A_f) = 2$ ist gleichwertig damit, dass es genau eine Singularität gibt, nämlich $(p_0 : p_1 : p_2)$, wenn

$$\mathrm{Kern}(A_f) = K \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$$

gilt. Den Rest haben wir bereits oben gezeigt. ■

Die folgenden Bilder sollen Quadriken mit $\mathrm{Rang}(A_f) = 2$ zeigen. Die Singularität ist rot gezeichnet. Im ersten Fall sind die beiden Geraden über K definiert, also über K „sichtbar“. Im zweiten Fall sind die Geraden nicht über K definiert, also über K „nicht sichtbar“ weswegen wir die Geraden gestrichelt haben.



Beispiel: Als Grundkörper wählen wir $K = \mathbb{R}$. Das Polynom

$$f(x_0, x_1, x_2) = x_1^2 - x_2^2 \text{ mit } A_f = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

definiert eine Quadrik, die wegen

$$f(x_0, x_1, x_2) = (x_1 - x_2)(x_1 + x_2)$$

aus den beiden, über $\mathbb{R}$ definierten Geraden

$$\{x_1 = x_2\} \text{ und } \{x_2 = -x_1\}$$

besteht.
Das Polynom

$$g(x_0, x_1, x_2) = x_1^2 + x_2^2 \text{ mit } A_g = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

definiert eine Quadrik mit Singularität in $(1 : 0 : 0)$. Über $\mathbb{C}$ zerfällt die Quadrik wegen $g(x_0, x_1, x_2) = (x_1 - ix_2)(x_1 + ix_2)$ in die beiden Geraden

$$\{x_1 = ix_2\} \text{ und } \{x_1 = -ix_2\},$$

die aber über $\mathbb{R}$ nicht definiert sind. Einziger über $\mathbb{R}$ definierter Punkt ist die Singularität $(1 : 0 : 0)$.

Das vorangegangene Beispiel lässt sich leicht verallgemeinern.

Beispiel: Sei K ein Körper mit von 2 verschiedener Charakteristik und $c \in K^*$. Wir betrachten die Quadrik C, die durch

$$f(x_0, x_1, x_2) = x_1^2 - cx_2^2$$

definiert wird. Es ist

$$A_f = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2c \end{pmatrix} \text{ mit } \operatorname{Rang}(A_f) = 2 \text{ und } \operatorname{Kern}(A_f) = K \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

C ist singulär in $(1:0:0)$. Wegen

$$f = (x_1 - \sqrt{c}x_2)(x_1 + \sqrt{c}x_2) \in \overline{K}[x_0, x_1, x_2]$$

besteht C aus den beiden Geraden

$$\{x_1 = \sqrt{c}x_2\} \text{ und } \{x_1 = -\sqrt{c}x_2\}.$$

Die Geraden sind genau dann über K definiert, wenn $\sqrt{c} \in K$ gilt, d.h. wenn c ein Quadrat in K ist.

SATZ. *(*$\operatorname{char}(K) \neq 2$*) Für einen über K durch das Polynom*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

definierten ebenen Kegelschnitt sind folgende Aussagen äquivalent:

- *C ist nichtsingulär.*
- $\operatorname{Rang}(A_f) = 3$.
- *$H_f \neq 0$, also* $4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 \neq 0$.
- *C ist absolut irreduzibel.*

Beweis: Die Äquivalenz von (1), (2), (3), also (1) $\iff$ (2) $\iff$ (3), folgt sofort aus dem vorangegangenen Lemma. Die Äquivalenz (1) $\iff$ (4) haben wir bereits zuvor gezeigt. ■

Nun betrachten wir noch kurz den Fall der Charakteristik 2.

SATZ. *Sei* $\operatorname{char}(K) = 2$ *und C eine über K durch das Polynom* $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0, x_1, x_2] \setminus \{0\}$ *definierte projektive ebene Quadrik.*

- *Es ist*
$$A_f = \begin{pmatrix} 0 & a_1 & a_2 \\ a_1 & 0 & a_4 \\ a_2 & a_4 & 0 \end{pmatrix} \quad \textit{und} \quad \operatorname{Rang}(A_f) \in \{0, 2\}.$$
- *Ist* $(a_1, a_2, a_4) = 0$*, so gilt* $\operatorname{Rang}(A_f) = 0$ *und über* $\overline{K}$
$$f = a_0x_0^2 + a_3x_1^2 + a_5x_2^2 = \left(\sqrt{a_0}x_0 + \sqrt{a_3}x_1 + \sqrt{a_5}x_2\right)^2.$$
Alle Punkte der Kurve sind singulär.
- *Ist* $(a_1, a_2, a_4) \neq 0$*, so gilt* $\operatorname{Rang}(A_f) = 2$*,*
$$\operatorname{Kern}(A_f) = K \begin{pmatrix} a_4 \\ a_2 \\ a_1 \end{pmatrix}$$
und
$$f(a_4, a_2, a_1) = a_0a_4^2 + a_1^2a_5 + a_1a_2a_4 + a_2^2a_3.$$
Es gilt:
$$C \textit{ singulär} \quad \iff \quad a_0a_4^2 + a_1^2a_5 + a_1a_2a_4 + a_2^2a_3 = 0.$$
Die einzige Singularität ist in diesem Fall $(a_4 : a_2 : a_1)$.

Beweis:

- Es ist $\det(A_f) = 0$. Die Rangaussagen erhält man dann durch ein paar Fallunterscheidungen.

- Da in $\overline{K}$ die Gleichung $2 = 0$ gilt, ergibt sich

$$\begin{aligned}(\sqrt{a_0}x_0 + \sqrt{a_3}x_1 + \sqrt{a_5}x_2)^2 &= a_0x_0^2 + a_3x_1^2 + a_5x_2^2 + 2\sqrt{a_0}\sqrt{a_3}x_0x_1 + 2\sqrt{a_0}\sqrt{a_5}x_0x_2 + 2\sqrt{a_3}\sqrt{a_5}x_1x_2 = \\ &= a_0x_0^2 + a_3x_1^2 + a_5x_2^2,\end{aligned}$$

  wie behauptet.
- Es ist

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = \begin{pmatrix} 0 & a_1 & a_2 \\ a_1 & 0 & a_4 \\ a_2 & a_4 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

  Im Fall $(a_1, a_2, a_4) \neq 0$ hat die Matrix Rang 2. Da aber (a_4, a_2, a_1) im Kern liegt, gilt

$$\{\frac{\partial f}{\partial x_0} = \frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial x_2} = 0\} = \{(a_4 : a_2 : a_1)\}.$$

  Nun rechnet man nach, dass in Charakteristik 2

$$f(a_4, a_2, a_1) = a_0a_4^2 + a_1^2a_5 + a_1a_2a_4 + a_2^2a_3$$

  gilt. Daher folgt nun:

$$\begin{aligned} C \text{ singulär} \quad &\iff \quad \{\frac{\partial f}{\partial x_0} = \frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial x_2} = f = 0\} \neq \emptyset \quad \iff \\ &\iff \quad \{\frac{\partial f}{\partial x_0} = \frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial x_2} = 0\} \cap \{f = 0\} \neq \emptyset \quad \iff \\ &\iff \quad \{(a_4 : a_2 : a_1)\} \cap \{f = 0\} \neq \emptyset \quad \iff \\ &\iff \quad f(a_4, a_2, a_1) = 0. \end{aligned}$$

  Dies beweist die Behauptung. ■

Allgemein gilt für $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$

$$H_f = \det(A_f) = 2 \cdot \left(4a_0a_4a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5\right).$$

Wir erhalten dann charakteristikunabhängig folgende Charakterisierung für die Singularität einer Quadrik:

FOLGERUNG. *Für eine über einem Körper K (beliebiger Charakteristik) durch ein homogenes Polynom $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0, x_1, x_2]$ definierte projektive ebene Quadrik C gilt:*

$$C \text{ singulär} \quad \iff \quad 4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 = 0.$$

(Im $\mathbb{P}^5$ aller ebenen Quadriken bilden die singulären Quadriken also eine kubische Hyperfläche.)

Beweis: Im Fall $\mathrm{char}(K) \neq 2$ wurde die Aussage bereits in einem früheren Satz formuliert. Im Fall $\mathrm{char}(K) = 2$ ergibt sich die Behauptung aus der Gleichung

$$4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 = a_0a_4^2 + a_1^2a_5 + a_1a_2a_4 + a_2^2a_3$$

und dem entsprechenden Satz für Charakteristik 2. ■

2. Beschreibung von ebenen projektiven Quadriken in Charakteristik $\neq 2$ durch Matrizen

Wir hatten zuvor einem homogenen quadratischen Polynom

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0, x_1, x_2]$$

die Matrix

$$A_f = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}$$

zugeordnet, wobei dann gilt

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = A_f \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Nun setzen wir $\mathrm{char}(K) \neq 2$ voraus; dann existiert $\frac{1}{2} \in K$. Definieren wir

$$A = \frac{1}{2} A_f = \begin{pmatrix} a_0 & \frac{1}{2}a_1 & \frac{1}{2}a_2 \\ \frac{1}{2}a_1 & a_3 & \frac{1}{2}a_2 \\ \frac{1}{2}a_2 & \frac{1}{2}a_4 & a_5 \end{pmatrix} \quad \text{und} \quad x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix},$$

so gilt

$$f(x) = x^t A x.$$

Dabei ist A eine symmetrische Matrix. (In der Sprache der Linearen Algebra: f ist eine quadratische Form in drei Veränderlichen.)

Koordinatenwechsel: Bei einem projektiven Koordinatenwechsel $x = Ty$ mit $T \in \mathrm{GL}_3(K)$ ergibt sich aus $f = x^t A x$

$$f = y^t (T^t A T) y,$$

d.h. A geht über in $T^t A T$, wie das auch aus der Linearen Algebra bekannt ist.

Ableitungen: Es gilt

$$\frac{\partial f}{\partial x_0} = 2a_0 x_0 + a_1 x_1 + a_2 x_2, \quad \frac{\partial f}{\partial x_1} = a_1 x_0 + 2a_3 x_1 + a_4 x_1, \quad \frac{\partial f}{\partial x_2} = a_2 x_0 + a_4 x_1 + 2a_5 x_2,$$

also

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = \begin{pmatrix} 2a_0 x_0 + a_1 x_1 + a_2 x_2 \\ a_1 x_0 + 2a_3 x_1 + a_4 x_4 \\ a_2 x_0 + a_4 x_1 + 2a_5 x_2 \end{pmatrix} = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = 2Ax.$$

Hier kann man auch nochmals explizit die Eulersche Relation sehen:

$$\frac{\partial f}{\partial x_0} x_0 + \frac{\partial f}{\partial x_1} x_1 + \frac{\partial f}{\partial x_2} x_2 = \begin{pmatrix} \frac{\partial f}{\partial x_0} & \frac{\partial f}{\partial x_1} & \frac{\partial f}{\partial x_2} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = (2Ax)^t x = 2x^t A^t x = 2x^t A x = 2f.$$

Der Rang der Matrix A wird auch als **Rang der Quadrik** C bezeichnet. C ist genau dann nichtsingulär, wenn C Rang 3 hat. Für das Folgende sei vorausgesetzt, dass C nichtsingulär ist.

Tangenten: Sei $P = (p_0 : p_1 : p_2) \in C(\overline{K})$ und $p = \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$. Die Tangente in P an C wird dann durch

$$\frac{\partial f}{\partial x_0}(P) x_0 + \frac{\partial f}{\partial x_1}(P) x_1 + \frac{\partial f}{\partial x_2}(P) x_2 = 0$$

definiert. Nun ist

$$\begin{pmatrix} \frac{\partial f}{\partial x_0}(P) \\ \frac{\partial f}{\partial x_1}(P) \\ \frac{\partial f}{\partial x_2}(P) \end{pmatrix} = 2Ap,$$

sodass wir die Tangentengleichung auch in der Form

$$0 = \begin{pmatrix} \frac{\partial f}{\partial x_0}(P) & \frac{\partial f}{\partial x_1}(P) & \frac{\partial f}{\partial x_2}(P) \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = (2Ap)^t x = 2p^t A x$$

schreiben können. Die Tangente in P an C wird also beschrieben durch die Gleichung

$$p^t A x = 0.$$

Ist $P = (p_0 : p_1 : p_2) \in C(\overline{K})$ ein Kurvenpunkt und $p = \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$, so ist

$$p^t Ax = 0$$

die Tangente in P an C.
Ist P kein Kurvenpunkt, so wird durch

$$p^t Ax = 0$$

die sogenannte **Polare von P bezüglich C** definiert; auch die Sprechweise **Polare von C bezüglich P** findet man.
Wegen

$$\begin{pmatrix} \frac{\partial f}{\partial x_0}(x_0, x_1, x_2) \\ \frac{\partial f}{\partial x_1}(x_0, x_1, x_2) \\ \frac{\partial f}{\partial x_2}(x_0, x_1, x_2) \end{pmatrix} = 2Ax$$

gilt

$$\frac{\partial f}{\partial x_0}(P)x_0 + \frac{\partial f}{\partial x_1}(P)x_1 + \frac{\partial f}{\partial x_2}(P)x_2 = 2x^t Ap = 2p^t Ax = p_0\frac{\partial f}{\partial x_0} + p_1\frac{\partial f}{\partial x_1} + p_2\frac{\partial f}{\partial x_2}.$$

Die Polare lässt sich also ohne Matrizen in der Form

$$\frac{\partial f}{\partial x_0}(P)x_0 + \frac{\partial f}{\partial x_1}(P)x_1 + \frac{\partial f}{\partial x_2}(P)x_2 = 0$$

oder in der Form

$$p_0\frac{\partial f}{\partial x_0} + p_1\frac{\partial f}{\partial x_1} + p_2\frac{\partial f}{\partial x_2} = 0$$

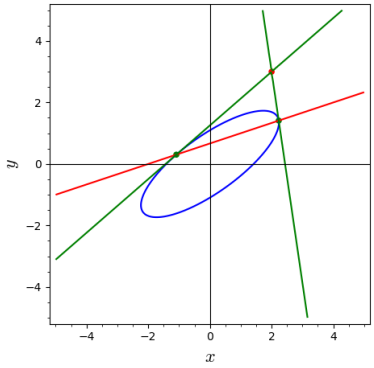
darstellen. Mittels der letzten Darstellung wird „Polare“ auch für Kurven höheren Grades definiert.

DEFINITION. *Ist C eine über K durch das Polynom $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ definierte nichtsinguläre projektive ebene Kurve vom Grad $d \geq 2$ und $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2$, so definiert das Polynom*

$$p_0\frac{\partial f}{\partial x_0}(x_0, x_1, x_2) + p_1\frac{\partial f}{\partial x_1}(x_0, x_1, x_2) + p_2\frac{\partial f}{\partial x_2}(x_0, x_1, x_2)$$

die **Polare** *von P bezüglich C, falls das Polynom nicht identisch verschwindet.*

Im Bild ist die Quadrik blau, Punkt und zugehörige Polare rot eingezeichnet.



SATZ. *Sei C eine durch das Polynom f definierte nichtsinguläre projektive ebene Kurve vom Grad $d \geq 2$, $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2$ ein Punkt und*

$$g = p_0\frac{\partial f}{\partial x_0} + p_1\frac{\partial f}{\partial x_1} + p_2\frac{\partial f}{\partial x_2}.$$

Der Durchschnitt $\{f = g = 0\}$ besteht genau aus den Kurvenpunkten $Q = (q_0 : q_1 : q_2)$, deren Tangente durch P geht.

Beweis: Sei $Q = (q_0 : q_1 : q_2)$ ein Punkt der Kurve, d.h. $f(q_0, q_1, q_2) = 0$. Die Tangente T_Q in Q an C wird durch die Gleichung

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

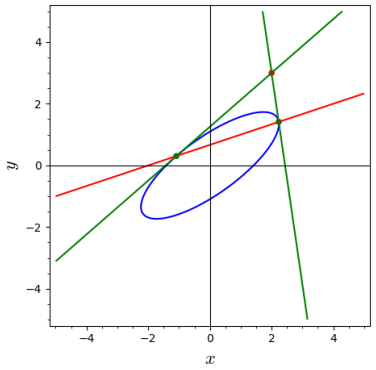
beschrieben. Damit gilt:

$$\begin{aligned} P \in T_Q \quad &\Longleftrightarrow \quad p_0 \frac{\partial f}{\partial x_0}(q_0, q_1, q_2) + p_1 \frac{\partial f}{\partial x_1}(q_0, q_1, q_2) + p_2 \frac{\partial f}{\partial x_2}(q_0, q_1, q_2) = 0 \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad g(q_0, q_1, q_2) = 0. \end{aligned}$$

Dies beweist die Behauptung. ■

Wir formulieren den vorangegangenen nochmals etwas genauer für Quadriken.

SATZ. *(*$\mathrm{char}(K) \neq 2$*) Sei C eine nichtsinguläre projektive ebene Quadrik und $P \in \mathbb{P}^2 \setminus C(\overline{K})$. Dann gibt es genau zwei Tangenten an C, die durch P gehen. Die Berührpunkte dieser Tangenten mit C sind genau die Schnittpunkte der Polaren des Punktes P mit C.*



Beweis: Wir schreiben $p = \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$ und $f = x^t A x$ mit einer symmetrischen Matrix A.

- Sei $Q = (q_0 : q_1 : q_2) \in C(\overline{K})$ und $q = \begin{pmatrix} q_0 \\ q_1 \\ q_2 \end{pmatrix}$. Da Q auf der Quadrik liegt, gilt $q^t A q = 0$. Die Tangente in Q an C ist $q^t A x = 0$, die Polare des Punktes P bezüglich C ist $p^t A x = 0$.

  Äquivalent sind folgende Aussagen:

  $$\begin{aligned} &P \text{ liegt auf der Tangente (in } Q \text{ an } C) \quad \Longleftrightarrow \quad q^t A p = 0 \quad \Longleftrightarrow \\ \Longleftrightarrow \quad &p^t A q = 0 \quad \Longleftrightarrow \quad Q \text{ liegt auf der Polaren des Punktes } P \text{ bezüglich } C. \end{aligned}$$

  Die Tangenten an C, die durch P gehen, berühren C also genau in den Schnittpunkten der Polaren mit C.
- Die Polare des Punktes P ist die Gerade $p^t A x = 0$. Sie schneidet die Quadrik zweimal, wenn man mit Vielfachheiten zählt. Gibt es also zwei verschiedene Schnittpunkte, so folgt damit unsere Behauptung.
- Angenommen, die Polare $p^t A x = 0$ würde C nur in einem Punkt $Q = (q_0 : q_1 : q_2)$ schneiden. Dann wäre die Schnittvielfachheit 2,

  die Polare würde also mit der Tangenten an C in Q übereinstimmen. Die Tangente ist $q^t A x = 0$ mit $q = \begin{pmatrix} q_0 \\ q_1 \\ q_2 \end{pmatrix}$. Dann gäbe es aber eine Konstante $\lambda \neq 0$ mit $q^t A x = \lambda p^t A x$, also $q^t A = \lambda p^t A$, was wegen $\mathrm{Rang}(A) = 3$ dann $q = \lambda p$ und damit $P = Q \in C(\overline{K})$ ergeben würde, im Widerspruch zur Annahme. ■

Beispiel: Wir betrachten (über $\mathbb{R}$) die durch

$$f = 6x_0^2 - 3x_1^2 + 6x_1x_2 - 5x_2^2$$

definierte projektive ebene Quadrik C. Es ist

$$\frac{\partial f}{\partial x_0} = 12x_0, \quad \frac{\partial f}{\partial x_1} = -6x_1 + 6x_2, \quad \frac{\partial f}{\partial x_2} = 6x_1 - 10x_2.$$

Die Polare des Punktes $P = (1:2:3)$ bezüglich C wird durch

$$1 \cdot \frac{\partial f}{\partial x_0} + 2 \cdot \frac{\partial f}{\partial x_1} + 3 \cdot \frac{\partial f}{\partial x_2} = 12x_0 + 2 \cdot (-6x_1 + 6x_2) + 3 \cdot (6x_1 - 10x_2) = 12x_0 + 6x_1 - 18x_2$$

gegeben, ist also die Gerade

$$2x_0 + x_1 - 3x_2 = 0.$$

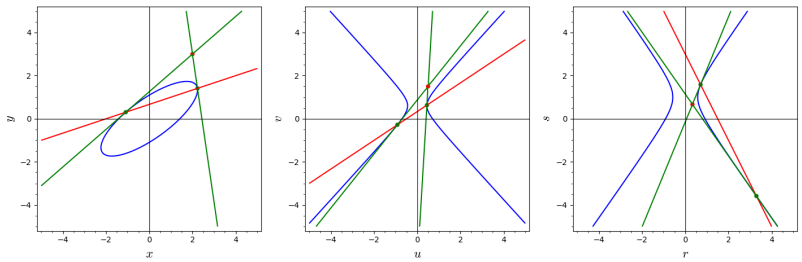
Die Schnittpunkte der Polaren mit der Kurve erhalten wir, indem wir $x_1 = -2x_0 + 3x_2$ in die Kurvengleichung einsetzen:

$$\begin{aligned} f(x_0, -2x_0 + 3x_2, x_2) &= \cdots = -6x_0^2 + 24x_0x_2 - 14x_2^2 = -14x_0^2 \cdot \left((\frac{x_2}{x_0})^2 - \frac{12}{7}(\frac{x_2}{x_0}) + \frac{3}{7} \right) = \\ &= -14x_0^2 \cdot \left(\frac{x_2}{x_0} - \frac{6+\sqrt{15}}{7} \right) \left(\frac{x_2}{x_0} - \frac{6-\sqrt{15}}{7} \right) = \\ &= -14 \cdot \left(x_2 - \frac{6+\sqrt{15}}{7} x_0 \right) \left(x_2 - \frac{6-\sqrt{15}}{7} x_0 \right). \end{aligned}$$

Daraus ergeben sich die beiden Schnittpunkte der Polaren mit der Kurve:

$$(1 : \frac{4+3\sqrt{15}}{7}, \frac{6+\sqrt{15}}{7}) \quad \text{und} \quad (1 : \frac{4-3\sqrt{15}}{7}, \frac{6-\sqrt{15}}{7}).$$

Die Bilder zeigen das Beispiel in den affinen Teilen U_0, U_1, U_2. Die Quadrik ist blau, Punkt und zugehörige Polare rot, die Tangenten grün eingezeichnet.



Bemerkung: ($\mathrm{char}(K) \neq 2$) Gegeben sei eine nichtsinguläre projektive ebene Quadrik C durch ein Polynom $f(x_0, x_1, x_2)$ und ein Punkt $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2 \setminus C(\overline{K})$. Wie bestimmt man die Geraden, die Tangenten an C sind und durch P gehen?

- Man bestimmt die partiellen Ableitungen

$$\frac{\partial f}{\partial x_0}, \quad \frac{\partial f}{\partial x_1}, \quad \frac{\partial f}{\partial x_2}.$$

- Man bestimmt die Polare von P bezüglich C:

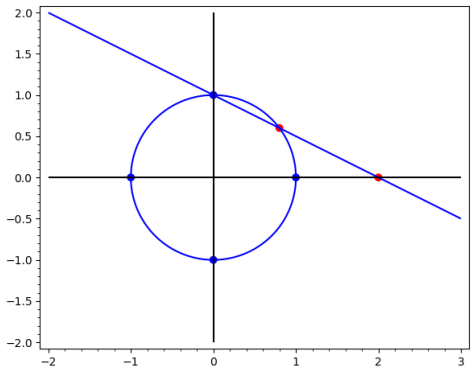
$$g = p_0 \frac{\partial f}{\partial x_0} + p_1 \frac{\partial f}{\partial x_1} + p_2 \frac{\partial f}{\partial x_2}.$$

- Man bestimmt die beiden Schnittpunkte S_1, S_2 der Polaren mit der Kurve.
- Die gesuchten Geraden sind dann

$$\frac{\partial f}{\partial x_0}(S_1)x_0 + \frac{\partial f}{\partial x_1}(S_1)x_1 + \frac{\partial f}{\partial x_2}(S_1)x_2 = 0 \quad \text{und} \quad \frac{\partial f}{\partial x_0}(S_2)x_0 + \frac{\partial f}{\partial x_1}(S_2)x_1 + \frac{\partial f}{\partial x_2}(S_2)x_2 = 0.$$

3. Nichtsinguläre ebene projektive Quadriken C mit $C(K) \neq \emptyset$

In der Einführung haben wir die rationalen Punkte des Einheitskreises $x^2 + y^2 = 1$ parametrisiert, indem wir zu den Geraden durch $(0, 1)$ den zweiten Schnittpunkt mit dem Kreis bestimmt haben.



Wir verallgemeinern dies nun.

Überlegung: Eine über K definierte ebene Quadrik C werde definiert durch das Polynom

$$f(x_0, x_1, x_2) = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0.$$

Wir nehmen an, dass $(1 : 0 : 0) \in C(K)$ gilt. Dann ist $a_0 = 0$, und affin wird die Quadrik durch das Polynom

$$f(1, x, y) = a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2$$

beschrieben.

Zu $u, v \in K$ mit $(u, v) \neq (0, 0)$ betrachten wir die Gerade, die sich durch

$$x = ut, \quad y = vt$$

parametrisieren lässt. Wir schneiden sie mit der Kurve, indem wir die Parametrisierung in $f(1, x, y)$ einsetzen:

$$f(1, ut, vt) = (a_1u + a_2v)t + (a_3u^2 + a_4uv + a_5v^2)t^2.$$

Für $t = 0$ erhalten wir den Schnittpunkt $(0, 0)$. Der zweite Schnittpunkt mit der Kurve ergibt sich für

$$t = -\frac{a_1u + a_2v}{a_3u^2 + a_4uv + a_5v^2},$$

falls der Ausdruck definiert ist. Der Schnittpunkt ist dann (x, y) mit

$$x = -\frac{u(a_1u + a_2v)}{a_3u^2 + a_4uv + a_5v^2}, \quad y = -\frac{v(a_1u + a_2v)}{a_3u^2 + a_4uv + a_5v^2}$$

bzw. projektiv:

$$(1 : x : y) = (a_3u^2 + a_4uv + a_5v^2 : -u(a_1u + a_2v) : -v(a_1u + a_2v)).$$

Dies führt zu folgendem Satz:

Satz. *Sei C eine über K durch das Polynom*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

definierte nichtsinguläre Quadrik mit $(1 : 0 : 0) \in C(K)$. (Daher ist $a_0 = 0$.) Dann definiert

$$\phi((u : v)) = (a_3u^2 + a_4uv + a_5v^2 : -u(a_1u + a_2v) : -v(a_1u + a_2v))$$

eine bijektive Abbildung

$$\phi : \mathbb{P}^1(K) \to C(K),$$

wobei die Umkehrabbildung $\phi^{-1} : C(K) \to \mathbb{P}^1(K)$ durch

$$\phi^{-1}((x_0 : x_1 : x_2)) = \begin{cases} (x_1 : x_2), & \text{falls } (x_0 : x_1 : x_2) \neq (1 : 0 : 0), \\ (a_2 : -a_1), & \text{falls } (x_0 : x_1 : x_2) = (1 : 0 : 0) \end{cases}$$

gegeben wird.

Beweis:

- Wir zeigen zunächst, dass ϕ als Abbildung $\mathbb{P}^1 \to \mathbb{P}^2$ definiert ist. Da die Einträge als Polynome in u, v homogen vom Grad 2 sind, müssen wir nur noch zeigen, dass die Einträge nicht alle gleichzeitig 0 sein können. Sei also
$$a_3u^2 + a_4uv + a_5v^2 = 0, \quad -u(a_1u + a_2v) = 0, \quad -v(a_1u + a_2v) = 0.$$
Da u und v nicht gleichzeitig 0 sind, gilt $a_1u + a_2v = 0$, also $(u : v) = (a_2 : -a_1)$. Setzen wir dies in die erste Gleichung ein, ergibt sich
$$a_3a_2^2 - a_4a_2a_1 + a_5a_1^2 = 0.$$
Wegen $a_0 = 0$ lässt sich dies (nach Multiplikation mit -1) auch in der Form
$$4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 = 0$$
schreiben. Wir haben aber gezeigt, dass dann C singulär wäre, im Widerspruch zur Voraussetzung. Also sind die drei Einträge nicht gleichzeitig 0. Also wird durch
$$\phi((u : v)) = (a_3u^2 + a_4uv + a_5v^2 : -u(a_1u + a_2v) : -v(a_1u + a_2v))$$
eine Abbildung $\phi : \mathbb{P}^1(K) \to \mathbb{P}^2(K)$ definiert.
- Nun rechnet man nach, dass
$$f(a_3u^2 + a_4uv + a_5v^2, -u(a_1u + a_2v), -v(a_1u + a_2v)) = 0$$
gilt (als Polynom in u, v). Damit erhalten wir eine Abbildung
$$\phi : \mathbb{P}^1(K) \to C(K).$$
- Wir definieren
$$\psi : C(K) \to \mathbb{P}^1(K) \text{ mit } \psi((x_0 : x_1 : x_2)) = \begin{cases} (x_1 : x_2), & \text{falls } (x_0 : x_1 : x_2)) \neq (1 : 0 : 0), \\ (a_2 : -a_1), & \text{falls } (x_0 : x_1 : x_2) = (1 : 0 : 0). \end{cases}$$
(Man überlegt sich sofort, dass ψ wohldefiniert ist.) Nun müssen wir noch zeigen, dass
$$\psi \circ \phi = \mathrm{id}_{\mathbb{P}^1(K)} \quad \text{und} \quad \phi \circ \psi = \mathrm{id}_{C(K)}$$
gilt.
- Wir betrachten $\psi \circ \phi$. Sei $(u : v) \in \mathbb{P}^1(K)$. Ist $(u : v) \neq (a_2 : -a_1)$, so ist $a_1u + a_2v \neq 0$ und damit $\phi((u : v)) \neq (1 : 0 : 0)$, was dann
$$\begin{aligned} \psi(\phi((u : v))) &= \psi((a_3u^2 + a_4uv + a_5v^2 : -u(a_1u + a_2v) : -v(a_1u + a_2v)) = \\ &= (-u(a_1u + a_2v) : -v(a_1u + a_2v)) = (u : v) \end{aligned}$$
liefert. Ist $(u : v) = (a_2 : -a_1)$, so gilt
$$\psi(\phi((a_2 : -a_1))) = \psi((1 : 0 : 0)) = (a_2 : -a_1).$$
Damit folgt
$$\psi \circ \phi = \mathrm{id}_{\mathbb{P}^1(K)}.$$
- Nun untersuchen wir $\phi \circ \psi$. Sei $(x_0 : x_1 : x_2) \in C(K)$.
Ist $(x_0 : x_1 : x_2) = (1 : 0 : 0)$, so ergibt sich
$$\phi(\psi((1 : 0 : 0))) = \phi((a_2 : -a_1)) = (1 : 0 : 0).$$
Ist $(x_0 : x_1 : x_2) \neq (1 : 0 : 0)$, so ist
$$\begin{aligned} \phi(\psi((x_0 : x_1 : x_2))) &= \phi((x_1 : x_2)) = \\ &= (a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 : -x_1(a_1x_1 + a_2x_2) : -x_2(a_1x_1 + a_2x_2)) = \\ &= (-a_1x_0x_1 - a_2x_0x_2 : -x_1(a_1x_1 + a_2x_2) : -x_2(a_1x_1 + a_2x_2)) = \\ &= (-x_0(a_1x_1 + a_2x_2) : -x_1(a_1x_1 + a_2x_2) : -x_2(a_1x_1 + a_2x_2)) = \\ &= (x_0 : x_1 : x_2). \end{aligned}$$
Also ist
$$\phi \circ \psi = \mathrm{id}_{C(K)}.$$
Dies beweist schließlich die Bijektivität von ϕ mit der angegebenen Umkehrabbildung. ■

Bemerkung: Im Sinne der Algebraischen Geometrie ist die Abbildung des letztes Satz sogar ein Isomorphismus.

Der vorangegangene Satz gibt eine Parametrisierung der Punkte einer nichtsingulären Quadrik C, die den Punkt $(1:0:0)$ enthält, an. Wir formulieren dies (nochmals) als Folgerung:

FOLGERUNG. *Sei C eine über K durch das Polynom*

$$f = a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

definierte nichtsinguläre ebene projektive Quadrik; sie enthält den Punkt $(1:0:0)$. Definiert man $c_0(u,v), c_1(u,v), c_2(u,v) \in K[u,v]$ durch

$$c_0(u,v) = a_3u^2 + a_4uv + a_5v^2,$$

$$c_1(u,v) = -u(a_1u + a_2v), \quad c_2(u,v) = -v(a_1u + a_2v),$$

so gilt

$$C(K) = \{(c_0(u,v) : c_1(u,v) : c_2(u,v)) : (u:v) \in \mathbb{P}^1(K)\}$$

und für jeden Oberkörper L von K

$$C(L) = \{(c_0(u,v) : c_1(u,v) : c_2(u,v)) : (u:v) \in \mathbb{P}^1(L)\}.$$

Beispiel: Wir betrachten die über $\mathbb{Q}$ durch das Polynom

$$f = x_0x_1 + 2x_0x_2 + 3x_1^2 + 4x_1x_2 + 5x_2^2$$

definierte ebene projektive Quadrik C; sie ist wegen $\det(A_f) = -18$ nichtsingulär. Setzen wir nun - wie in der Folgerung -

$$c_0(u,v) = 3u^2 + 4uv + 5v^2, \quad c_1(u,v) = -u(u+2v), \quad c_2(u,v) = -v(u+2v),$$

so gilt

$$C(\mathbb{Q}) = \{(c_0(u,v) : c_1(u,v) : c_2(u,v)) : (u:v) \in \mathbb{P}^1(\mathbb{Q})\}.$$

Für $(u:v) = (0:1)$ erhält man den Punkt

$$(5:0:-2) = (1:0:-\frac{2}{5}),$$

für $(u:v) = (1:t)$ erhält man den Punkt

$$(3+4t+5t^2 : -(1+2t) : -t(1+2t)) = (1 : -\frac{1+2t}{3+4t+5t^2} : -\frac{t(1+2t)}{3+4t+5t^2}).$$

Zusammengefasst:

$$C(\mathbb{Q}) = \{(1:0:-\frac{2}{5})\} \cup \{(1 : -\frac{1+2t}{3+4t+5t^2} : -\frac{t(1+2t)}{3+4t+5t^2}) : t \in \mathbb{Q}\}.$$

Wir interpretieren dies affin: Die Lösungen $(x,y) \in \mathbb{Q}^2$ der Gleichung

$$x + 2y + 3x^2 + 4xy + 5y^2 = 0$$

sind genau die Punkte der Menge

$$\{(0, -\frac{2}{5})\} \cup \{(-\frac{1+2t}{3+4t+5t^2}, -\frac{t(1+2t)}{3+4t+5t^2}) : t \in \mathbb{Q}\}.$$

Wir haben eben nichtsinguläre projektive ebene Quadriken parametrisiert, die Punkt $(1:0:0)$ enthalten. Was macht man im Allgemeinfall? Koordinatenwechsel.

Parametrisierung einer nichtsingulären ebenen projektiven Quadrik C, wenn man einen Punkt $P \in C(K)$ kennt.

- Sei C gegeben durch ein Polynom $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0,x_1,x_2]$ und $P = (p_0 : p_1 : p_2) \in C(K)$ mit $p_0, p_1, p_2 \in K$.

- Wähle eine Matrix $T \in \mathrm{GL}_3(K)$, deren erste Zeile der Vektor $\begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$ ist, beispielsweise

$$T = \begin{cases} \begin{pmatrix} p_0 & 0 & 0 \\ p_1 & 1 & 0 \\ p_2 & 0 & 1 \end{pmatrix} & \text{im Fall } p_0 \neq 0, \\ \begin{pmatrix} 0 & 1 & 0 \\ p_1 & 0 & 0 \\ p_2 & 0 & 1 \end{pmatrix} & \text{im Fall } p_0 = 0, p_1 \neq 0, \\ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ p_2 & 0 & 0 \end{pmatrix} & \text{im Fall } p_0 = 0, p_1 = 0, p_2 \neq 0. \end{cases}$$

- Führe neue Koordinaten y_0, y_1, y_2 ein durch

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}.$$

  Der Punkt $P = (p_0 : p_1 : p_2)$ hat dann die y-Koordinaten $(y_0 : y_1 : y_2) = (1 : 0 : 0)$. Schreibt man f als Polynom in y, so ergibt wegen sich $P \in C(K)$ die Gestalt

$$f = b_1 y_0 y_1 + b_2 y_0 y_2 + b_3 y_1^2 + b_4 y_1 y_2 + b_5 y_2^2.$$

- Für das Polynom f in y_0, y_1, y_2 können wir eine Parametrisierung angeben:

  $d_0(u,v) = b_3 u^2 + b_4 uv + b_5 v^2, \quad d_1(u,v) = -u(b_1 u + b_2 v), \quad d_2(u,v) = -v(b_1 u + b_2 v).$

  Mit der Matrix T erhalten wir eine Parametrisierung in x-Koordinaten,
  d.h. definieren wir

$$\begin{pmatrix} c_0(u,v) \\ c_1(u,v) \\ c_2(u,v) \end{pmatrix} = T \begin{pmatrix} d_0(u,v) \\ d_1(u,v) \\ d_2(u,v) \end{pmatrix},$$

  so gilt

$$C(K) = \{(c_0(u,v) : c_1(u,v) : c_2(u,v)) : (u,v) \in \mathbb{P}^1(K)\}.$$

Beispiel: Wir betrachten die durch das Polynom $f = x_0^2 - x_1^2 - x_2^2$ definierte Quadrik C (über $\mathbb{Q}$). Sie enthält den Punkt $P = (1 : 1 : 0)$. Wir wählen

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

und den durch $x = Ty$ beschriebenen Koordinatenwechsel:

$$x_0 = y_0, \quad x_1 = y_0 + y_1, \quad x_2 = y_2.$$

Dann wird

$$f = -2y_0 y_1 - y_1^2 - y_2^2.$$

Wir erhalten (mit den Formeln des Satzes) die Parametrisierung

$$(y_0 : y_1 : y_2) = (-u^2 - v^2 : -u(-2u) : -v(-2u)) = (-u^2 - v^2 : 2u^2 : 2uv),$$

in den x-Koordinaten ergibt sich

$$(x_0 : x_1 : x_2) = (y_0 : y_0 + y_1 : y_2) = (-u^2 - v^2 : u^2 - v^2 : 2uv),$$

und damit

$$C(\mathbb{Q}) = \{(-u^2 - v^2 : u^2 - v^2 : 2uv) : (u : v) \in \mathbb{P}^1(\mathbb{Q})\}.$$

Bemerkung: Wir wollen nochmal die geometrische Idee hinter der Abbildung $\psi = \phi^{-1} : C(K) \to \mathbb{P}^1(K)$ beschreiben.

- Gegeben sei also eine nichtsinguläre ebene Quadrik C und ein Punkt $P_0 \in C(K)$.

- Wir wählen eine (über K definierte) Gerade G_0, die den Punkt P_0 nicht enthält.
- Für jeden Punkt $P \in C(K)$ sei

$$G_P = \begin{cases} \text{Gerade durch } P \text{ und } P_0, & \text{im Fall } P \neq P_0, \\ \text{Tangente in } P_0 \text{ an } C, & \text{im Fall } P = P_0. \end{cases}$$

- Für $P \in C(K)$ sei $\psi(P)$ der Schnittpunkt von G_P mit G_0, d.h.

$$\{\psi(P)\} = G_P \cap G_0.$$

  Dann erhält man also eine Abbildung $\psi : C(K) \to G_0(K)$.

Frage: Kann man sehen, ob eine über K definierte nichtsinguläre projektive ebene Quadrik C einen K-rationalen Punkt besitzt? Wie kann man einen solchen finden, wenn er existiert? (Hat man einen Punkt $P \in C(K)$, so kann ganz $C(K)$ durch eine Parametrisierung beschreiben.)

4. Diagonalisierung von Quadriken in Charakteristik $\neq 2$

Satz. *Sei K ein Körper der Charakteristik $\neq 2$ und C eine durch das Polynom*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

definierte Quadrik. Dann gibt es einen Koordinatenwechsel

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} \qquad \textit{mit} \qquad T \in \mathrm{GL}_3(K),$$

sodass dass gilt

$$f = b_0y_0^2 + b_1y_1^2 + b_2y_2^2.$$

Der Beweis ergibt sich aus dem nachfolgenden Verfahren:
Diagonalisierung einer ebenen Quadrik: Wir beginnen mit einer Quadrik

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

und werden sie schrittweise auf Diagonalgestalt bringen. In den Zwischenschritten wird eine Quadrik in x_0, x_1, x_2 eingegeben, zurückgegeben wird eine Quadrik in y_0, y_1, y_2 mit der verwendeten Transformationsmatrix T, sodass gilt

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}.$$

- Das erste Ziel ist, eine Quadrik mit $a_0 \neq 0$ zu haben. Im Folgenden werden alle Möglichkeiten mit $a_0 = 0$ behandelt. Durch eine geeignete Transformation wird dann $a_0 \neq 0$ erreicht:
  - Fall $a_0 = 0$, $a_3 \neq 0$: $f = a_1x_0x_1 + a_2x_0x_1 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ wird mit

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

    zu

$$f = a_3y_0^2 + a_1y_0y_1 + a_4a_0y_2 + a_2y_1y_2 + a_5y_2^2.$$

  - Fall $a_0 = 0$, $a_3 = 0$, $a_5 \neq 0$: $f = a_1x_0x_1 + a_2x_0x_2 + a_4x_1x_2 + a_5x_2^2$ wird mit

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

    zu

$$f = a_5y_0^2 + a_4y_0y_1 + a_2y_0y_2 + a_1y_1y_2.$$

– Fall $a_0 = 0$, $a_3 = 0$, $a_5 = 0$, $a_1 \neq 0$: $f = a_1x_0x_1 + a_2x_0x_2 + a_4x_1x_2$ wird mit

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

zu

$$f = a_1y_0^2 + a_1y_0y_1 + (a_2 + a_4)y_0y_2 + a_4y_1y_2.$$

– Fall $a_0 = 0$, $a_3 = 0$, $a_5 = 0$, $a_1 = 0$, $a_2 \neq 0$: $f = a_2x_0x_2 + a_4x_1x_2$ wird mit

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

zu

$$f = a_2y_0^2 + a_4y_0y_1 + a_2y_0y_2 + a_4y_1y_2.$$

– Fall $a_0 = 0$, $a_3 = 0$, $a_5 = 0$, $a_1 = 0$, $a_2 = 0$, $a_4 \neq 0$:
$f = a_4x_1x_2$ wird mit

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

zu

$$f = a_4y_0^2 + a_4y_0y_1 + a_4y_0y_2 + a_4y_1y_2.$$

– Der Fall $a_0 = 0$, $a_3 = 0$, $a_5 = 0$, $a_1 = 0$, $a_2 = 0$, $a_4 = 0$ kann nicht auftreten, da sonst f identisch 0 wäre, was nicht sein darf.

Wir haben nun erreicht, dass wir $a_0 \neq 0$ und $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ annehmen können.

- Ist $a_1 \neq 0$ (und $a_0 \neq 0$), so führt

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{a_1}{2a_0} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

zu

$$f = a_0y_0^2 + a_2y_0y_2 + (a_3 - \frac{a_1^2}{4a_0})y_1^2 + (a_4 - \frac{a_1a_2}{2a_0})y_1y_2 + a_5y_2^2.$$

Nach Umbenennung der Koeffizienten können wir also

$$f = a_0x_0^2 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

annehmen.

- Ist $a_2 \neq 0$ (und $a_0 \neq 0$, $a_1 = 0$), so führt die Transformation

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -\frac{a_2}{2a_0} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

zu

$$f = a_0y_0^2 + a_3y_1^2 + a_4y_1y_2 + (a_5 - \frac{a_2^2}{4a_0})y_2^2.$$

Nach Umbenennung der Koeffizienten können wir daher

$$f = a_0x_0^2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

annehmen.

- Falls $a_3 = 0$ (und $f = a_0x_0^2 + a_4x_1x_2 + a_5x_2^2$) ist, so versuchen wir, durch eine geeignete Transformation $a_3 \neq 0$ zu erreichen:

– Fall $a_0 \neq 0$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_5 \neq 0$: Die Transformation

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

führt zu

$$f = a_0 y_0^2 + a_5 y_1^2 + a_4 y_1 y_2.$$

– Fall $a_0 \neq 0$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_5 = 0$, $a_4 \neq 0$: Die Transformation

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

führt zu

$$f = a_0 y_0^2 + a_4 y_1^2 + a_4 y_1 y_2.$$

– Fall $a_0 \neq 0$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_5 = 0$, $a_4 = 0$: Hier ist $f = a_0 x_0^2$ und wir sind fertig; wir beenden das Verfahren.

Sind wir soweit gekommen, können wir $a_0 \neq 0$, $a_1 = 0$, $a_2 = 0$, $a_3 \neq 0$ und $f = a_0 x_0^2 + a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2$ annehmen.

- Fall $a_0 \neq 0$, $a_1 = 0$, $a_2 = 0$, $a_3 \neq 0$, $a_4 \neq 0$: Die Transformation

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{a_4}{2a_3} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

führt zu

$$f = a_0 y_0^2 + a_3 y_1^2 + (a_5 - \frac{a_4^2}{4a_3}) y_2^2.$$

Damit haben wir unser Ziel erreicht. Nachfolgend gibt es noch eine etwas algorithmischere Version:

Verfahren zum Diagonalisieren einer ebene Quadrik:

Eingabe: Quadrik
Ausgabe: Diagonalisierte Quadrik und Transformationsmatrix

$(a_0, a_1, a_2, a_3, a_4, a_5)$, $T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
if $a_0 = 0$ **then**
  if $a_3 \neq 0$ **then**
    $T \leftarrow T \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_3, a_1, a_4, 0, a_2, a_5)$ ▷ Vertausche x_0 und x_1.
  else if $a_5 \neq 0$ **then**
    $T \leftarrow T \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_5, a_4, a_2, 0, a_1, 0)$ ▷ Vertausche x_0 und x_2.
  else if $a_1 \neq 0$ **then**
    $T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_1, a_1, a_2 + a_4, 0, a_4, 0)$
  else if $a_2 \neq 0$ **then**
    $T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_2, a_4, a_2, 0, a_4, 0)$
  else if $a_4 \neq 0$ **then**
    $T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_4, a_4, a_4, 0, a_4, 0)$
  else
    return Fehler: $(a_0, a_1, a_2, a_3, a_4, a_5) = (0, 0, 0, 0, 0, 0)$
  end if
end if
▷ Nun ist $a_0 \neq 0$.
if $a_1 \neq 0$ **then**
  $T \leftarrow T \begin{pmatrix} 1 & -\frac{a_1}{2a_0} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, a_2, a_3 - \frac{a_1^2}{4a_0}, a_4 - \frac{a_1 a_2}{2a_0}, a_5)$ ▷ Quadratische Ergänzung
end if
if $a_2 \neq 0$ **then**

22: $T \leftarrow T \begin{pmatrix} 1 & 0 & -\frac{a_2}{2a_0} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_3, a_4, a_5 - \frac{a_2^2}{4a_0})$
23: Quadratische Ergänzung
24: **end if**
25: ▷ Nun ist $a_0 \neq 0$, $a_1 = a_2 = 0$. $a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ muss noch bearbeitet werden.
26: **if** $a_3 = 0$ **then** ▷ $f = a_0x_0^2 + a_4x_1x_2 + a_5x_2^2$. Was macht man nun?
27: **if** $a_5 \neq 0$ **then**
28: $T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_5, a_4, 0)$ ▷ Vertausche x_1 und x_2.
29: **else if** $a_4 \neq 0$ **then**
30: $T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_4, a_4, 0)$
31: **else**
32: **return** $(a_0, 0, 0, 0, 0, 0)$,T ▷ $f = a_0x_0^2$
33: **end if**
34: **end if**
35: ▷ Nun ist $f = a_0x_0^2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ mit $a_0, a_3 \neq 0$.
36: **if** $a_4 \neq 0$ **then**
37: $T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{a_4}{2a_3} \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_3, 0, a_5 - \frac{a_4^2}{4a_3})$
38: **end if**
39: **return** $(a_0, a_1, a_2, a_3, a_4, a_5)$,$T$ ▷ Fertig!

Beispiele:

- Wir betrachten die Quadrik

$$f = x_0^2 + 2x_0x_1 + 3x_0x_2 + 4x_1^2 + 5x_1x_2 + 6x_2^2.$$

Wir machen quadratische Ergänzung:

$$\begin{aligned} f &= x_0^2 + 2x_0x_1 + 3x_0x_2 + 4x_1^2 + 5x_1x_2 + 6x_2^2 = \\ &= (x_0 + x_1 + \frac{3}{2}x_2)^2 - (x_1^2 + 3x_1x_2 + \frac{9}{4}x_2^2) + 4x_1^2 + 5x_1x_2 + 6x_2^2 = \\ &= (x_0 + x_1 + \frac{3}{2}x_2)^2 + 3x_1^2 + 2x_1x_2 + \frac{15}{4}x_2^2 = \\ &= (x_0 + x_1 + \frac{3}{2}x_2)^2 + 3\left(x_1^2 + \frac{2}{3}x_1x_2\right) + \frac{15}{4}x_2^2 = \\ &= (x_0 + x_1 + \frac{3}{2}x_2)^2 + 3(x_1 + \frac{1}{3}x_2)^2 - \frac{1}{3}x_2^2 + \frac{15}{4}x_2^2 = \\ &= (x_0 + x_1 + \frac{3}{2}x_2)^2 + 3(x_1 + \frac{1}{3}x_2)^2 + \frac{41}{12}x_2^2. \end{aligned}$$

Setzen wir

$$y_0 = x_0 + x_1 + \frac{3}{2}x_2, \quad y_1 = x_1 + \frac{1}{3}x_2, \quad y_2 = x_2,$$

so wird also

$$f = y_0^2 + 3y_1^2 + \frac{41}{12}y_2^2.$$

Es gilt

$$\begin{aligned} x_2 &= y_2, \\ x_1 &= y_1 - \frac{1}{3}x_2 = y_1 - \frac{1}{3}y_2, \\ x_0 &= y_0 - x_1 - \frac{3}{2}x_2 = y_0 - (y_1 - \frac{1}{3}y_2) - \frac{3}{2}y_2 = y_0 - y_1 - \frac{7}{6}y_2, \end{aligned}$$

also

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -\frac{7}{6} \\ 0 & 1 & -\frac{1}{3} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}.$$

- Für die Quadrik

$$f = 431x_0^2 + 865x_0x_1 + 216x_0x_2 + 431x_1^2 + 216x_1x_2 + 36x_2^2$$

erhalten wir mit der Transformation

$$x_0 = y_0 - \frac{865}{862}y_1 - \frac{216}{1727}y_2, \quad x_1 = y_1 - \frac{216}{1727}y_2, \quad x_2 = y_2$$

die Gestalt

$$f = 431y_0^2 - \frac{5181}{1724}y_1^2 + \frac{15516}{1727}y_2^2.$$

Beispiel: Gegeben sei eine Quadrik C durch das Polynom

$$f = x_0x_1 + 3x_0x_2 - 5x_1x_2 \in \mathbb{Q}[x_0, x_1, x_2].$$

Die Quadrik soll diagonalisiert werden, d.h. wir suchen einen Koordinatenwechsel, sodass f in neuen Koordinaten y_0, y_1, y_2 die Gestalt

$$f = b_0y_0^2 + b_1y_1^2 + b_2y_2^2$$

hat.
Wir gehen schrittweise vor. Dabei führen wir jedesmal neue Koordinaten ein, die einem projektiven Koordinatenwechsel entsprechen. Die Bezeichnung für die jeweils „neuen“ Koordinaten ist ziemlich willkürlich.

- Da kein Term x_0^2 in f vorkommt, führen wir neue Koordinaten z_0, z_1, z_2 ein durch

  $$x_0 = z_0, \quad x_1 = z_0 + z_1, \quad x_2 = z_2.$$

  Dann wird

  $$\begin{aligned} f &= x_0x_1 + 3x_0x_2 - 5x_1x_2 = z_0(z_0 + z_1) + 3z_0z_2 - 5(z_0 + z_1)z_2 = \\ &= z_0^2 + z_0z_1 - 2z_0z_2 - 5z_1z_2. \end{aligned}$$

- Da in f nun ein Term z_0^2 vorkommt, können wir mit quadratischer Ergänzung die Terme z_0z_1 und $-2z_0z_2$ „entfernen“:

  $$\begin{aligned} f &= z_0^2 + z_0z_1 - 2z_0z_2 - 5z_1z_2 = \\ &= \left(z_0 + \frac{1}{2}z_1 - z_2\right)^2 - \frac{1}{4}z_1^2 - z_2^2 + z_1z_2 - 5z_1z_2 = \\ &= \left(z_0 + \frac{1}{2}z_1 - z_2\right)^2 - \frac{1}{4}z_1^2 - 4z_1z_2 - z_2^2. \end{aligned}$$

  Wir führen jetzt neue Variable u_0, u_1, u_2 durch

  $$u_0 = z_0 + \frac{1}{2}z_1 - z_2, \quad u_1 = z_1, \quad u_2 = z_2.$$

  Dann wird

  $$f = u_0^2 - \frac{1}{4}u_1^2 - 4u_1u_2 - u_2^2.$$

  Wir können z_0, z_1, z_2 auch in Abhängigkeit von u_0, u_1, u_2 schreiben:

  $$\begin{aligned} z_0 &= u_0 - \frac{1}{2}z_1 + z_2 = u_0 - \frac{1}{2}u_1 + u_2, \\ z_1 &= u_1, \\ z_2 &= u_2. \end{aligned}$$

- Wir machen wieder quadratische Ergänzung:

  $$\begin{aligned} f &= u_0^2 - \frac{1}{4}u_1^2 - 4u_1u_2 - u_2^2 = \\ &= u_0^2 - \frac{1}{4}\left(u_1^2 + 16u_1u_2\right) - u_2^2 = \\ &= u_0^2 - \frac{1}{4}\left((u_1 + 8u_2)^2 - 64u_2^2\right) - u_2^2 = \\ &= u_0^2 - \frac{1}{4}(u_1 + 8u_2)^2 + 16u_2^2 - u_2^2 = \\ &= u_0^2 - \frac{1}{4}(u_1 + 8u_2)^2 + 15u_2^2. \end{aligned}$$

Wir führen neue Variable y_0, y_1, y_2 ein durch

$$y_0 = u_0, \quad y_1 = u_1 + 8u_2, \quad y_2 = u_2.$$

Dann wird

$$f = y_0^2 - \frac{1}{4}y_1^2 + 15y_2^2,$$

wie sind also am Ziel. Wir schreiben noch u_0, u_1, u_2 in Abhängigkeit von y_0, y_1, y_2:

$$\begin{aligned} u_0 &= y_0, \\ u_1 &= y_1 - 8u_2 = y_1 - 8y_2, \\ u_2 &= y_2. \end{aligned}$$

- Wir wollen noch sehen, wie man von x_0, x_1, x_2 zu y_0, y_1, y_2 kommt, und benutzen dazu die zuvor angegebenen Beziehungen:

$$\begin{aligned} x_0 &= z_0 = u_0 - \frac{1}{2}u_1 + u_2 = y_0 - \frac{1}{2}(y_1 - 8y_2) + y_2 = y_0 - \frac{1}{2}y_1 + 5y_2, \\ x_1 &= z_0 + z_1 = u_0 - \frac{1}{2}u_1 + u_2 + u_1 = u_0 + \frac{1}{2}u_1 + u_2 = y_0 + \frac{1}{2}(y_1 - 8y_2) + y_2 = \\ &= y_0 + \frac{1}{2}y_1 - 3y_2, \\ x_2 &= z_2 = u_2 = y_2. \end{aligned}$$

  Zusammengefasst:

$$\begin{aligned} x_0 &= y_0 - \frac{1}{2}y_1 + 5y_2, \\ x_1 &= y_0 + \frac{1}{2}y_1 - 3y_2, \\ x_2 &= y_2. \end{aligned}$$

- Ergebnis: Führen wir neue Koordinaten y_0, y_1, y_2 ein durch

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} & 5 \\ 1 & \frac{1}{2} & -3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix},$$

  so hat f in den neuen Koordinaten folgende Gestalt:

$$f = y_0^2 - \frac{1}{4}y_1^2 + 15y_2^2.$$

  (Wenn man will, kann man noch bemerken, dass die „Übergangsmatrix“ von x_0, x_1, x_2 zu y_0, y_1, y_2 eine von 0 verschiedene Determinante hat, dass es sich also um einen projektiven Koordinatenwechsel handelt.)

Bemerkung: Zu dem beschriebenen Diagonalisierungsverfahren lässt sich leicht eine SAGE-Funktion schreiben. Für `a012345` muss man das Koeffiziententupel $(a_0, a_1, a_2, a_4, a_5)$ eingeben, für K den zugrundeliegenden Körper K.

```
def diagonalisiere(a012345,K):
  a0,a1,a2,a3,a4,a5=a012345
  a0,a1,a2,a3,a4,a5=K(a0),K(a1),K(a2),K(a3),K(a4),K(a5)
  T=Matrix(K,[[1,0,0],[0,1,0],[0,0,1]])
  if a0==0:
    if a3!=0:
      T=T*Matrix([[0,1,0],[1,0,0],[0,0,1]])
      a0,a1,a2,a3,a4,a5=a3,a1,a4,0,a2,a5
    elif a5!=0:
      T=T*Matrix([[0,0,1],[0,1,0],[1,0,0]])
      a0,a1,a2,a3,a4,a5=a5,a4,a2,0,a1,0
    elif a1!=0:
      T=T*Matrix([[1,0,0],[1,1,0],[0,0,1]])
      a0,a1,a2,a3,a4,a5=a1,a1,a2+a4,0,a4,0
```

```
    elif a2!=0:
      T=T*Matrix([[1,0,0],[0,1,0],[1,0,1]])
      a0,a1,a2,a3,a4,a5=a2,a4,a2,0,a4,0
    elif a4!=0:
      T=T*Matrix([[1,0,0],[1,1,0],[1,0,1]])
      a0,a1,a2,a3,a4,a5=a4,a4,a4,0,a4,0
    else:
      return False
  if a1!=0:
    T=T*Matrix([[1,-a1/(2*a0),0],[0,1,0],[0,0,1]])
    a0,a1,a2,a3,a4,a5=a0,0,a2,a3-a1^2/(4*a0),a4-a1*a2/(2*a0),a5
  if a2!=0:
    T=T*Matrix([[1,0,-a2/(2*a0)],[0,1,0],[0,0,1]])
    a0,a1,a2,a3,a4,a5=a0,0,0,a3,a4,a5-a2^2/(4*a0)
  if a3==0:
    if a5!=0:
      T=T*Matrix([[1,0,0],[0,0,1],[0,1,0]])
      a0,a1,a2,a3,a4,a5=a0,0,0,a5,a4,0
    elif a4!=0:
      T=T*Matrix([[1,0,0],[0,1,0],[0,1,1]])
      a0,a1,a2,a3,a4,a5=a0,0,0,a4,a4,0
    else:
      return (a0,a1,a2,a3,a4,a5),T
  if a4!=0:
    T=T*Matrix([[1,0,0],[0,1,-a4/(2*a3)],[0,0,1]])
    a0,a1,a2,a3,a4,a5=a0,0,0,a3,0,a5-a4^2/(4*a3)
  return (a0,a1,a2,a3,a4,a5),T
```

5. Wann besitzen reelle Quadriken ℝ-rationale Punkte?

Gegeben sei eine über $\mathbb{R}$ definierte projektive ebene Quadrik C durch ein Polynom

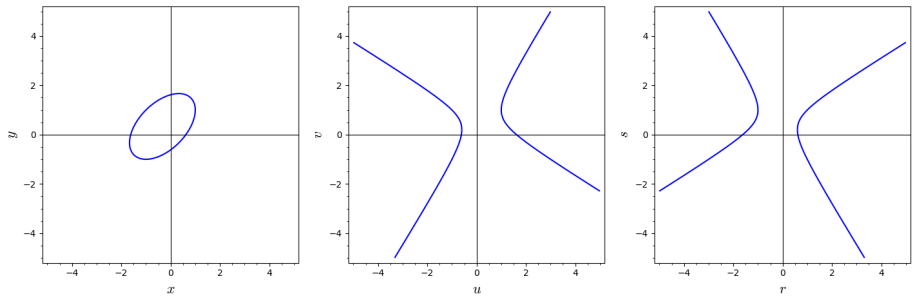
$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in \mathbb{R}[x_0, x_1, x_2].$$

Frage: Kann man an Hand der Koeffizienten $a_0, \ldots, a_5$ entscheiden, ob die Kurve $\mathbb{R}$-rationale Punkte besitzt, d.h. ob man die Kurve reell zeichnen kann?
Wir fragen also, ob die Kurve in den affinen Teilen U_0, U_1, U_2 reell sichtbar ist, d.h. ob die Mengen

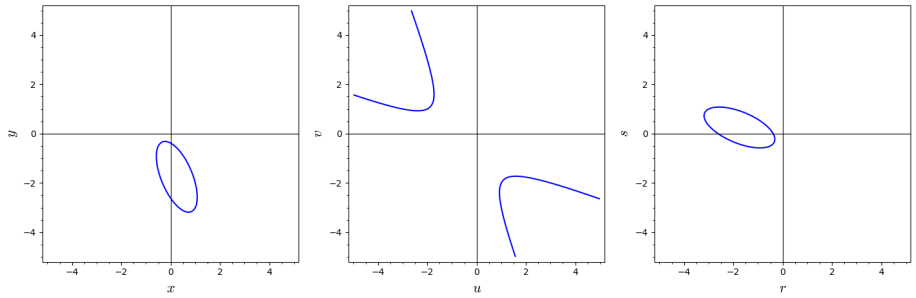
$$\{(x,y) \in \mathbb{R}^2 : f(1,x,y) = 0\},$$
$$\{(u,v) \in \mathbb{R}^2 : f(u,1,v) = 0\},$$
$$\{(r,s) \in \mathbb{R}^2 : f(r,s,1) = 0\}$$

nicht leer sind.
Beispiele: Wir betrachten verschiedene homogene quadratische Polynome $f(x_0, x_1, x_2) \in \mathbb{R}[x_0, x_1, x_2]$ und versuchen, die zugehörigen Quadriken in den affinen Teilen U_0, U_1, U_2 zu zeichnen - wie eben beschrieben.

- $f = x_0^2 - x_0x_1 + x_0x_2 - x_1^2 + x_1x_2 - x_2^2$:



- $f = x_0^2 + 2x_0x_1 + 3x_0x_2 + 3x_1^2 + 2x_1x_2 + x_2^2$:



- $f = 2x_0^2 + 2x_0x_1 - x_0x_2 + 2x_1^2 - x_1x_2 + x_2^2$: Hier ist reell nichts zu sehen.

Ein quadratisches Polynom $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in \mathbb{R}[x_0, x_1, x_2] \setminus \{0\}$ liefert auch eine quadratische Form $\mathbb{R}^3 \to \mathbb{R}$

$$f(x) = x^tAx \text{ mit } A = \begin{pmatrix} a_0 & \frac{1}{2}a_1 & \frac{1}{2}a_2 \\ \frac{1}{2}a_1 & a_3 & \frac{1}{2}a_4 \\ \frac{1}{2}a_2 & \frac{1}{2}a_4 & a_5 \end{pmatrix} \text{ und } x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Die quadratische Form f heißt **positiv definit**, falls

$$f(x) > 0 \text{ für alle } x \in \mathbb{R}^3 \setminus \{0\}$$

gilt, sie heißt **negativ definit**, falls

$$f(x) < 0 \text{ für alle } x \in \mathbb{R}^3 \setminus \{0\}$$

gilt. Mit diesen Bezeichnungen gilt:

LEMMA. *Das homogene quadratische Polynom* $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in \mathbb{R}[x_0, x_1, x_2] \setminus \{0\}$ *definiere die projektive ebene Quadrik* C *über* $\mathbb{R}$. *Dann gilt:*

$$C(\mathbb{R}) = \emptyset \quad \Longleftrightarrow \quad f \text{ ist positiv definit oder negativ definit.}$$

Beweis: Wir können einen Koordinatenwechsel machen, sodass

$$f = b_0y_0^2 + b_1y_1^2 + b_2y_2^2$$

gilt. Wir unterscheiden verschiedene Fälle:

- **Fall** $b_i = 0$ **für ein** i**:** O.E. können wir $b_0 = 0$ annehmen. Dann ist f weder positiv noch negativ definit, da $f(1, 0, 0) = 0$ ist. Außerdem gilt $(1 : 0 : 0) \in C(\mathbb{R})$.
- **Fall** $b_0 > 0, b_1 > 0, b_2 > 0$**:** Dann ist f positiv definit wegen $f(x_0, x_1, x_2) > 0$ für alle $(x_0, x_1, x_2) \in \mathbb{R}^3 \setminus \{0\}$. Damit gilt auch $C(\mathbb{R}) = \emptyset$.
- **Fall** $b_0 < 0, b_1 < 0, b_2 < 0$**:** Dann ist f negativ definit wegen $f(x_0, x_1, x_2) < 0$ für alle $(x_0, x_1, x_2) \in \mathbb{R}^3 \setminus \{0\}$. Natürlich gilt auch $C(\mathbb{R}) = \emptyset$.
- **Fall Es gibt** i, j, k **mit** $\{i, j, k\} = \{0, 1, 2\}$ **und** $b_i > 0$**,** $b_j < 0$**,** $b_k \neq 0$**:** Der einfacheren Schreibweise halber nehmen wir wieder $b_0 > 0$ und $b_1 < 0$ an. Dann gilt $f(\sqrt{|b_1|}, \sqrt{b_0}, 0) = 0$, f ist also weder positiv noch negativ definit. Außerdem gilt $(\sqrt{|b_1|} : \sqrt{b_0} : 0) \in C(\mathbb{R})$.

Dies zeigt die Aussage des Lemmas. ■

SATZ. *Sei C eine projektive ebene Quadrik über $\mathbb{R}$, definiert durch das Polynom*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2.$$

Dann gilt:

$$C(\mathbb{R}) \neq \emptyset \quad \Longleftrightarrow \quad \begin{cases} 4a_0a_3 - a_1^2 \leq 0 \\ \text{oder} \\ a_0(4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_3a_2^2 - a_5a_1^2) \leq 0. \end{cases}$$

Beweis:

- Wir schreiben f als quadratische Form:

$$f = \begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} \begin{pmatrix} a_0 & \frac{1}{2}a_1 & \frac{1}{2}a_2 \\ \frac{1}{2}a_1 & a_3 & \frac{1}{2}a_4 \\ \frac{1}{2}a_2 & \frac{1}{2}a_4 & a_5 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

  Die Hauptminoren der darstellenden Matrix sind

$$\begin{aligned} \begin{vmatrix} a_0 \end{vmatrix} &= a_0, \\ \begin{vmatrix} a_0 & \frac{1}{2}a_1 \\ \frac{1}{2}a_1 & a_3 \end{vmatrix} &= a_0a_3 - \frac{1}{4}a_1^2 = \frac{1}{4} \cdot \left(4a_0a_3 - a_1^2\right), \\ \begin{vmatrix} a_0 & \frac{1}{2}a_1 & \frac{1}{2}a_2 \\ \frac{1}{2}a_1 & a_3 & \frac{1}{2}a_4 \\ \frac{1}{2}a_2 & \frac{1}{2}a_4 & a_5 \end{vmatrix} &= \frac{1}{4} \cdot \left(4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_3a_2^2 - a_5a_1^2\right). \end{aligned}$$

  Definieren wir

$$d_1 = a_0, \quad d_2 = 4a_0a_3 - a_1^2, \quad d_3 = 4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_3a_2^2 - a_5a_1^2,$$

  so sind die Hauptminoren also

$$d_1, \quad \frac{1}{4}\,d_2, \quad \frac{1}{4}\,d_3.$$

  Das Hauptminorenkriterium für Definitheit lautet:

$$f \text{ ist positiv definit} \quad \Longleftrightarrow \quad d_1 > 0 \quad \text{und} \quad d_2 > 0 \quad \text{und} \quad d_3 > 0.$$

  Das Hauptminorenkriterium für Definitheit kann man nachlesen bei *G. Fischer. Lineare Algebra. 18. Auflage. Springer Spektrum, 2014* auf Seite 327.

- Nun gilt:

$$f \text{ ist positiv definit} \quad \Longleftrightarrow \quad d_1 > 0, \quad d_2 > 0, \quad d_3 > 0$$

  und

$$f \text{ ist negativ definit} \quad \Longleftrightarrow \quad -f \text{ ist positiv definit} \quad \Longleftrightarrow \quad d_1 < 0, \quad d_2 > 0, \quad d_3 < 0.$$

  Mit dem vorangegangenen Lemma folgt

$$\begin{aligned} C(\mathbb{R}) = \emptyset \quad &\Longleftrightarrow \quad f \text{ ist positiv definit oder } f \text{ ist negativ definit} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad (d_1 > 0, d_2 > 0, d_3 > 0) \quad \text{oder} \quad (d_1 < 0, d_2 > 0, d_3 < 0). \end{aligned}$$

  Da nun aber gilt:

$$d_1d_3 > 0 \quad \Longleftrightarrow \quad (d_1 > 0, d_3 > 0) \quad \text{oder} \quad (d_1 < 0, d_3 < 0)$$

  können wir weiter schreiben

$$C(\mathbb{R}) = \emptyset \quad \Longleftrightarrow \quad d_1d_3 > 0 \text{ und } d_2 > 0.$$

  Die Negation liefert

$$C(\mathbb{R}) \neq \emptyset \quad \Longleftrightarrow \quad d_1d_3 \leq 0 \text{ oder } d_2 \leq 0.$$

  Dies beweist die Behauptung. ■

Mit

$$d_1 = a_0, \quad d_2 = 4a_0a_3 - a_1^2, \quad d_3 = 4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_3a_2^2 - a_5a_1^2$$

gilt das Kriterium

$$C(\mathbb{R}) \neq \emptyset \quad \Longleftrightarrow \quad d_1d_3 \leq 0 \text{ oder } d_2 \leq 0.$$

Beispiele:

$(a_0, a_1, a_2, a_3, a_4, a_5)$	(d_1, d_2, d_3)	$C(\mathbb{R}) \neq \emptyset$
$(1, -1, 1, -1, 1, -1)$	$(1, -5, 4)$	ja
$(1, 2, 3, 3, 2, 1)$	$(1, 8, -11)$	ja
$(2, 2, -1, 2, -1, 2)$	$(2, 12, 22)$	nein
$(0, 0, 0, 1, 0, -1)$	$(0, 0, 0)$	ja
$(0, 0, 0, 1, 0, 1)$	$(0, 0, 0)$	ja

(Im singulären Fall ($d_3 = 0$) unterscheidet das Kriterium nicht, ob $C(\mathbb{R})$ nur aus einem Punkt besteht oder unendlich viele Punkte enthält.)

6. Ebene projektive Quadriken über $\mathbb{F}_p$

Wir beginnen mit ein paar Bemerkungen zu Charakteristik p und endlichen Körpern.

Lemma. *Ist p eine Primzahl und R ein kommutativer Ring (mit Eins) mit*

$$p \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{p\text{-mal}} = 0 \text{ in } R,$$

so gilt

$$(a + b)^p = a^p + b^p \text{ für alle } a, b \in R.$$

Beweis: Für $1 \leq i \leq p - 1$ ist

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \cdots \cdot (p-(i-1))}{i!}.$$

Da p eine Primzahl ist, kürzt sich p im Zähler nicht heraus, sodass $\binom{p}{i}$ ein Vielfaches von p ist. Damit gilt

$$\binom{p}{i} = 0 \text{ in } R.$$

Der binomische Lehrsatz wird in R damit zu

$$(a + b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}b^i + b^p = a^p + b^p,$$

wie behauptet. ■

Satz (Kleiner Satz von Fermat). *Für eine Primzahl p gilt*

$$a^p = a \text{ für alle } a \in \mathbb{F}_p$$

und

$$a^{p-1} = 1 \text{ für alle } a \in \mathbb{F}_p^*.$$

Beweis: In $\mathbb{F}_p$ erhält man mit der Formel $(a + b)^p = a^p + b^p$ induktiv

$$\begin{aligned}
0^p &= 0, \\
1^p &= 1, \\
2^p &= (1+1)^p = 1^p + 1^p = 1 + 1 = 2, \\
3^p &= (2+1)^p = 2^p + 1^p = 2 + 1 = 3, \\
&\vdots \\
(p-1)^p &= ((p-2)+1)^p = (p-2)^p + 1^p = (p-2) + 1 = p - 1.
\end{aligned}$$

Zusammengefasst: $a^p = a$ für alle $a \in \mathbb{F}_p$. Ist nun $a \neq 0$, so folgt aus $0 = a^p - a = a(a^{p-1} - 1)$ wegen $a \neq 0$ und der Tatsache, dass $\mathbb{F}_p$ ein Körper ist

$$a^{p-1} = 1,$$

wie behauptet. ■

Steht im Folgenden die Potenz a^0, so soll dies immer 1 sein.

LEMMA. *Für $0 \leq e \leq p-2$ gilt*

$$\sum_{u \in \mathbb{F}_p} u^e = 0.$$

Beweis:

- **Fall $e = 0$:** Hier ist
$$\sum_{u \in \mathbb{F}_p} u^0 = \sum_{u \in \mathbb{F}_p} 1 = p \cdot 1 = 0.$$
- **Fall $1 \leq e \leq p-2$:** Da das Polynom $f(x) = x^e - 1 \in \mathbb{F}_p[x]$ höchstens e Nullstellen besitzt, gibt es wegen $e \leq p-2$ in $v \in \mathbb{F}_p^*$ mit $f(v) \neq 0$, d.h.
$$v^e \neq 1.$$
Mit u durchläuft auch uv ganz $\mathbb{F}_p$, also folgt
$$\sum_{u \in \mathbb{F}_p} u^e = \sum_{u \in \mathbb{F}_p} (uv)^e = v^e \sum_{u \in \mathbb{F}_p} u^e,$$
und damit
$$(v^e - 1) \cdot \sum_{u \in \mathbb{F}_p} u^e = 0.$$
Wegen $v^e \neq 1$ folgt
$$\sum_{u \in \mathbb{F}_p} u^e = 0,$$
wie behauptet. ■

SATZ. *Sei p eine Primzahl und $f(x_0, x_1, x_2) \in \mathbb{F}_p[x_0, x_1, x_2] \setminus \{0\}$ homogen vom Grad 2. Dann gibt es einen Punkt $(u_0, u_1, u_2) \in \mathbb{F}_p^3 \setminus \{(0,0,0)\}$ mit*

$$f(u_0, u_1, u_2) = 0.$$

Anders ausgedrückt: Die durch $f = 0$ definierte projektive ebene Quadrik hat mindestens einen $\mathbb{F}_p$-rationalen Punkt.

Beweis: Wir bilden

$$f(x_0, x_1, x_2)^{p-1} = \sum_{e_0+e_1+e_2=2(p-1)} a_{e_0,e_1,e_2} x_0^{e_0} x_1^{e_1} x_2^{e_2}.$$

Es folgt

$$\begin{aligned}
\sum_{(u_0,u_1,u_2) \in \mathbb{F}_p^3} f(u_0, u_1, u_2)^{p-1} &= \sum_{(u_0,u_1,u_2) \in \mathbb{F}_p^3} \sum_{e_0+e_1+e_2=2(p-1)} a_{e_0,e_1,e_2} u_0^{e_0} u_1^{e_1} u_2^{e_2} = \\
&= \sum_{u_0 \in \mathbb{F}_p} \sum_{u_1 \in \mathbb{F}_p} \sum_{u_2 \in \mathbb{F}_p} \sum_{e_0+e_1+e_2=2(p-1)} a_{e_0,e_1,e_2} u_0^{e_0} u_1^{e_1} u_2^{e_2} = \\
&= \sum_{e_0+e_1+e_2=2(p-1)} a_{e_0,e_1,e_2} \left(\sum_{u_0 \in \mathbb{F}_p} u_0^{e_0} \right) \left(\sum_{u_1 \in \mathbb{F}_p} u_1^{e_1} \right) \left(\sum_{u_2 \in \mathbb{F}_p} u_2^{e_2} \right).
\end{aligned}$$

Wegen $e_0 + e_1 + e_2 = 2(p-1)$ gibt es dabei immer ein e_i mit $e_i \leq p-2$.

Nach dem letzten Lemma ist $\sum_{u_i \in \mathbb{F}_p} u_i^{e_i} = 0$, also ist die gesamte Summe 0:

$$\sum_{(u_0,u_1,u_2)\in\mathbb{F}_p^3} f(u_0,u_1,u_2)^{p-1} = 0.$$

Wäre $f(u_0,u_1,u_2) \neq 0$ für alle $(u_0,u_1,u_2) \neq (0,0,0)$, so wäre $f(u_0,u_1,u_2)^{p-1} = 1$ für alle $(u_0,u_1,u_2) \neq (0,0,0)$. Es würde folgen (wegen $f(0,0,0) = 0$)

$$\sum_{(u_0,u_1,u_2)\in\mathbb{F}_p^3} f(u_0,u_1,u_2)^{p-1} = p^3 - 1 = -1 \neq 0,$$

ein Widerspruch zu der vorangegangenen Gleichung. Also gibt es ein $(u_0,u_1,u_2) \in \mathbb{F}_p^3 \setminus \{(0,0,0)\}$ mit $f(u_0,u_1,u_2) = 0$. Dies war zu zeigen. ■

Der folgende Satz fasst die Möglichkeiten für $\#C(\mathbb{F}_p)$ zusammen:

SATZ. *Ist C eine über $\mathbb{F}_p$ definierte ebene projektive Quadrik, so gilt*

$$\#C(\mathbb{F}_p) \in \{1, p+1, 2p+1\}.$$

Genauer:

- *Ist C nichtsingulär, so ist $\#C(\mathbb{F}_p) = p+1$.*
- *Ist C singulär mit genau einer Singularität, so ist C reduzibel über $\overline{\mathbb{F}}_p$.*
  - *Ist C reduzibel über $\mathbb{F}_p$, so gilt $\#C(\mathbb{F}_p) = 2p+1$.*
  - *Ist C irreduzibel über $\mathbb{F}_p$, so gilt $\#C(\mathbb{F}_p) = 1$.*
- *Hat C mehr als eine Singularität, so gilt $\#C(\mathbb{F}_p) = p+1$.*

Beweis: Wir wissen aus den vorangegangenen Überlegungen, dass $\#C(\mathbb{F}_p) \geq 1$ gilt.

- Sei C nichtsingulär. Da C einen $\mathbb{F}_p$ rationalen Punkt besitzt, lässt sich C parametrisieren, es gibt eine Bijektion

  $$C(\mathbb{F}_p) \simeq \mathbb{P}^1(\mathbb{F}_p).$$

  Insbesondere gilt $\#C(\mathbb{F}_p) = \#\mathbb{P}^1(\mathbb{F}_p) = p+1$.
- Ist C singulär mit genau einer Singularität P, so ist $P \in \mathbb{P}^2(\mathbb{F}_p)$. O.E. $P = (1:0:0)$, $f = (b_1x_1+b_2x_2)(c_1x_1+c_2x_2)$. Ist $b_1x_1+b_2x_2 = 0$ nicht über $\mathbb{F}_p$ definiert, so gibt es genau einen Punkt in $C(\mathbb{F}_p)$, nämlich P. Ist $b_1x_1 + b_2x_2 \in \mathbb{F}_p[x_0,x_1,x_2]$, so auch $c_1x_1 + c_2x_2 \in \mathbb{F}_p[x_0,x_1,x_2]$ und

  $$C(\mathbb{F}_p) = \{g = 0\} \cup \{h = 0\}$$

  und $\#C(\mathbb{F}_p) = (p+1) + (p+1) - 1 = 2p+1$.
- Ist C singulär mit mehreren Singularitäten, so gilt $f = c(b_0x_0 + b_1x_1 + b_2x_2)^2$. O.E. $b_0 \neq 0$ und damit o.E. $b_0 = 1$. Dann sind $b_i, c \in \mathbb{F}_p$ und $\#C(\mathbb{F}_p) = p+1$.

Beispiel: Wir betrachten alle über $\mathbb{F}_2$ definierten ebenen projektiven Quadriken C. Sie stehen in Bijektion zu den Polynomen

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

mit $(a_0,a_1,a_2,a_3,a_4,a_5) \in \mathbb{F}_2^6 \setminus \{0\}$. Im Fall $d = 0$ ist die Kurve singulär, im Fall $d = 1$ nichtsingulär.

d	$\#C(\mathbb{F}_2)$	f
0	1	$x_0^2 + x_0x_1 + x_1^2$
0	1	$x_0^2 + x_0x_1 + x_1^2 + x_0x_2 + x_1x_2 + x_2^2$
0	1	$x_0^2 + x_0x_1 + x_1^2 + x_0x_2 + x_2^2$
0	1	$x_0^2 + x_0x_1 + x_1^2 + x_1x_2 + x_2^2$
0	1	$x_0^2 + x_0x_2 + x_2^2$
0	1	$x_0^2 + x_1^2 + x_0x_2 + x_1x_2 + x_2^2$
0	1	$x_1^2 + x_1x_2 + x_2^2$
0	3	x_0^2
0	3	$x_0^2 + x_1^2$
0	3	$x_0^2 + x_1^2 + x_2^2$
0	3	$x_0^2 + x_2^2$
0	3	x_1^2
0	3	$x_1^2 + x_2^2$
0	3	x_2^2
0	5	$x_0^2 + x_0x_1$
0	5	$x_0^2 + x_0x_1 + x_0x_2$
0	5	$x_0^2 + x_0x_1 + x_0x_2 + x_1x_2$
0	5	$x_0^2 + x_0x_1 + x_1x_2 + x_2^2$
0	5	$x_0^2 + x_0x_2$
0	5	$x_0^2 + x_1^2 + x_0x_2 + x_1x_2$
0	5	x_0x_1
0	5	$x_0x_1 + x_0x_2$
0	5	$x_0x_1 + x_0x_2 + x_1x_2 + x_2^2$
0	5	$x_0x_1 + x_1^2$
0	5	$x_0x_1 + x_1^2 + x_0x_2 + x_1x_2$
0	5	$x_0x_1 + x_1^2 + x_0x_2 + x_2^2$
0	5	$x_0x_1 + x_1^2 + x_1x_2$
0	5	$x_0x_1 + x_1x_2$
0	5	x_0x_2
0	5	$x_0x_2 + x_1x_2$
0	5	$x_0x_2 + x_1x_2 + x_2^2$
0	5	$x_0x_2 + x_2^2$
0	5	$x_1^2 + x_1x_2$
0	5	x_1x_2
0	5	$x_1x_2 + x_2^2$

d	$\#C(\mathbb{F}_2)$	f
1	3	$x_0^2 + x_0x_1 + x_0x_2 + x_1x_2 + x_2^2$
1	3	$x_0^2 + x_0x_1 + x_0x_2 + x_2^2$
1	3	$x_0^2 + x_0x_1 + x_1^2 + x_0x_2$
1	3	$x_0^2 + x_0x_1 + x_1^2 + x_0x_2 + x_1x_2$
1	3	$x_0^2 + x_0x_1 + x_1^2 + x_1x_2$
1	3	$x_0^2 + x_0x_1 + x_1^2 + x_2^2$
1	3	$x_0^2 + x_0x_1 + x_1x_2$
1	3	$x_0^2 + x_0x_1 + x_2^2$
1	3	$x_0^2 + x_0x_2 + x_1x_2$
1	3	$x_0^2 + x_0x_2 + x_1x_2 + x_2^2$
1	3	$x_0^2 + x_1^2 + x_0x_2$
1	3	$x_0^2 + x_1^2 + x_0x_2 + x_2^2$
1	3	$x_0^2 + x_1^2 + x_1x_2$
1	3	$x_0^2 + x_1^2 + x_1x_2 + x_2^2$
1	3	$x_0^2 + x_1x_2$
1	3	$x_0^2 + x_1x_2 + x_2^2$
1	3	$x_0x_1 + x_0x_2 + x_1x_2$
1	3	$x_0x_1 + x_0x_2 + x_2^2$
1	3	$x_0x_1 + x_1^2 + x_0x_2$
1	3	$x_0x_1 + x_1^2 + x_0x_2 + x_1x_2 + x_2^2$
1	3	$x_0x_1 + x_1^2 + x_1x_2 + x_2^2$
1	3	$x_0x_1 + x_1^2 + x_2^2$
1	3	$x_0x_1 + x_1x_2 + x_2^2$
1	3	$x_0x_1 + x_2^2$
1	3	$x_1^2 + x_0x_2$
1	3	$x_1^2 + x_0x_2 + x_1x_2$
1	3	$x_1^2 + x_0x_2 + x_1x_2 + x_2^2$
1	3	$x_1^2 + x_0x_2 + x_2^2$

Wie findet man Punkte in $C(\mathbb{F}_p)$?
Wir beschränken uns auf den Fall $p \geq 3$. Ist C gegeben durch

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2,$$

so können wir f diagonalisieren, d.h. wir finden eine Matrix $T \in \mathrm{GL}_3(\mathbb{F}_p)$ und neue Koordinaten y_0, y_1, y_2, sodass mit

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

sich f schreibt als

$$f = b_0y_0^2 + b_1y_1^2 + b_2y_2^2.$$

Wir schreiben im Folgenden wieder x_0, x_1, x_2 statt y_0, y_1, y_2.

Fall $\mathrm{Rang}(C) = 1$**:** O.E. ist $f = x_0^2$. Die Punkte von C sind genau die Punkte der Geraden $x_0 = 0$.

Fall $\mathrm{Rang}(C) = 2$**:** O.E. können wir schreiben $f = cx_0^2 - x_1^2$ mit $c \in \mathbb{F}_p^*$. Die Kurve C enthält den unendlich fernen Punkt $(0:0:1)$. Im Endlichen ist

$$C(\mathbb{F}_p) \cap U_0 \simeq \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 = c\}.$$

Ist c ein Quadrat in $\mathbb{F}_p$, d.h. $c = d^2$ mit $d \in \mathbb{F}_p^*$, so gilt

$$C(\mathbb{F}_p) \cap U_0 = \{(d,y) : y \in \mathbb{F}_p\} \cup \{(-d,y) : y \in \mathbb{F}_p\},$$

$C(\mathbb{F}_p) \cap U_0$ besteht also aus zwei affinen parallelen Geraden, die sich im unendlich fernen Punkt $(0:0:1)$ schneiden.
Ist c kein Quadrat in $\mathbb{F}_p$, so ist

$$C(\mathbb{F}_p) \cap U_0 = \emptyset.$$

Fall $\mathrm{Rang}(C) = 3$**:** O.E. können wir schreiben $f = ax_0^2 + bx_1^2 - x_2^2$ mit $a, b \in \mathbb{F}_p^*$. Dann ist

$$C(\mathbb{F}_p) \cap U_0 \simeq \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = a + bx^2\}.$$

Da C nichtsingulär ist, gilt $\#C(\mathbb{F}_p) = p+1$. Wählt man einige x-Werte zufällig, sollte es darunten welche geben, für die $a + bx^2$ ein Quadrat ist, d.h. $a + bx^2 = y^2$. Dann hat man einen Kurvenpunkt $(1:x:y)$. Nun gibt es eine Reihe von Verfahren um Quadratwurzeln in $\mathbb{F}_p$ zu berechnen. Daher kann man praktisch schnell Punkte in $C(\mathbb{F}_p)$ finden. (Wir gehen darauf nicht näher ein.)

Der folgende Satz behandelt die Frage, ob -1 ein Quadrat in $\mathbb{F}_p$ ist.

Satz. *Sei p eine ungerade Primzahl. Dann gilt:*

- *Ist $p = 4k+1$ für ein $k \in \mathbb{N}$, so gibt es eine Zahl $i \in \mathbb{F}_p$ mit $i^2 = -1$, d.h. -1 ist ein Quadrat in $\mathbb{F}_p$.*
- *Ist $p = 4k+3$ für ein $k \in \mathbb{N}_0$, so hat die Gleichung $x^2 = -1$ keine Lösung in $\mathbb{F}_p$, d.h. -1 ist kein Quadrat in $\mathbb{F}_p$.*

Beweis:

- Wir haben den kleinen Satz von Fermat gezeigt, der besagt, dass

  $$a^{p-1} = 1 \text{ für alle } a \in \mathbb{F}_p^*$$

  gilt. Das Polynom $f(x) = x^{p-1} - 1$ hat Grad $p-1$, also höchstens $p-1$ Nullstellen. Da aber alle Zahlen $a \in \mathbb{F}_p^*$ Nullstellen von f sind, sind die Nullstellen von f genau die Zahlen aus $\mathbb{F}_p^*$, d.h.

  $$\{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p-1} = 1\} = \mathbb{F}_p^*.$$

  Sei $i \in \overline{\mathbb{F}}_p$ mit $i^2 = -1$. Dann gilt

  $$i^{p-1} = (i^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

- Ist $p = 4k+1$, so folgt

  $$i^{p-1} = (-1)^{2k} = 1,$$

  also ist $i \in \mathbb{F}_p^*$.
- Ist $p = 4k+3$, so folgt

  $$i^{p-1} = (-1)^{2k+1} = -1 \neq 1,$$

  also ist $i \notin \mathbb{F}_p^*$. ■

Beispiele: Für die Primzahlen $p \leq 100$ der Form $p = 4k + 1$ haben wir hier die Zahlen $i \in \mathbb{F}_p$ bestimmt mit $i^2 = -1$.

p	i mit $i^2 = -1$ in $\mathbb{F}_p$
5	2,3
13	5,8
17	4,13
29	12,17
37	6,31
41	9,32
53	23,30
61	11,50
73	27,46
89	34,55
97	22,75

Erfüllt i die Bedingung $i^2 = -1$, so natürlich auch $-i = p - i$.

7. Ebene Quadriken über $\mathbb{Q}$

Wir betrachten eine ebene projektive Quadrik C über $\mathbb{Q}$, die durch ein Polynom

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in \mathbb{Q}[x_0, x_1, x_2] \setminus \{0\}$$

definiert wird. Wir wollen untersuchen, wann $C(\mathbb{Q}) \neq \emptyset$ gilt. Schön wäre es, wenn wir $C(\mathbb{Q})$ gut beschreiben könnten.

Diagonalisierung: Mit dem zuvor beschriebenen Diagonalisierungsverfahren bestimmen wir eine Matrix $T \in \mathrm{GL}_3(\mathbb{Q})$ und führen neue Koordinaten y_0, y_1, y_2 durch

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

ein, sodass f in den neuen Koordinaten die Form

$$f = b_0y_0^2 + b_1y_1^2 + b_2y_2^2 \quad \text{mit} \quad b_0, b_1, b_2 \in \mathbb{Q}$$

hat, wobei $(b_0, b_1, b_2) \neq (0, 0, 0)$ gilt. Um nicht zu viele Variablennamen zu brauchen, schreiben wir aber wieder x_0, x_1, x_2 für y_0, y_1, y_2:

$$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \quad \text{mit} \quad b_0, b_1, b_2 \in \mathbb{Q}.$$

Die Hesse-Matrix ist

$$A_f = \begin{pmatrix} 2b_0 & 0 & 0 \\ 0 & 2b_1 & 0 \\ 0 & 0 & 2b_2 \end{pmatrix}.$$

Wir unterscheiden nun nach $\mathrm{Rang}(C) = \mathrm{Rang}(A_f) \in \{1, 2, 3\}$.
Fall $\mathrm{Rang}(C) = 1$**:** Dann ist genau eine der Zahlen b_0, b_1, b_2 von 0 verschieden. Nach Koordinatentausch können wir $b_0 \neq 0$, und nach Division durch b_0 dann

$$f = x_0^2$$

annehmen. Hier ist

$$C(\mathbb{Q}) = \{(0 : x_1 : x_2) : (x_1 : x_2) \in \mathbb{P}^1(\mathbb{Q})\}.$$

Fall $\mathrm{Rang}(C) = 2$**:** Genau eine der Zahlen b_0, b_1, b_2 ist 0. Nach eventuellem Koordinatentausch können wir $b_0 \neq 0$, $b_1 \neq 0$, $b_2 = 0$ annehmen, also

$$f = b_0x_0^2 + b_1x_1^2.$$

Der einzige unendlich ferne Punkt, d.h. mit $x_0 = 0$, ist $(0 : 0 : 1)$. Affin schreibt sich die Kurve

$$b_0 + b_1x^2 = 0 \quad \text{bzw. } x^2 = -\frac{b_0}{b_1}.$$

Ist $-\frac{b_0}{b_1}$ kein Quadrat in $\mathbb{Q}$, dann ist

$$C(\mathbb{Q}) = \{(0:0:1)\}.$$

Ist $-\frac{b_0}{b_1}$ ein Quadrat in $\mathbb{Q}$, d.h. $-\frac{b_0}{b_1} = c^2$ für ein $c \in \mathbb{Q}^*$, dann ist

$$C(\mathbb{Q}) = \{(0:0:1)\} \cup \{(1:c:y) : y \in \mathbb{Q}\} \cup \{(1:-c:y) : y \in \mathbb{Q}\}.$$

Fall $\mathrm{Rang}(C) = 3$ **- Reduktion auf Legendre-Normalform:** Wir haben jetzt C gegeben durch

$$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \text{ mit } b_0, b_1, b_2 \in \mathbb{Q}^*.$$

Die Kurve ist nichtsingulär.

1. Schritt:

- Wir bestimmen den gemeinsamen Nenner von b_0, b_1, b_2, also

  $$N = \mathrm{kgV}(\mathrm{Nenner}(b_0), \mathrm{Nenner}(b_1), \mathrm{Nenner}(b_2))$$

  und multiplizieren f damit:

  $$N \cdot f = (Nb_0)x_0^2 + (Nb_1)x_1^2 + (Nb_2)x_2^2.$$

  Dann nennen wir das Polynom wieder f, die Koeffizienten wieder b_0, b_1, b_2 und haben dann $b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}$.
- Nun bestimmen wir den größten gemeinsamen Teiler von b_0, b_1, b_2, also

  $$Z = \mathrm{ggT}(b_0, b_1, b_2),$$

  und dividieren das Polynom durch Z:

  $$\frac{1}{Z} \cdot f = \frac{b_0}{Z}x_0^2 + \frac{b_1}{Z}x_1^2 + \frac{b_2}{Z}x_2^2.$$

  Anschließend nennen wir die Koeffizienten wieder b_0, b_1, b_2 und das Polynom wieder f.
- Wir haben jetzt

  $$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \text{ mit } b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\} \text{ und } \mathrm{ggT}(b_0, b_1, b_2) = 1.$$

2. Schritt: (Ziel: quadratfreie b_0, b_1, b_2)

- Wir zerlegen

  $$b_i = b_i'c_i^2,$$

  wo b_i' der quadratfreie Anteil von b_i und $c_i \in \mathbb{N}$ ist. Wegen

  $$b_ix_i^2 = b_i'c_i^2x_i^2 = b_i'(c_ix_i)^2$$

  führen wir neue Koordinaten y_0, y_1, y_2 durch

  $$y_i = c_ix_i \text{ bzw. } x_i = \frac{1}{c_i}y_i$$

  ein und erhalten dann

  $$f = b_0'y_0^2 + b_1'y_1^2 + b_2'y_2^2.$$

  Danach schreiben wir wieder b_i für b_i' und x_i für y_i.
- Wir haben also

  $$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2$$

  mit

  $$b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}, b_0, b_1, b_2 \text{ quadratfrei und } \mathrm{ggT}(b_0, b_1, b_2) = 1.$$

3. Schritt: (Ziel: paarweise teilerfremde b_0, b_1, b_2)

- Wir führen neue Koordinaten y_0, y_1, y_2 ein durch

$$x_0 = \mathrm{ggT}(b_1, b_2) \cdot y_0, \quad x_1 = \mathrm{ggT}(b_0, b_2) \cdot y_1, \quad x_2 = \mathrm{ggT}(b_0, b_1) \cdot y_2.$$

Dann wird

$$f = b_0 \cdot (\mathrm{ggT}(b_1, b_2))^2 \cdot y_0^2 + b_1 \cdot (\mathrm{ggT}(b_0, b_2))^2 \cdot y_1^2 + b_2 \cdot (\mathrm{ggT}(b_0, b_1))^2 \cdot y_2^2.$$

Nun dividieren wir das Polynom durch $G = \mathrm{ggT}(b_0, b_1)\mathrm{ggT}(b_0, b_2)\mathrm{ggT}(b_1, b_2)$:

$$\frac{f}{G} = \frac{b_0 \cdot \mathrm{ggT}(b_1, b_2)}{\mathrm{ggT}(b_0, b_1)\mathrm{ggT}(b_0, b_2)} \cdot y_0^2 + \frac{b_1 \cdot \mathrm{ggT}(b_0, b_2)}{\mathrm{ggT}(b_0, b_1)\mathrm{ggT}(b_1, b_2)} \cdot y_1^2 + \frac{b_2 \cdot \mathrm{ggT}(b_0, b_1)}{\mathrm{ggT}(b_0, b_2)\mathrm{ggT}(b_1, b_2)} \cdot y_2^2.$$

Man kann sich überlegen, dass die Koeffizienten nun ganze Zahlen, paarweise teilerfremd und quadratfrei sind. Nun schreiben wir wieder f für das Polynom, b_0, b_1, b_2 für die Koeffizienten und x_0, x_1, x_2 für die Variablen.

- Wir haben nun

$$f = b_0 x_0^2 + b_1 x_1^2 + b_2 x_2^2$$

mit

$$b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}, \quad b_0, b_1, b_2 \text{ quadratfrei und paarweise teilerfremd.}$$

4. Schritt: (Ziel: $b_0 > 0$, $b_1 > 0$)

- Sind zwei oder drei der b_i negativ, multiplizieren wir die Gleichungen mit -1 und können dann annehmen, dass höchstens ein b_i negativ ist.
- Ist $b_0 < 0$, vertauschen wir b_0 mit b_2 und x_0 mit x_2.
- Ist $b_1 < 0$, vertauschen wir b_1 mit b_2 und x_1 mit x_2.
- Wir haben nun

$$f = b_0 x_0^2 + b_1 x_1^2 + b_2 x_2^2 \quad \text{mit} \quad b_0 \in \mathbb{N}, \quad b_1 \in \mathbb{N}, \quad b_2 \in \mathbb{Z} \setminus \{0\}$$

und

$$b_0, b_1, b_2 \text{ quadratfrei}, \quad \mathrm{ggT}(b_0, b_1) = \mathrm{ggT}(b_0, b_2) = \mathrm{ggT}(b_1, b_2) = 1.$$

Diese Darstellung nennen wir Legendre-Normalform:

DEFINITION. *Ein eine über $\mathbb{Q}$ definierte projektive ebene Quadrik beschreibendes Polynom f ist in* **Legendre-Normalform**, *wenn es sich schreiben lässt als*

$$f = b_0 x_0^2 + b_1 x_1^2 + b_2 x_2^2$$

mit folgenden Eigenschaften:

- $b_0 \in \mathbb{N}$, $b_1 \in \mathbb{N}$, $b_2 \in \mathbb{Z} \setminus \{0\}$.
- b_0, b_1, b_2 *sind quadratfrei, d.h. nicht durch das Quadrat einer Primzahl teilbar.*
- b_0, b_1, b_2 *sind paarweise teilerfremd, d.h.* $\mathrm{ggT}(b_0, b_1) = \mathrm{ggT}(b_0, b_2) = \mathrm{ggT}(b_1, b_2) = 1$.

Bemerkung: Mit dem zuvor beschriebenen Reduktionsprozess können wir jede über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadrik in Legendre-Normalform transformieren.

Beispiel: Wir beginnen mit

$$f = x_0^2 - 2x_0x_1 + 3x_0x_2 - 4x_1^2 + 5x_1x_2 - 6x_2^2.$$

Diagonalisieren führt zu

$$f = x_0^2 - 5x_1^2 - \frac{101}{20}x_2^2.$$

Multiplikation mit 20 ergibt

$$f = 20x_0^2 - 100x_1^2 - 101x_2^2.$$

Wegen $f = 5(2x_0)^2 - (10x_1)^2 - 101x_2^2$ betrachten wir

$$f = 5x_0^2 - x_1^2 - 101x_2^2.$$

Die Koeffizienten sind nun quadratfrei und paarweise teilerfremd. Da zwei der Koeffizienten negativ sind, multiplizieren wir mit -1:

$$f = -5x_0^2 + x_1^2 + 101x_2^2.$$

Da b_0 negativ ist, vertauschen wir b_0 und b_2:

$$f = 101x_0^2 + x_1^2 - 5x_2^2.$$

Wenn man schaut, welche Koordinatentransformationen durchgeführt wurden, so findet man

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -\frac{7}{10} & \frac{1}{10} & \frac{1}{2} \\ \frac{4}{5} & \frac{1}{10} & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

und erhält

$$f = -\frac{1}{20}\left(101y_0^2 + y_1^2 - 5y_2^2\right).$$

LEMMA. *Sei $f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2$ in Legendre-Normalform und C die zugehörige über $\mathbb{Q}$ definierte Kurve, also*

$$b_0 \in \mathbb{N}, b_1 \in \mathbb{N}, b_2 \in \mathbb{Z} \setminus \{0\}, b_1, b_2, b_2 \text{ quadratfrei}$$

und

$$\mathrm{ggT}(b_0, b_1) = \mathrm{ggT}(b_0, b_2) = \mathrm{ggT}(b_1, b_2) = 1.$$

Dann gilt:

$$C(\mathbb{R}) \neq \emptyset \quad \Longleftrightarrow \quad b_2 < 0.$$

Dies impliziert

$$C(\mathbb{Q}) \neq \emptyset \quad \Longrightarrow \quad b_2 < 0$$

und

$$b_2 > 0 \quad \Longrightarrow \quad C(\mathbb{Q}) = \emptyset.$$

Eine notwendige Bedingung für die Existenz von $\mathbb{Q}$-rationalen Punkten auf der Kurve ist also $b_2 < 0$.
Reduktion modulo p: Ist $f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \in \mathbb{Q}[x_0, x_1, x_2]$ in Legendre-Normalform, so kann man für eine Primzahl p die Koeffizienten auch als Elemente von $\mathbb{F}_p$ betrachten und erhält ein Polynom

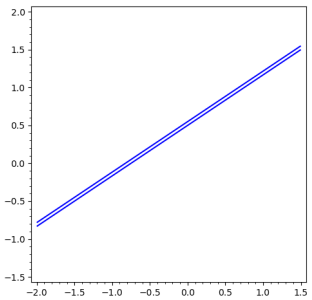
$$f_p = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \in \mathbb{F}_p[x_0, x_1, x_2].$$

Die zugehörige über $\mathbb{F}_p$ definierte Kurve werde mit C_p bezeichnet.
Wir unterscheiden verschiedene Fälle:

- **Fall $p = 2$:** Über $\mathbb{F}_2$ gilt

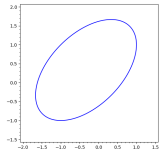
  $$f_2 = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = (b_0x_0 + b_1x_1 + b_2x_2)^2 \in \mathbb{F}_2[x_0, x_1, x_2].$$

  C_2 ist also eine Doppelgerade.



- **Fall $p > 2$, $p \nmid b_0b_1b_2$:** Betrachtet man b_0, b_1, b_2 in $\mathbb{F}_p$, so gilt $b_0, b_1, b_2 \in \mathbb{F}_p^*$. Dann hat C_p Rang 3, ist also nichtsingulär und

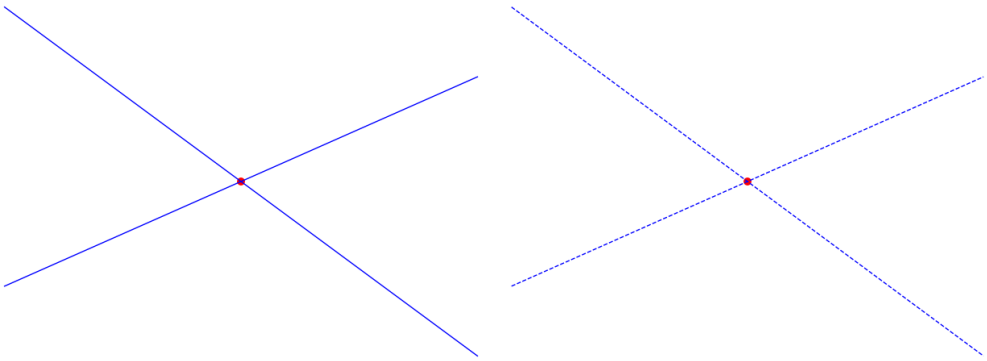
  $$\#C_p(\mathbb{F}_p) = p + 1.$$



- **Fall $p > 2$, $p \mid b_0b_1b_2$:** Da die b_i paarweise teilerfremd sind, teilt p genau eine der Zahlen b_0, b_1, b_2, also o.E. b_0. Dann gilt

$$f_p = b_1x_1^2 + b_2x_2^2 \in \mathbb{F}_p[x_0, x_1, x_2], \quad b_1, b_2 \neq 0 \text{ in } \mathbb{F}_p.$$

  C_p hat Rang 2 und genau eine Singularität, nämlich in $(1 : 0 : 0)$. Es gibt zwei Möglichkeiten: f_p zerfällt über $\mathbb{F}_p$ in zwei Linearfaktoren oder f_p ist irreduzibel über $\mathbb{F}_p$.



- Weiter im Fall $p > 2$, $p \mid b_0b_1b_2$: Es sei

$$f_p = b_1x_1^2 + b_2x_2^2 \text{ und } b_1, b_2 \neq 0 \text{ in } \mathbb{F}_p.$$

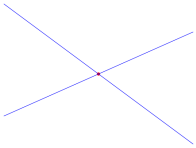
  Es ist

$$f_p = \frac{1}{b_1}\left(b_1^2x_1^2 + b_1b_2x_2^2\right) = \frac{1}{b_1}\left((b_1x_1)^2 - (-b_1b_2)\,x_2^2\right).$$

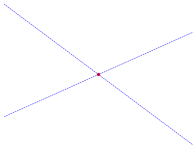
  Sei $c \in \overline{\mathbb{F}}_p$ mit $c^2 = -b_1b_2$. Dann folgt

$$f_p = \frac{1}{b_1}(b_1x_1 - cx_2)(b_1x_2 + cx_2).$$

  – **Fall: $-b_1b_2$ ist ein Quadrat in $\mathbb{F}_p$:** Dann ist $c \in \mathbb{F}_p$ und f_p reduzibel über $\mathbb{F}_p$ und $\#C_p(\mathbb{F}_p) = 2p + 1$.



  – **Fall: $-b_1b_2$ ist kein Quadrat in $\mathbb{F}_p$:** Dann ist $c \in \overline{\mathbb{F}}_p \setminus \mathbb{F}_p$. Das Polynom f_p ist irreduzibel über $\mathbb{F}_p$, von der Kurve ist nur die Singularität über $\mathbb{F}_p$ zu sehen. Insbesondere $\#C_p(\mathbb{F}_p) = 1$.



Das folgende Lemma zeigt, welche Auswirkungen die Existenz eines $\mathbb{Q}$-rationalen Punktes von C auf die Kurven C_p hat.

LEMMA. *Sei $f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \in \mathbb{Q}[x_0, x_1, x_2]$ in Legendre-Normalform und C die zugehörige über $\mathbb{Q}$ definierte Kurve. Dann gilt:*

$$C(\mathbb{Q}) \neq \emptyset \quad \Longrightarrow \quad \begin{cases} \text{für alle ungeraden Primteiler } p \text{ von } b_0b_1b_2 \\ \text{zerfällt } f_p \text{ in zwei verschiedene Linearfaktoren} \\ \text{über } \mathbb{F}_p, \text{ d.h. } \#C_p(\mathbb{F}_p) = 2p + 1. \end{cases}$$

Beweis:

- Sei $Q = (q_0 : q_1 : q_2) \in C(\mathbb{Q})$, wobei wir $q_0, q_1, q_2 \in \mathbb{Z}$ und $\mathrm{ggT}(q_0, q_1, q_2) = 1$ voraussetzen können. Dann gilt also
$$b_0 q_0^2 + b_1 q_1^2 + b_2 q_2^2 = 0.$$
- Sei p ein beliebiger ungerader Primteiler von $b_0 b_1 b_2$. Wir betrachten den Fall $p \mid b_0$. Da die b_i paarweise teilerfremd sind, folgt $p \nmid b_1$ und $p \nmid b_2$. Nun benutzt man die Beziehung $b_0 q_0^2 + b_1 q_1^2 + b_2 q_2^2 = 0$. Würde $p \mid q_1$ gelten, so würde $p \mid b_2 q_2^2$, also $p \mid q_2$ folgen; da dann p^2 die Zahl $b_1 q_1^2 + b_2 q_2^2$, und damit $b_0 q_0^2$ teilen würde, erhält man einen Widerspruch zur Quadratfreiheit von b_0 und $p \nmid q_0$. Also gilt $p \nmid q_1$ und analog $p \nmid q_2$.
- Wir interpretieren die Gleichung $b_0 q_0^2 + b_1 q_1^2 + b_2 q_2^2 = 0$ nun in $\mathbb{F}_p$:
$$b_1 q_1^2 + b_2 q_2^2 = 0, \quad \text{also} \quad b_2 = -b_1 \frac{q_1^2}{q_2^2} \text{ in } \mathbb{F}_p.$$
Dann ist
$$f_p \;=\; b_1 x_1^2 + b_2 x_2^2 = b_1 x_1^2 - b_1 \frac{q_1^2}{q_2^2} x_2^2 = b_1 (x_1 - \frac{q_1}{q_2} x_2)(x_1 + \frac{q_1}{q_2} x_2),$$
was die Behauptung beweist. Wir bemerken außerdem noch, dass
$$-b_1 b_2 = b_1^2 \frac{q_1^2}{q_2^2} = \left(\frac{b_1 q_1}{q_2} \right)^2$$
ein Quadrat in $\mathbb{F}_p$ ist. ■

Bemerkung: Für eine ungerade Primzahl p und eine ganze Zahl a definiert man das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ wie folgt:
$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } a = b^2 \text{ in } \mathbb{F}_p \text{ für ein } b \in \mathbb{F}_p^*, \\ -1, & \text{falls } a \neq b^2 \text{ in } \mathbb{F}_p \text{ für alle } b \in \mathbb{F}_p, \\ 0, & \text{falls } a = 0 \text{ in } \mathbb{F}_p. \end{cases}$$
Es gibt eine Reihe von Rechenregeln für das Legendre-Symbol, auf die wir hier nicht eingehen.

Die zuvor hergeleiteten notwendigen Bedingungen für die Existenz von $\mathbb{Q}$-rationalen Punkten sind auch hinreichend. Mit Hilfe des Legendre-Symbols lassen sie sich wie folgt formulieren:

Satz (Legendre). *Sei $f = b_0 x_0^2 + b_1 x_1^2 + b_2 x_2^2$ in Legendre-Normalform. Genau dann hat die über $\mathbb{Q}$ durch $f = 0$ definierte projektive ebene Quadrik $\mathbb{Q}$-rationale Punkte, wenn gilt:*

- $\left(\frac{-b_1 b_2}{p}\right) = 1$ *für alle ungeraden Primzahlen p mit $p \mid b_0$,*
- $\left(\frac{-b_0 b_2}{p}\right) = 1$ *für alle ungeraden Primzahlen p mit $p \mid b_1$,*
- $\left(\frac{-b_0 b_1}{p}\right) = 1$ *für alle ungeraden Primzahlen p mit $p \mid b_2$,*
- $b_2 < 0$.

Wir gehen hier nicht auf den Beweis ein.
Beispiel: Wir betrachten $f = 101x_0^2 + x_1^2 - 5x_2^2$. Das Polynom ist in Legendre-Normalform ($b_0 = 101$, $b_1 = 1$, $b_2 = -5$). Wir gehen die Bedingungen des letzten Satzes nacheinander durch und schauen, ob sie erfüllt sind.

- Es gibt nur einen ungeraden Primteiler von $b_0 = 101$, nämlich $p = 101$. Es ist $-b_1 b_5 = 5$. Wir müssen überprüfen, ob $-b_1 b_2 = 5$ ein Quadrat in $\mathbb{F}_{101}$ ist. Mit dem Legendre-Symbol geht das wie folgt:
$$\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1,$$
also ist 5 ein Quadrat in $\mathbb{F}_{101}$.
- $b_1 = 1$ hat keinen Primteiler, sodass hier nichts zu tun ist.
- $b_2 = -5$ hat nur einen ungeraden Primteiler, nämlich 5. Es ist $-b_0 b_1 = -101$. Wir müssen überprüfen, ob $-b_0 b_1 = -101$ ein Quadrat in $\mathbb{F}_5$ ist. Nun gilt in $\mathbb{F}_5$ aber $-101 = -1 = 4 = 2^2$, was zeigt, dass $-b_0 b_1$ ein Quadrat in $\mathbb{F}_5$ ist.

- Es ist $b_2 = -5 < 0$.

Alle Bedingungen des Satzes von Legendre sind also erfüllt. Daher besitzt die Kurve $\mathbb{Q}$-rationale Punkte. Kann man auch praktisch Punkte bestimmen?
Hat eine über $\mathbb{Q}$ durch

$$b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = 0$$

definierte projektive ebene Quadrik $\mathbb{Q}$-rationale Punkte, so interessiert natürlich auch die Frage, wie man solche Punkte finden kann.
Hierfür ist folgender Satz hilfreich:

SATZ (Holzer). *Hat die für $b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}$ durch*

$$b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = 0$$

definierte Quadrik $\mathbb{Q}$-rationale Punkte, so gibt es auch einen Kurvenpunkt $(q_0 : q_1 : q_2)$ mit $q_0, q_1, q_2 \in \mathbb{Z}$ und

$$|q_0| \leq \sqrt{|b_1b_2|}, \quad |q_1| \leq \sqrt{|b_0b_2|}, \quad |q_2| \leq \sqrt{|b_0b_1|}.$$

Hat man mit Hilfe des Satzes von Legendre gezeigt, kann man nun mit Hilfe des Satzes von Holzer nach Lösungen suchen.
Beispiel: Wir hatten zuvor mit dem Satz von Legendre gezeigt, dass die durch

$$101x_0^2 + x_1^2 - 5x_2^2 = 0$$

definierte Quadrik C einen $\mathbb{Q}$-rationalen Punkt besitzt. Der Satz von Holzer besagt, dass ein Punkt $(q_0 : q_1 : q_2) \in C(\mathbb{Q})$ existiert mit $q_0, q_1, q_2 \in \mathbb{Z}$ und

$$|q_0| \leq \sqrt{|1 \cdot (-5)|} \leq 2.24, \quad |q_1| \leq \sqrt{|101 \cdot (-5)|} \leq 22.48, \quad |q_2| \leq \sqrt{|101 \cdot 1|} \leq 10.05.$$

Mit Rechnerhilfe findet man dann folgende Lösungen

$$(2 : \pm 1 : \pm 9), \quad (1 : \pm 12 : \pm 7).$$

Wir wollen noch eine Anwendung des Satzes von Legendre geben:

SATZ. *Zu einer Primzahl $p \neq 5$ gibt es genau dann Zahlen $x, y \in \mathbb{Q}$ mit*

$$p = x^2 - 5y^2,$$

wenn p in der Dezimaldarstellung auf 1 oder 9 endet. (Für $p = 5$ gilt $5 = 5^2 - 5 \cdot 2^2$.)

Beweis:

- Durch Homogenisieren und Umstellen erhalten wir aus $p = x^2 - 5y^2$ die Gleichung
$$px_0^2 + 5x_1^2 - x_2^2 = 0,$$
die wegen $p \neq 5$ offensichtlich in Legendre-Normalform ist.
- Wir zeigen, dass $p = x^2 - 5y^2$ genau dann eine Lösung in $\mathbb{Q}^2$ besitzt, wenn $px_0^2 + 5x_1^2 - x_2^2 = 0$ eine nichttriviale Lösung in $\mathbb{Q}^3$ besitzt.
  - Ist $(x, y) \in \mathbb{Q}^2$ eine Lösung von $p = x^2 - 5y^2$, so ist $(1, y, x) \in \mathbb{Q}^3$ eine nichttriviale Lösung von $px_0^2 + 5x_1^2 - x_2^2 = 0$.
  - Ist $(x_0, x_1, x_2) \in \mathbb{Q}^3$ eine nichttriviale Lösung von $px_0^2 + 5x_1^2 - x_2^2 = 0$, so gilt $x_0 \neq 0$, da andernfalls aus $5x_1^2 = x_2^2$ sofort $x_1 = x_2 = 0$ folgen würde. Daher ist
  $$p = (\frac{x_2}{x_0})^2 - 5(\frac{x_1}{x_0})^2,$$
  sodass auch $p = x^2 - 5y^2$ eine Lösung in $\mathbb{Q}$ besitzt.
- Wir betrachten den Fall $p = 2$. Die Gleichung lautet
$$2x_0^2 + 5x_1^2 - x_2^2 = 0$$
und ist bereits in Legendre-Normalform. Mit $b_0 = 2$, $b_1 = 5$, $b_2 = -1$ ist der einzige ungerade Primteiler von $b_0b_1b_2$ die Zahl 5. Wegen
$$\left(\frac{-2 \cdot (-1)}{5}\right) = \left(\frac{2}{5}\right) = -1$$
besitzt die Gleichung keine nichttriviale Lösung.

- Sei nun $p \notin \{2,5\}$. Um die Lösbarkeit der Gleichung $px_0^2 + 5x_1^2 - x_2^2 = 0$ mit dem Satz von Legendre zu untersuchen, müssen wir die ungeraden Primteiler von $p \cdot 5 \cdot (-1)$ betrachten, also p und 5. Nach dem Satz von Legendre hat die Gleichung genau dann eine nichttriviale Lösung in $\mathbb{Q}^3$, wenn gilt

$$\left(\frac{-5\cdot(-1)}{p}\right) = \left(\frac{5}{p}\right) = 1 \quad \text{und} \quad \left(\frac{-p\cdot(-1)}{5}\right) = \left(\frac{p}{5}\right) = 1.$$

(Die Vorzeichenbedingung $b_2 < 0$ ist trivialerweise erfüllt.) Das quadratische Reziprozitätsgesetz liefert wegen $5 \equiv 1 \bmod 4$

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$

sodass als einzige Bedingung

$$\left(\frac{p}{5}\right) = 1$$

bleibt. Nun ist

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{für } p \equiv 1,4 \bmod 5, \\ -1 & \text{für } p \equiv 2,3 \bmod 5. \end{cases}$$

Primzahlen $p \neq 2,5$ enden in der Dezimaldarstellung auf $1,3,7,9$.

Da eine Kongruenz modulo 10 eine Kongruenz modulo 5 liefert, erhalten wir

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{für } p \equiv 1,9 \bmod 10, \\ -1 & \text{für } p \equiv 3,7 \bmod 10. \end{cases}$$

Damit folgt: Die Quadrik hat genau dann $\mathbb{Q}$-rationale Punkte, wenn $p \equiv 1 \bmod 10$ oder $p \equiv 9 \bmod 10$ gilt. Dies war zu zeigen. ■

Beispiele: Für die Primzahlen $p \leq 200$, die sich in der Form $p = x^2 - 5y^2$ schreiben lassen, haben wir eine entsprechende Darstellung angegeben:

$$\begin{aligned}
5 &= 5^2 - 5\cdot 2^2 \\
11 &= 4^2 - 5\cdot 1^2 \\
19 &= 8^2 - 5\cdot 3^2 \\
29 &= 7^2 - 5\cdot 2^2 \\
31 &= 6^2 - 5\cdot 1^2 \\
41 &= 11^2 - 5\cdot 4^2 \\
59 &= 8^2 - 5\cdot 1^2 \\
61 &= 9^2 - 5\cdot 2^2 \\
71 &= 14^2 - 5\cdot 5^2 \\
79 &= 18^2 - 5\cdot 7^2 \\
89 &= 13^2 - 5\cdot 4^2 \\
101 &= 11^2 - 5\cdot 2^2 \\
109 &= 17^2 - 5\cdot 6^2 \\
131 &= 16^2 - 5\cdot 5^2 \\
139 &= 12^2 - 5\cdot 1^2 \\
149 &= 13^2 - 5\cdot 2^2 \\
151 &= 14^2 - 5\cdot 3^2 \\
179 &= 28^2 - 5\cdot 11^2 \\
181 &= 19^2 - 5\cdot 6^2 \\
191 &= 14^2 - 5\cdot 1^2 \\
199 &= 18^2 - 5\cdot 5^2
\end{aligned}$$

Wir haben nur bewiesen, dass für Primzahlen $p \equiv 1, 9 \bmod 10$ rationale Zahlen x, y mit $p = x^2 - 5y^2$ existieren. Die obigen Beispiele deuten darauf hin, dass sich sogar ganze Zahlen x, y finden lassen.

8. Büschel ebener Quadriken

(Wir setzen hier der Einfachkeit halber einen algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2$ voraus.)
Ein **Büschel ebener (projektiver) Quadriken** ist eine „Familie“ von ebenen Quadriken

$$ug(x_0, x_1, x_2) + vh(x_0, x_1, x_2) = 0, \quad (u : v) \in \mathbb{P}^1$$

von ebenen Quadriken, parametrisiert durch $(u : v) \in \mathbb{P}^1$. Dabei sind $g(x_0, x_1, x_2), h(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ linear unabhängige homogene Polynome vom Grad 2. Wir schreiben auch

$$f_{(u,v)}(x_0, x_1, x_2) = ug(x_0, x_1, x_2) + vh(x_0, x_1, x_2).$$

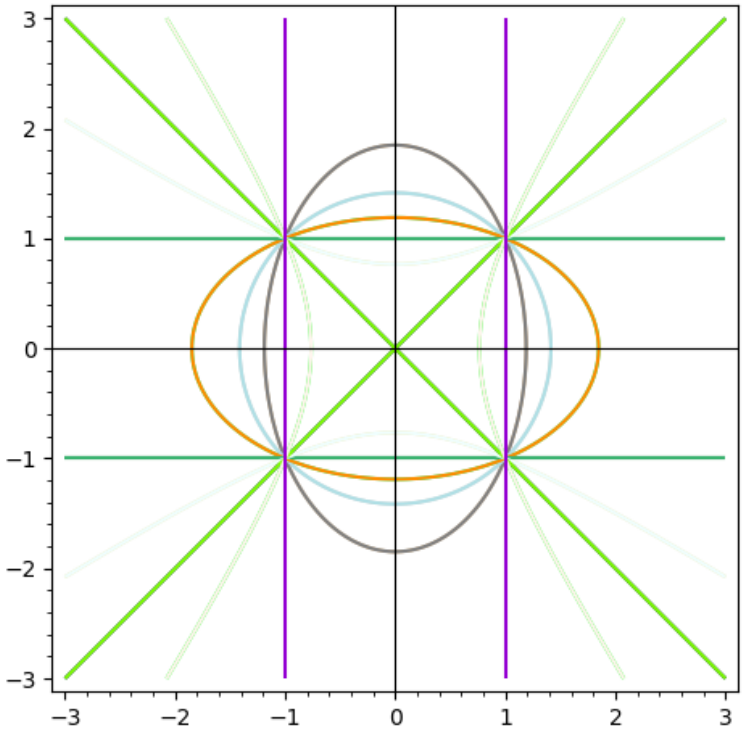
Es ist klar, dass die Nullstellenmenge $f_{(u,v)} = 0$ nur von $(u : v) \in \mathbb{P}^1$ abhängt. (Statt u, v verwenden wir auch manchmal andere Parameter.)
Beispiel: Die folgende Zeichnung zeigt einige Kurven des Büschels

$$u(x_1^2 - x_0^2) + v(x_2^2 - x_0^2) = 0,$$

das sich affin in der Form

$$u(x^2 - 1) + v(y^2 - 1) = 0$$

schreibt.



Bemerkung: Mit SAGE kann man Büschel auch leicht animiert darstellen:

```
# Animation des Quadrikenbueschels u*g+v*h=0 mit SAGE.
# g=a0*x0^2+a1*x0*x1+...+a_5*x2^2 und h=b0*x0^2+b1*x0*x1+...+b5*x2^2 sind
# als 6-Tupel (a0,a1,a2,a3,a4,a5),(b0,b1,b2,b3,b4,b5) einzugeben. Das
# Bueschel wir affin (in U_0) gezeichnet im Quadrat [-M,M]x[-M,M].
def zeichne_bueschel(g,h,M=10):
  var("x,y")
  a0,a1,a2,a3,a4,a5=g
  b0,b1,b2,b3,b4,b5=h
  g=a0+a1*x+a2*y+a3*x^2+a4*x*y+a5*y^2
```

```
h=b0+b1*x+b2*y+b3*x^2+b4*x*y+b5*y^2
G=animate(implicit_plot(cos(t)*g+sin(t)*h==0,(x,-M,M),(y,-M,M))
          for t in sxrange(0,pi,0.1))
G.show()
```

Beispielsweise erhält man das Büschel

$$u(x_1^2 - x_0^2) + v(x_2^2 - x_0^2) = 0$$

durch den Aufruf

```
zeichne_bueschel((-1,0,0,1,0,0),(-1,0,0,0,0,1))
```

Bemerkung: Definiert

$$f_{(u,v)} = ug + vh$$

ein Büschel ebener Quadriken, sind $\widetilde{g} = 0$ und $\widetilde{h} = 0$ zwei verschiedene Kurven des Büschels, so liefert

$$\widetilde{f}_{(u,v)} = u\widetilde{g} + v\widetilde{h}$$

das gleiche Büschel.

Beweis: Es gibt $a, b, c, d \in K$ mit $\begin{pmatrix}\widetilde{g}\\ \widetilde{h}\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}g\\ h\end{pmatrix}$. Dann ist

$$\widetilde{f}_{(u,v)} = u(ag + bh) + v(cg + dh) = (au + cv)g + (ub + dv)h = f_{(au+cv,ub+dv)}.$$

Wäre $\det \begin{pmatrix}a & c\\ b & d\end{pmatrix} = 0$, so gäbe es ein $\lambda \in K^*$ mit $(c, d) = \lambda(a, b)$, was zu

$$\widetilde{h} = cg + dh = \lambda(ag + bh) = \lambda\widetilde{g}$$

führen würde. $\widetilde{g} = 0$ und $\widetilde{h} = 0$ wären also die gleichen Kurven, im Widerspruch zur Voraussetzung.
$\widetilde{f}_{(u,v)}$ entsteht also aus $f_{(u,v)}$ durch Koordinatenwechsel im parametrisierenden $\mathbb{P}^1$.

Basispunkte eines Büschels: Die Punkte, durch die alle Kurven eines Büschels $ug(x_0, x_1, x_2) + vh(x_0, x_1, x_2) = 0$ gehen, heißen die **Basispunkte** des Büschels:

$$\{P \in \mathbb{P}^2 : ug(P) + vh(P) = 0 \text{ für alle } u, v \in K\}.$$

Offensichtlich ist

$$\{P \in \mathbb{P}^2 : ug(P) + vh(P) = 0 \text{ für alle } u, v \in K\} = \{P \in \mathbb{P}^2 : g(P) = h(P) = 0\}.$$

Zur Bestimmung der Basispunkte eines Büschels reicht es also, den Durchschnitt zweier verschiedener Kurven des Büschels zu bestimmen.

Beispiel: Wir wollen die Basispunkte des Büschels

$$u(x_1^2 - x_0^2) + v(x_2^2 - x_0^2) = 0$$

bestimmen, also die Punkte der Menge $\{x_1^2 = x_0^2, x_2^2 = x_0^2\}$. Im Unendlichen ($x_0 = 0$) liegt offensichtlich kein Punkt der Menge. Daher können wir uns auf den affinen Teil mit $(x_0 : x_1 : x_2) = (1 : x : y)$ beschränken. (x, y) ist Basispunkt, wenn $x^2 = 1$ und $y^2 = 1$ gilt. Hierfür gibt es 4 Möglichkeiten:

$$(1, 1), \quad (1, -1), \quad (-1, 1), \quad (-1, -1)$$

bzw. projektiv

$$(1 : 1 : 1), \quad (1 : 1 : -1), \quad (1 : -1 : 1), \quad (1 : -1 : -1).$$

Das Büschel hat also 4 Basispunkte.
Schreiben wir

$$\begin{aligned} g &= a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2,\\ h &= b_0x_0^2 + b_1x_0x_1 + b_2x_0x_2 + b_3x_1^2 + b_4x_1x_2 + b_5x_2^2, \end{aligned}$$

so wird die Hesse-Matrix des Büschels $f_{(u,v)} = ug + vh$

$$A_{f_{(u,v)}} = uA_g + vA_f = \begin{pmatrix} 2(ua_0 + vb_0) & ua_1 + vb_1 & ua_2 + vb_2\\ ua_1 + vb_1 & 2(ua_3 + vb_3) & ua_4 + vb_4\\ ua_2 + vb_2 & ua_4 + vb_4 & 2(ua_5 + vb_5)\end{pmatrix}.$$

Nun ist

$$\det(A_{f_{(u,v)}}) = \det(uA_g + vA_f) \in K[u,v]$$

ein homogenes Polynom vom Grad 3 und u, v.
Das Büschelelement $f_{(u,v)}$ ist genau dann reduzibel, wenn $\det(A_{f_{(u,v)}}) = 0$ gilt.
Da das homogene Polynom $\det(A_{f_{(t_0,t_1)}}) \in K[u,v]$ mindestens eine Nullstelle - K war als algebraisch abgeschlossen vorausgesetzt - besitzt, folgt insbesondere:
Jedes Büschel enthält mindestens eine reduzible Kurve.
Beispiel: Wir betrachten das Büschel

$$f_{(u,v)} = u(x_1^2 - x_0^2) + v(x_2^2 - x_0^2) = (-u-v)x_0^2 + ux_1^2 + vx_2^2.$$

Die zugehörige Hesse-Matrix ist

$$A = \begin{pmatrix} 2(-u-v) & 0 & 0 \\ 0 & 2u & 0 \\ 0 & 0 & 2v \end{pmatrix}$$

mit der Determinante

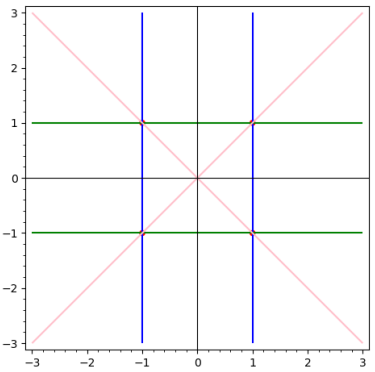
$$-8(u+v)uv.$$

Die Nullstellen sind

$$(u:v) = (0:1), (1:0), (1:-1).$$

Dazu gehören die reduziblen Quadriken

$$\begin{aligned} f_{(0,1)} &= x_2^2 - x_0^2 = (x_2 - x_0)(x_2 + x_0), \\ f_{(1,0)} &= x_1^2 - x_0^2 = (x_1 - x_0)(x_1 + x_0), \\ f_{(1,-1)} &= (x_1^2 - x_0^2) - (x_2^2 - x_0^2) = x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2). \end{aligned}$$



Wieviele Basispunkte hat ein Büschel? Sei $f_{(u,v)} = ug + vh$ ein Büschel von ebenen Quadriken. Da das Büschel mindestens eine reduzible Kurve enthält, können wir annehmen, dass h reduzibel ist, d.h. $h = \ell_1\ell_2$ mit zwei Linearformen ℓ_1, ℓ_2. Die Menge der Basispunkte des Büschels ist dann

$$\{g = h = 0\} = \{g = \ell_1\ell_2 = 0\} = \{g = \ell_1 = 0\} \cup \{g = \ell_2 = 0\}.$$

- **Fall ℓ_1 oder ℓ_2 ist ein Teiler von g:** O.E. $g = \ell_2\ell_0$. Dann ist das Büschel

  $$f_{(u,v)} = u\ell_2\ell_0 + v\ell_1\ell_2 = \ell_2(u\ell_0 + v\ell_1).$$

  Die Menge der Basispunkte ist dann

  $$\{\ell_2 = 0\} \cup \{\ell_0 = \ell_1 = 0\}.$$

  Die Menge besteht also aus einer Geraden und einem Punkt, wobei der Punkt aber auch auf der Geraden liegen kann.
- **Fall ℓ_1 und ℓ_2 sind keine Teiler von g:** Da eine Gerade $\ell_i = 0$ die Quadrik $g = 0$ in einem oder in zwei Punkten schneidet, besteht

  $$\{g = h = 0\} = \{g = \ell_1 = 0\} \cup \{g = \ell_2 = 0\}$$

  mindestens aus einem, aber höchstens aus vier Punkten.

Wir fassen das Ergebnis zusammen:

SATZ. *Ist $f_{(u,v)} = 0$ ein Büschel ebener projektiver Quadriken, so gibt es für die Menge der Basispunkte B folgende Möglichkeiten:*

- *B besteht aus den Punkten einer Geraden.*
- *B besteht aus den Punkten einer Geraden und einem zusätzlichen Punkt.*
- *B ist endlich mit*

$$\#B \in \{1, 2, 3, 4\}.$$

Wir geben eine Anwendung:

SATZ. *Zwei ebene projektive Quadriken $C_1, C_2 \subseteq \mathbb{P}^2$ ohne gemeinsame Komponente schneiden sich in 1, 2, 3 oder 4 Punkten, d.h.*

$$C_1(K) \cap C_2(K) \in \{1, 2, 3, 4\}.$$

Beweis: Sei C_1 gegeben durch $g = 0$, C_2 durch $h = 0$. Dann ist

$$C_1(K) \cap C_2(K) = \{g = h = 0\}.$$

Wir betrachten das Büschel $f_{(u,v)} = ug + vh$. Da C_1 und C_2 keine gemeinsame Komponente haben sollen, haben g und h keinen gemeinsamen Teiler. Im letzten Satz bleibt nur die letzte Möglichkeit: Das durch $f_{(u,v)} = ug + vh$ definierte Büschel hat dann 1, 2, 3 oder 4 Basispunkte, die genau die Punkte von $C_1(K) \cap C_2(K)$ sind. ■

Büschel mit genau 4 Basispunkten:

- Das durch $f_{(u,v)} = ug+vh$ definierte Büschel besitze genau 4 verschiedene Basispunkte P_1, P_2, P_3, P_4. Wir zeigen zunächst, dass keine der 3 Punkte auf einer Geraden liegen können.
- Angenommen P_1, P_2, P_3 liegen auf der Geraden $\ell = 0$. Die Gerade $\ell = 0$ schneidet dann $g = 0$ und $h = 0$ in mehr als 2 Punkten, weswegen die Gerade Teil der Quadriken $g = 0$ und $h = 0$ ist: $g = \ell\ell_g$ und $h = \ell\ell_h$. Alle Punkte der Geraden $\ell = 0$ sind Basispunkte, was aber der Voraussetzung, dass es genau 4 Basispunkte gibt, widerspricht.
- Also liegen keine drei Punkte von P_1, P_2, P_3, P_4 auf einer Geraden. Nach Koordinatenwechsel können wir

  $$P_1 = (1:0:0), \quad P_2 = (0:1:0), \quad P_3 = (0:0:1), \quad P_4 = (1:1:1)$$

  annehmen. Welche durch

  $$\widetilde{f} = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

  definierten Quadriken gehen durch P_1, P_2, P_3, P_4? Es ist

  $$f(P_1) = a_0, \quad f(P_2) = a_3, \quad f(P_3) = a_5, \quad f(P_4) = a_0 + a_1 + a_2 + a_3 + a_4 + a_5.$$

  Daher gilt:

  $$f(P_1) = f(P_2) = f(P_3) = f(P_4) = 0 \iff a_0 = a_3 = a_5 = 0 \text{ und } a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = 0 \iff$$
  $$\iff a_0 = a_3 = a_5 = 0 \text{ und } a_4 = -a_1 - a_2.$$

  Die Quadriken, die durch die 4 Punkte gehen, sind also genau die Quadriken, die durch ein Polynom folgender Gestalt definiert werden:

  $$\widetilde{f} = a_1x_0x_1 + a_2x_0x_2 + (-a_1 - a_2)x_1x_2.$$

  Dies sind also genau die Quadriken des Büschels

  $$f_{(u,v)} = ux_0x_1 + vx_0x_2 + (-u - v)x_1x_2 = u(x_0x_1 - x_1x_2) + v(x_0x_2 - x_1x_2).$$

- Wir haben also gezeigt, dass zu Punkten P_1, P_2, P_3, P_4, von denen keine drei auf einer Geraden liegen, genau ein Büschel mit den Basispunkten P_1, P_2, P_3, P_4 existiert.
- Welche reduziblen Kurven enthält das durch

  $$f_{(u,v)} = ux_0x_1 + vx_0x_2 + (-u - v)x_1x_2$$

  definierte Büschel? Wir bilden die Hesse-Matrix:

  $$A_{f_{(u,v)}} = \begin{pmatrix} 0 & u & v \\ u & 0 & -u-v \\ v & -u-v & 0 \end{pmatrix}.$$

Es ist

$$\det(A_{f_{(u,v)}}) = -2uv(u+v).$$

Die Nullstellen sind $(u:v) = (0:1), (1:0), (1:-1)$. Die zugehörigen Kurven des Büschels sind:

$$\begin{aligned} f_{(0,1)} &= x_0x_2 - x_1x_2 = (x_0 - x_1)x_2, \\ f_{(1,0)} &= x_0x_1 - x_1x_2 = (x_0 - x_2)x_1, \\ f_{(1,-1)} &= x_0x_1 - x_0x_2 = (x_1 - x_2)x_0. \end{aligned}$$

- Zur Erinnerung:

$$P_1 = (1:0:0), \quad P_2 = (0:1:0), \quad P_3 = (0:0:1), \quad P_4 = (1:1:1).$$

Setzt man

$$\ell_{1,2} = x_2, \ell_{1,3} = x_1, \ell_{1,4} = x_1 - x_2, \ell_{2,3} = x_0, \ell_{2,4} = x_0 - x_2, \ell_{3,4} = x_0 - x_1,$$

so ist $\ell_{i,j}$ die Verbindungsgerade von P_i und P_j und

$$f_{(0,1)} = \ell_{1,2}\ell_{3,4}, \quad f_{(1,0)} = \ell_{1,3}\ell_{2,4}, \quad f_{(1,-1)} = \ell_{1,4}\ell_{2,3}.$$

Wir formulieren das Ergebnis als Satz:

SATZ. *Seien $P_1, P_2, P_3, P_4 \in \mathbb{P}^2$ vier verschiedene Punkte, von denen keine drei auf einer Geraden liegen. Für $1 \le i < j \le 4$ sei $\ell_{i,j}$ eine Linearform, sodass $\ell_{i,j} = 0$ die Verbindungsgerade von P_i und P_j ist. Es gibt genau ein Büschel von Quadriken $f_{(u,v)} = 0$, das die Punkte P_1, P_2, P_3, P_4 als Basispunkte hat. Das Büschel enthält genau drei reduzible Kurven, nämlich*

$$\ell_{1,2}\ell_{3,4} = 0, \quad \ell_{1,3}\ell_{2,4} = 0, \quad \ell_{1,4}\ell_{2,3} = 0.$$

Insbesondere kann man (nach eventuellem Koordinatenwechsel im parametrisierenden $\mathbb{P}^1$) schreiben

$$f_{(u,v)} = u\ell_{1,2}\ell_{3,4} + v\ell_{1,3}\ell_{2,4}.$$

9. Geometrische Bedingungen an Quadriken

Wir setzen hier einen algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2$ voraus.
Eine projektive ebene Quadrik wird gegeben durch ein Polynom

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0, x_1, x_2] \setminus \{0\}.$$

Bilden wir die Hesse-Matrix

$$A_f = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix},$$

so ist

$$f = \frac{1}{2}\begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix}\begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Der Rang von A_f wird auch als Rang der Quadrik bezeichnet. Die zu f gehörige Quadrik bestimmt f nur bis auf einen Skalar. Dann ist $(a_0 : a_1 : \cdots : a_5)$ ein Punkt eines $\mathbb{P}^5$. Die Zuordnung ist bijektiv, d.h. wir haben eine Bijektion

$$\text{Quadriken } \subseteq \mathbb{P}^2 \longleftrightarrow \text{ Punkte } \in \mathbb{P}^5.$$

Wir wollen nun ein paar Teilmengen dieses $\mathbb{P}^5$ betrachten.
Die Menge R der singulären bzw. reduziblen Quadriken: Wir wissen:

$$\begin{aligned} f \text{ definiert eine singuläre Quadrik} &\iff \operatorname{Rang}(A_f) \le 2 \iff \\ &\iff \det(A_f) = 0 \iff \\ &\iff f \text{ zerfällt in 2 Linearfaktoren.} \end{aligned}$$

Nun ist

$$\det(A_f) = 8a_0a_3a_5 + 2a_1a_2a_4 - 2a_2^3 - 2a_0a_4^2 - 2a_1^2a_5.$$

Ist nun R die Menge der reduziblen Kegelschnitte in $\mathbb{P}^2$, so ist also

$$R = \{4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 = 0\} \subseteq \mathbb{P}^5.$$

R ist eine algebraische Teilmenge von $\mathbb{P}^5$, genauer: eine kubische Hyperfläche.
Die Menge D der Doppelgeraden: f beschreibt eine Doppelgerade, wenn gilt $f = (b_0x_0+b_1x_1+b_2x_2)^2$. Dies ist genau dann der Fall, wenn $\mathrm{Rang}(A_f) = 1$ gilt. Dies läßt sich dadurch ausdrücken, dass alle 2×2-Unterdeterminanten von

$$A_f = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}$$

verschwinden. Also ergibt sich

$$\begin{aligned} D &= \{ \text{ Doppelgeraden } \} = \\ &= \big\{4a_0a_3 - a_1^2 = 0, 4a_0a_5 - a_2^2 = 0, 4a_3a_5 - a_4^2 = 0, \\ &\qquad 2a_0a_4 - a_1a_2 = 0, 2a_1a_5 - a_2a_4 = 0, 2a_2a_3 - a_1a_4 = 0\big\}. \end{aligned}$$

D ist also auch eine algebraische Teilmenge von $\mathbb{P}^5$, die natürlich in R enthalten ist.
Quadriken durch vorgegebene Punkte:
Gegeben sei ein Punkt $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2$. Für

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

gilt:

$$f(P) = 0 \quad \Longleftrightarrow \quad a_0p_0^2 + a_1p_0p_1 + a_2p_0p_2 + a_3p_1^2 + a_4p_1p_2 + a_5p_2^2 = 0.$$

Bei gegebenem Punkt P wird also die Menge der Quadriken, die durch diesen Punkt gehen, beschrieben durch die (in $a_0, \ldots, a_5$ lineare) Gleichung

$$a_0p_0^2 + a_1p_0p_1 + a_2p_0p_2 + a_3p_1^2 + a_4p_1p_2 + a_5p_2^2 = 0.$$

Wir geben uns nun Punkte $P_1, P_2, P_3, \ldots$ vor und wollen alle Quadriken bestimmen, die durch diese Punkte gehen.
Jeder Punkt liefert für $a_0, \ldots, a_5$ eine lineare Gleichung.
Quadriken durch 5 vorgegebene Punkte: Seien $P_1, \ldots, P_5 \in \mathbb{P}^2$ gegeben. Wir schreiben $P_i = (p_{i,0} : p_{i,1} : p_{i,2})$. Eine Quadrik, die durch das Polynom

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

gegeben wird, geht durch alle 5 Punkte, wenn gilt

$$\begin{pmatrix} p_{1,0}^2 & p_{1,0}p_{1,1} & p_{1,0}p_{1,2} & p_{1,1}^2 & p_{1,1}p_{1,2} & p_{1,2}^2 \\ p_{2,0}^2 & p_{2,0}p_{2,1} & p_{2,0}p_{2,2} & p_{2,1}^2 & p_{2,1}p_{2,2} & p_{2,2}^2 \\ p_{3,0}^2 & p_{3,0}p_{3,1} & p_{3,0}p_{3,2} & p_{3,1}^2 & p_{3,1}p_{3,2} & p_{3,2}^2 \\ p_{4,0}^2 & p_{4,0}p_{4,1} & p_{4,0}p_{4,2} & p_{4,1}^2 & p_{4,1}p_{4,2} & p_{4,2}^2 \\ p_{5,0}^2 & p_{5,0}p_{5,1} & p_{5,0}p_{5,2} & p_{5,1}^2 & p_{5,1}p_{5,2} & p_{5,2}^2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = 0$$

Der Lösungsraum ist mindestens 1-dimensional, was projektiv einem Punkt entspricht. Daher geht durch 5 Punkte mindestens eine Quadrik.
Wir unterscheiden verschiedene Fälle:

- **Fall: Alle 5 Punkte liegen auf einer Geraden:** Sei $\ell = 0$ die Gerade, auf der die Punkte liegen. Sei $f = 0$ eine Quadrik, die die 5 Punkte enthält. Da $\{f = 0\} \cap \{\ell = 0\}$ mindestens 5 Punkte enthält, ist f eine Komponente von ℓ. Die Quadriken durch die 5 Punkte werden also durch die Polynome

  $$f = \ell \cdot (b_0x_0 + b_1x_1 + b_2x_2)$$

  gegeben.
- **Fall: Vier der Punkte liegen auf einer Geraden, der fünfte aber nicht:** Seien ℓ_0, ℓ_1 zwei verschiedene Geraden durch den 5. Punkt. Dann werden die Quadriken gegeben durch

  $$f = \ell \cdot (t_0\ell_0 + t_1\ell_1).$$

  Es gibt also ein ganzes Büschel von Quadriken durch die 5 Punkte.

- **Fall: Drei der Punkte liegen auf einer Geraden, aber keine vier der Punkte:** Seien P_1, P_2, P_3 die Punkte, die auf einer Geraden $\ell_1 = 0$ liegen. Ist $\ell_2 = 0$ die Gerade durch P_4, P_5, so wird die Quadrik durch die 5 Punkte beschrieben durch
$$f = \ell_1 \ell_2.$$
- **Fall: Keine drei der Punkte liegen auf einer Geraden:** Angenommen, es gäbe mehr als eine Quadrik durch die 5 Punkte. Dann gäbe es ein Büschel durch die Punkte, daher auch eine reduzible Quadrik $\ell_1 \ell_2 = 0$. Daher gilt
$$P_1, P_2, P_3, P_4, P_5 \in \{\ell_1 = 0\} \cup \{\ell_2 = 0\}.$$
Daher müssen drei der Punkte auf einer Geraden liegen, was aber der Voraussetzung widerspricht. Daher gibt es nur eine Quadrik durch die 5 Punkte, die außerdem irreduzibel ist.

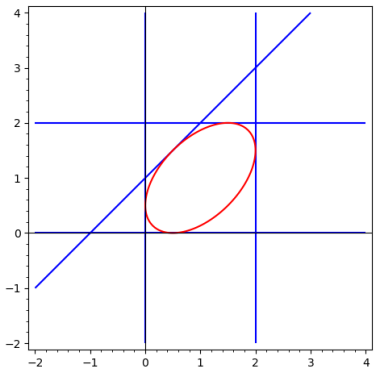
Geometrische Bedingungen: Die vorangegangenen Betrachtungen kann man verallgemeinern. Man sucht dann alle Quadriken, die bestimmte Bedingungen erfüllen.

Beispiel: Sind $P_1, P_2, P_3, P_4, P_5 \in \mathbb{P}^2$ fünf Punkte, von denen keine vier auf einer Geraden liegen, so gibt es genau eine Quadrik, die durch alle fünf Punkte geht. (Dies haben wir zuvor gezeigt.)

Beispiel:

- Für eine Gerade $g \subseteq \mathbb{P}^2$ sei τ_g die Menge aller Quadriken, die g berühren.
- Wir betrachten als Beispiel die Gerade g mit der Gleichung $x_0 = 0$. Wir schneiden g mit der durch $a_0 x_0^2 + a_1 x_0 x_1 + \cdots + a_5 x_2^2 = 0$ definierten Quadrik, indem wir $x_0 = 0$ einsetzen: $a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2 = 0$. Die Quadrik berührt die Gerade, wenn es genau einen Schnittpunkt gibt, d.h. wenn gilt $a_4^2 - 4a_3 a_5 = 0$ (Diskriminantenbedingung). Also folgt
$$\tau_{\{x_0=0\}} = \{(a_0 : a_1 : a_2 : a_3 : a_4 : a_5) \in \mathbb{P}^2 : a_4^2 - 4a_3 a_5 = 0\},$$
d.h. τ_g bildet eine quadratische Hyperfläche im $\mathbb{P}^5$.

Beispiel: Hat man die 5 Geraden
$$x = 0, \quad x = 2, \quad y = 0, \quad y = 2, \quad y = x + 1$$
gegeben, so ist die Menge der Quadriken, die diese Geraden berühren
$$\{1 - 4x - 4y + 4x^2 - 4xy + 4y^2 = 0\} \cup D.$$
Die Doppelgeraden kommen ins Spiel, weil $D \subseteq \tau_g$ gilt.



Wir schließen mit einem weiterführenden Problem:

Steiners Kegelschnitt-Problem: Jakob Steiner stellte 1848 die Frage, wieviele nichtsinguläre Kegelschnitte es gibt, die 5 vorgegebene Kegelschnitte „in allgemeiner Lage“ berühren. Nach verschiedenen Irrtümern beim Zählen ist man sich heute einig, dass die richtige Zahl $\boxed{3264}$ ist.

KAPITEL 5

Funktionen, Divisoren und der Satz von Riemann-Roch auf $\mathbb{P}^1$

Der Einfachkeit halber setzen wir in diesem Kapitel voraus, dass K ein algebraisch abgeschlossener Körper ist. Dies hat den Vorteil, dass sich jedes Polynom $f \in K[x] \setminus \{0\}$ in der Form

$$f(x) = c \cdot (x - \alpha_1)^{n_1} \dots (x - \alpha_r)^{n_r}$$

schreiben lässt mit $c \in K^*$, paarweise verschiedenen $\alpha_i \in K$, $n_i \in \mathbb{N}$ und $r \in \mathbb{N}_0$.

1. Funktionen auf $\mathbb{P}^1$

Überlegungen: Wir starten mit

$$\mathbb{P}^1 = \{(p_0 : p_1) : (p_0, p_1) \in K^2 \setminus \{(0,0)\}\}.$$

Sei $A(x_0, x_1) \in K[x_0, x_1]$ ein homogenes Polynom vom Grad d, d.h.

$$A(x_0, x_1) = \sum_{i=0}^{d} a_i x_0^{d-i} x_1^i.$$

Dann gilt

$$A(\lambda x_0, \lambda x_1) = \lambda^d A(x_0, x_1).$$

Das Polynom A können wir (im Fall $d \geq 1$) nicht als Funktion auf $\mathbb{P}^1$ auffassen, da die Repräsentanten (p_0, p_1) und $(\lambda p_0, \lambda p_1)$ eines Punktes im Allgemeinen verschiedene Werte liefern:

$$A(\lambda p_0, \lambda p_1) = \lambda^d A(p_0, p_1).$$

Ist $B(x_0, x_1)$ ein weiteres homogenes Polynom vom Grad d, so gilt natürlich auch

$$B(\lambda p_0, \lambda p_1) = \lambda^d B(p_0, p_1).$$

Ist nun $B(p_0, p_1) \neq 0$, so folgt

$$\frac{A(p_0, p_1)}{B(p_0, p_1)} = \frac{A(\lambda p_0, \lambda p_1)}{B(\lambda p_0, \lambda p_1)},$$

d.h. der Wert von

$$\frac{A(p_0, p_1)}{B(p_0, p_1)}$$

hängt nur von $P = (p_0 : p_1)$ und nicht vom ausgewählten Repräsentanten ab. Daher definiert

$$\frac{A(x_0, x_1)}{B(x_0, x_1)}$$

eine Funktion auf (einer Teilmenge von) $\mathbb{P}^1$, wobei natürlich $B(x_0, x_1)$ nicht das Nullpolynom sein sollte.

DEFINITION. *Wir definieren den* **Funktionenkörper** $K(\mathbb{P}^1)$ *von* $\mathbb{P}^1$ *über* K *als*

$$K(\mathbb{P}^1) \quad = \quad \{\frac{A(x_0, x_1)}{B(x_0, x_1)} : A(x_0, x_1), B(x_0, x_1) \in K[x_0, x_1], B(x_0, x_1) \neq 0,$$
$$A, B \text{ homogene Polynome gleichen Grades}\}.$$

Datei: algku5.tex. Version vom 19.7.2021

Man rechnet in $K(\mathbb{P}^1)$ wie mit Brüchen:

$$\begin{aligned}
\frac{A(x_0,x_1)}{B(x_0,x_1)} = \frac{\widetilde{A}(x_0,x_1)}{\widetilde{B}(x_0,x_1)} \quad &\Longleftrightarrow \quad A(x_0,x_1)\widetilde{B}(x_0,x_1) = \widetilde{A}(x_0,x_1)B(x_0,x_1) \quad \text{in } K[x_0,x_1],\\
\frac{A(x_0,x_1)}{B(x_0,x_1)} + \frac{\widetilde{A}(x_0,x_1)}{\widetilde{B}(x_0,x_1)} \quad &= \quad \frac{A(x_0,x_1)\widetilde{B}(x_0,x_1) + \widetilde{A}(x_0,x_1)B(x_0,x_1)}{B(x_0,x_1)\widetilde{B}(x_0,x_1)}, \quad B(x_0,x_1)\neq 0, \widetilde{B}(x_0,x_1)\neq 0,\\
\frac{A(x_0,x_1)}{B(x_0,x_1)} \cdot \frac{\widetilde{A}(x_0,x_1)}{\widetilde{B}(x_0,x_1)} \quad &= \quad \frac{A(x_0,x_1)\widetilde{A}(x_0,x_1)}{B(x_0,x_1)\widetilde{B}(x_0,x_1)}, \quad B(x_0,x_1)\neq 0, \widetilde{B}(x_0,x_1)\neq 0,\\
\left(\frac{A(x_0,x_1)}{B(x_0,x_1)}\right)^{-1} \quad &= \quad \frac{B(x_0,x_1)}{A(x_0,x_1)}, \quad A(x_0,x_1)\neq 0, B(x_0,x_1)\neq 0.
\end{aligned}$$

Damit gilt:

SATZ. *Der Funktionenkörper $K(\mathbb{P}^1)$ ist mit der oben beschriebenen Addition und Multiplikation ein Körper. Nullelement ist das konstante Polynom 0, Einselement ist das konstante Polynom 1.*

Wann ist eine Funktion $f \in K(\mathbb{P}^1)$ in einem Punkt $P = (p_0 : p_1) \in \mathbb{P}^1$ definiert? Wir schreiben $f(x_0,x_1) = \frac{A(x_0,x_1)}{B(x_0,x_1)}$, wo $A(x_0,x_1)$ und $B(x_0,x_1)$ homogene Polynome gleichen Grades sind und $B(x_0,x_1)$ nicht das Nullpolynom ist. Wir unterscheiden drei Fälle:

- **Fall $B(p_0,p_1)\neq 0$:** Dann definiert man
$$f(P) = \frac{A(p_0,p_1)}{B(p_0,p_1)}.$$
Wir sagen, f **ist in P definiert**.
- **Fall $B(p_0,p_1) = 0$ und $A(p_0,p_1)\neq 0$:** Dann ist f **nicht in P definiert**.
- **Fall $B(p_0,p_1) = 0$ und $A(p_0,p_1) = 0$:** Da K algebraisch abgeschlossen ist, zerfallen A und B in Linearfaktoren:
$$A(x_0,x_1) = \prod_{i=1}^{d}(a_ix_0 - b_ix_1) \quad \text{und} \quad B(x_0,x_1) = \prod_{j=1}^{d}(c_jx_0 - d_jx_1).$$
Wegen $A(p_0,p_1) = B(p_0,p_1) = 0$ gibt es Indizes i,j mit
$$a_ip_0 - b_ip_1 = 0 \quad \text{und} \quad c_jp_0 - d_jp_1 = 0.$$
Es folgt (zunächst für $b_i\neq 0$)
$$(p_0:p_1) = (b_ip_0 : b_ip_1) = (b_ip_0 : a_ip_0) = (b_i : a_i) \quad \text{und analog} \quad (p_0:p_1) = (d_j : c_j).$$
Es gibt also $\lambda,\mu \in K^*$ mit $(b_i,a_i) = \lambda(p_0,p_1)$ und $(d_j,c_j) = \mu(p_0,p_1)$, was zu
$$a_ix_0 - b_ix_1 = \lambda(p_1x_0 - p_0x_1) \quad \text{und} \quad c_jx_0 - d_jx_1 = \mu(p_1x_0 - p_0x_1)$$
führt. Die Linearfaktoren $a_ix_0 - b_ix_1$ und $c_jx_0 - d_jx_1$ unterscheiden sich also nur um eine Zahl aus K^* und können daher herausgekürzt werden. Wiederholt man dies bei Bedarf, erreicht man schließlich $(A(p_0,p_1),B(p_0,p_1))\neq(0,0)$ und ist dann bei einem der ersten beiden Fälle.

Beispiele: Wir betrachten
$$f = \frac{2x_0^2 + x_0x_1 - 3x_1^2}{x_0^2 - 3x_0x_1 + 2x_1^2}.$$
Wie verhält sich f im Punkt $P = (1:1)$? Man findet $A(1,1) = B(1,1) = 0$, weswegen sowohl A als auch B durch einen Faktor $x_0 - x_1$ teilber sein sollten. Nun ist
$$f = \frac{(x_0-x_1)(2x_0+3x_1)}{(x_0-x_1)(x_0-2x_1)} = \frac{2x_0+3x_1}{x_0-2x_1} \quad \text{und} \quad f(P) = \frac{5}{-1} = -5,$$
d.h. f ist in $(1:1)$ definiert und nimmt dort den Wert -5 an.

Aus der Definition von Addition und Multiplikation folgt sofort:

LEMMA. *Sind $f,g \in K(\mathbb{P}^1)$ in einem Punkt $P \in \mathbb{P}^1$ definiert, so auch $f+g$ und fg.*

Die Funktionen x und u: Wir betrachten zwei spezielle Funktionen:

$$x = \frac{x_1}{x_0} \quad \text{und} \quad u = \frac{x_0}{x_1}.$$

x ist einfach die übliche Koordinatenfunktion im affinen Teil

$$U_0 = \{(1 : x) \in \mathbb{P}^1\} \simeq \mathbb{A}^1.$$

Es gilt dann:

$$x(P) = \begin{cases} p & \text{für } P = (1 : p), \\ \text{nicht definiert} & \text{in } P = (0 : 1). \end{cases}$$

u ist die Koordinatenfunktion im affinen Teil

$$U_1 = \{(u : 1) \in \mathbb{P}^1\} \simeq \mathbb{A}^1.$$

Es gilt:

$$u(P) = \begin{cases} \text{nicht definiert} & \text{in } P = (1 : 0), \\ \frac{1}{p} & \text{für } P = (1 : p) \text{ mit } p \neq 0, \\ 0 & \text{für } P = (0 : 1). \end{cases}$$

Mit Hilfe der Funktionen $x = \frac{x_1}{x_0}$ und $u = \frac{x_0}{x_1}$ können wir alle Funktionen des Funktionenkörpers beschreiben: Seien $A(x_0, x_1), B(x_0, x_1)$ homogen vom Grad d und $B(x_0, x_1) \neq 0$. Wir schreiben

$$A(x_0, x_1) = \sum_{i=0}^{d} a_i x_0^{d-i} x_1^i, \quad B(x_0, x_1) = \sum_{i=0}^{d} b_i x_0^{d-i} x_1^i.$$

Es ist

$$A(x_0, x_1) = \sum_{i=0}^{d} a_i x_0^d (\frac{x_1}{x_0})^i = x_0^d \sum_{i=0}^{d} a_i x^i \quad \text{und analog} \quad B(x_0, x_1) = x_0^d \sum_{i=0}^{d} b_i x^i.$$

Es folgt

$$\frac{A(x_0, x_1)}{B(x_0, x_1)} = \frac{x_0^d \sum_{i=0}^{d} a_i x^i}{x_0^d \sum_{i=0}^{d} b_i x^i} = \frac{\sum_{i=0}^{d} a_i x^i}{\sum_{i=0}^{d} b_i x^i} = \frac{A(1, x)}{B(1, x)}.$$

Ganz analog zeigt man für $u = \frac{x_0}{x_1}$

$$\frac{A(x_0, x_1)}{B(x_0, x_1)} = \frac{A(u, 1)}{B(u, 1)}.$$

Wir fassen dies zusammen:

LEMMA. *Sind $A(x_0, x_1), B(x_0, x_1) \in K[x_0, x_1]$ homogene Polynome gleichen Grad mit $B(x_0, x_1) \neq 0$, so gilt*

$$\frac{A(x_0, x_1)}{B(x_0, x_1)} = \frac{A(1, x)}{B(1, x)} = \frac{A(u, 1)}{B(u, 1)}.$$

Insbesondere gilt dann

$$K(\mathbb{P}^1) = \{\frac{p(x)}{q(x)} : p(x), q(x) \in K[x], q(x) \neq 0\}.$$

Bemerkung: Für den Polynomring in der Variablen x mit Koeffizienten aus K schreibt man

$$K[x].$$

Für den Quotientenkörper schreibt man

$$K(x) = \{\frac{p(x)}{q(x)} : p(x), q(x) \in K[x], q(x) \neq 0\}.$$

Dann gilt also

$$K(\mathbb{P}^1) = K(x).$$

Dies erklärt eventuell die etwas ungewöhnliche Schreibweise für den Funktionenkörper von $\mathbb{P}^1$. Man nennt $K(\mathbb{P}^1) = K(x)$ auch den rationalen Funktionenkörper.

Beispiele: Wir rechnen zunächst ausführlich:

$$\begin{aligned} f &= \frac{2x_0^2 + x_0x_1 - 3x_1^2}{x_0^2 - 3x_0x_1 + 2x_1^2} = \frac{x_0^2 \cdot (2 + \frac{x_1}{x_0} - 3(\frac{x_1}{x_0})^2)}{x_0^2 \cdot (1 - 3\frac{x_1}{x_0} + 2(\frac{x_1}{x_0})^2)} = \\ &= \frac{2 + x - 3x^2}{1 - 3x + 2x^2} = \frac{(x-1)(-3x-2)}{(x-1)(2x-1)} = \frac{-3x-2}{2x-1}. \end{aligned}$$

Nun kürzer, in dem wir für (x_0, x_1) einfach $(1, x)$ bzw. $(u, 1)$ einsetzen:

$$g = \frac{x_0^2 + 2x_0x_1 + 3x_1^2}{3x_0^2 + 2x_0x_1 + x_1^2} = \frac{1 + 2x + 3x^2}{3 + 2x + x^2} = \frac{u^2 + 2u + 3}{3u^2 + 2u + 1}.$$

Wir wollen noch sehen, wie man aus einer rationalen Funktion in x eine Darstellung als Quotient homogener Polynome gleichen Grades erhält. Sei

$$f = \frac{p(x)}{q(x)}.$$

Dabei sei

$$p(x) = p_m x^m + p_{m-1}x^{m-1} + \cdots + p_0, \quad q(x) = q_n x^n + q_{n-1}x^{n-1} + \cdots + q_0.$$

Wir nehmen an, dass $p_m \neq 0$ und $q_n \neq 0$ gilt, d.h. $p(x)$ hat Grad m und $q(x)$ hat Grad n. Dann folgt

$$\begin{aligned} f &= \frac{p_m x^m + p_{m-1}x^{m-1} + \cdots + p_0}{q_n x^n + q_{n-1}x^{n-1} + \cdots + q_n} = \frac{p_m(\frac{x_1}{x_0})^m + p_{m-1}(\frac{x_1}{x_0})^{m-1} + \cdots + p_0}{q_n(\frac{x_1}{x_0})^n + q_{n-1}(\frac{x_1}{x_0})^{n-1} + \cdots + q_0} = \\ &= \frac{x_0^n}{x_0^m} \cdot \frac{p_m x_1^m + p_{m-1}x_0x_1^{m-1} + \cdots + p_0x_0^m}{q_n x_1^n + q_{n-1}x_0x_1^{n-1} + \cdots + q_0x_0^n} = \\ &= \frac{x_0^n \cdot (p_m x_1^m + p_{m-1}x_0x_1^{m-1} + \cdots + p_0x_0^m)}{x_0^m \cdot (q_n x_1^n + q_{n-1}x_0x_1^{n-1} + \cdots + q_0x_0^n)}. \end{aligned}$$

In der letzten Darstellung hat man f als Quotienten homogener Polynome vom Grad $m+n$ geschrieben. Natürlich sollte man noch Potenzen von x_0 kürzen, soweit möglich.
Es ist

$$\mathbb{P}^1 = \{(p_0 : p_1) : (p_0, p_1) \in K^2 \setminus \{(0,0)\}\} = \{(1 : p) : p \in K\} \cup \{(0 : 1)\}.$$

Identifizieren wir $(1 : p)$ mit p, schreiben wir $\infty = (0 : 1)$, so ist

$$\mathbb{P}^1 \simeq K \cup \{\infty\}.$$

Mit diesen Abkürzungen gilt für $x = \frac{x_1}{x_0}$ und $u = \frac{x_0}{x_1}$:

$$x \text{ ist nicht definiert in } \infty, \quad x(\alpha) = \alpha \text{ für } \alpha \in K$$

und

$$u \text{ ist nicht definiert in } 0 \in K, \quad u(\alpha) = \frac{1}{\alpha} \text{ für } \alpha \in K \setminus \{0\}, \quad u(\infty) = 0.$$

2. Ordnung (Bewertung) einer Funktion in einem Punkt

Sei $f(x) \in K(x)$ und $P \in \mathbb{P}^1$. Wir schreiben $f(x) = \frac{p(x)}{q(x)}$ mit Polynomen $p(x), q(x) \in K[x] \setminus \{0\}$. (Beide Polynome seien von 0 verschieden.) Wir betrachten das Verhalten von f in den Punkten von $\mathbb{P}^1$.

- **Fall** $P = (1 : \alpha) \simeq \alpha$**:** Dabei ist $\alpha \in K$. Wir klammern $x - \alpha$ so oft wie möglich aus:

$$p(x) = (x-\alpha)^{e_p}\widetilde{p}(x) \text{ mit } \widetilde{p}(\alpha) \neq 0$$

und

$$q(x) = (x-\alpha)^{e_q}\widetilde{q}(x) \text{ mit } \widetilde{q}(\alpha) \neq 0.$$

Setzen wir

$$e = e_p - e_q \text{ und } g(x) = \frac{\widetilde{p}(x)}{\widetilde{q}(x)},$$

so gilt

$$f(x) = (x-\alpha)^e \cdot g(x), \text{ wobei } g \text{ in } \alpha \text{ definiert ist und } g(\alpha) \neq 0 \text{ gilt.}$$

Wir nennen e **die Ordnung von f in α** und schreiben

$$\operatorname{ord}_\alpha(f) = e.$$

(Statt Ordnung findet man auch die Bezeichnung **Bewertung** und $v_\alpha(f)$.) Ist $e \geq 0$, so ist f in α definiert. Wir nennen die Funktion $x - \alpha$ auch eine **Uniformisierende im Punkt** α. Es gibt drei Fälle:

- **Fall $e > 0$:** Dann ist $f(\alpha) = 0$. Die Funktion f hat in α eine **Nullstelle der Ordnung** $e = \operatorname{ord}_\alpha(f)$.
- **Fall $e = 0$:** Dann gilt $f(\alpha) = g(\alpha) \neq 0$.
- **Fall $e < 0$:** Die Funktion f ist in α nicht definiert. Man sagt, f hat in α einen **Pol der Ordnung** $|\operatorname{ord}_\alpha(f)| = -\operatorname{ord}_\alpha(f)$.

- **Fall $P = (0:1) \simeq \infty$:** Wir schreiben

$$p(x) = p_0 + p_1 x + \cdots + p_m x^m, \quad q(x) = q_0 + q_1 x + \cdots + q_n x^n \text{ mit } p_m \neq 0, q_n \neq 0.$$

Wegen $xu = 1$ folgt

$$f(x) = \frac{u^n}{u^m} \cdot \frac{u^m(p_0 + p_1 x + \cdots + p_m x^m)}{u^n(q_0 + q_1 x + \cdots + q_n x^n)} = u^{n-m} \cdot \frac{p_0 u^m + p_1 u^{m-1} + \cdots + p_m}{q_0 u^n + q_1 u^{n-1} + \cdots + q_n}.$$

Wegen $u(\infty) = 0$ ist die Funktion

$$g(x) = \frac{p_0 u^m + p_1 u^{m-1} + \cdots + p_m}{q_0 u^n + q_1 u^{n-1} + \cdots + q_n}$$

in ∞ definiert und hat den Wert $g(\infty) = \frac{p_m}{q_n} \neq 0$.

Wir haben die Zerlegung

$$f = u^{n-m} \cdot g.$$

Wir nennen $n - m$ die Ordnung von f in ∞ und schreiben

$$\operatorname{ord}_\infty(f) = n - m.$$

Die Funktion $u = \frac{1}{x}$ wird eine **Uniformisierende im Punkt** ∞ genannt. Wir unterscheiden drei Fälle:

- **Fall $m < n$, also $\operatorname{ord}_\infty(f) > 0$:** Dann ist $f(\infty) = 0$. Die Funktion f hat in ∞ eine **Nullstelle der Ordnung** $\operatorname{ord}_\infty(f) = n - m$.
- **Fall $m = n$, also $\operatorname{ord}_\infty(f) = 0$:** Dann gilt $f(\infty) = \frac{p_m}{q_n} \neq 0$.
- **Fall $m > n$, also $\operatorname{ord}_\infty(f) < 0$:** Die Funktion f ist in ∞ nicht definiert. Man sagt, f hat in ∞ einen **Pol der Ordnung** $|\operatorname{ord}_\infty(f)| = -\operatorname{ord}_\alpha(f) = m - n$.

Wir fassen dies nochmals zusammen:

LEMMA. *Definiert man für $P \in \mathbb{P}^1$*

$$u_P = \begin{cases} x - \alpha & \text{für } P = (1:\alpha) \simeq \alpha, \quad \alpha \in K, \\ u = \frac{1}{x} & \text{für } P = (0:1) \simeq \infty, \end{cases}$$

so lässt sich jede Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ schreiben als

$$f = u_P^e \cdot g,$$

wobei g in P definiert ist mit $g(P) \neq 0$ und $e \in \mathbb{Z}$ gilt. e heißt die Ordnung von f in P, $\operatorname{ord}_P(f) = e$. Es ist $u_P(P) = 0$. (u_P ist eine Uniformisierende im Punkt P.)

- **Fall $e > 0$:** *f ist in P definiert mit $f(P) = 0$. f hat in P eine Nullstelle der Ordnung e.*
- **Fall $e = 0$:** *f ist in P definiert mit $f(P) \neq 0$.*
- **Fall $e < 0$:** *f ist in P nicht definiert. f hat in P einen Pol der Ordnung $|e| = -e$.*

Es gilt:

$$\begin{aligned} \operatorname{ord}_P(f) = 0 \quad &\iff \quad f \text{ hat in } P \text{ weder eine Nullstelle noch eine Polstelle} \quad \iff \\ &\iff \quad f \text{ ist in } P \text{ definiert mit } f(P) \neq 0. \end{aligned}$$

SATZ (Eigenschaften der Ordnungsfunktion). *Für $P \in \mathbb{P}^1$ und $f, g \in K(\mathbb{P}^1) \setminus \{0\}$ gilt:*

- $\operatorname{ord}_P(fg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g)$,
- $\operatorname{ord}_P(f+g) \geq \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$ *im Fall* $f+g \neq 0$.
- *Im Fall* $\operatorname{ord}_P(f) \neq \operatorname{ord}_P(g)$ *gilt* $\operatorname{ord}_P(f+g) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$.

Beweis: Wir schreiben

$$f = u_P^a F, \quad g = u_P^b G \text{ mit } a, b \in \mathbb{Z}, F, G \in K(\mathbb{P}^1), F(P) \neq 0, G(P) \neq 0.$$

Dann ist

$$fg = u_P^{a+b} FG.$$

Da F und G in P definiert sind, ist es auch FG; wegen $(FG)(P) = F(P)G(P) \neq 0$, kann man die Ordnung von fg aus obiger Gleichung ablesen:

$$\operatorname{ord}_P(fg) = a + b = \operatorname{ord}_P(f) + \operatorname{ord}_P(g).$$

(Fortsetzung des Beweises mit $f = u_P^a F$ und $g = u_P^b G$) Für die Summe $f+g$ unterscheiden wir zwei Fälle:

- **Fall** $a \neq b$**:** O.E. können wir $a < b$ annehmen. Dann ist

  $$f + g = u_P^a F + u_P^b G = u_P^a \cdot \left(F + u_P^{b-a} G\right).$$

  Die Funktion $F + u_P^{b-a} G$ ist in P definiert und erfüllt

  $$(F + u_P^{b-a} G)(P) = F(P) + u_P(P)^{b-a} G(P) = F(P) \neq 0,$$

  weswegen wir

  $$\operatorname{ord}_P(f+g) = a = \operatorname{ord}_P(f) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$$

  erhalten.
- **Fall** $a = b$**:** Es ist

  $$f + g = u_P^a (F + G).$$

  Da F und G in P definiert sind, ist es auch $F+G$ und wir können zerlegen

  $$F + G = u_P^c H,$$

  wo H in P definiert ist mit $H(P) \neq 0$ und $c \geq 0$ gilt. Dann ist

  $$f + g = u_P^{a+c} H$$

  und

  $$\operatorname{ord}_P(f+g) = a + c = \operatorname{ord}_P(f) + c \geq \operatorname{ord}_P(f) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g)).$$

Damit ist der Satz bewiesen. ■

Im folgenden Lemma geht wesentlich ein, dass der Grundkörper K als algebraisch abgeschlossen vorausgesetzt wurde.

LEMMA. *Sei* $f \in K(\mathbb{P}^1) \setminus \{0\}$ *geschrieben als*

$$f = c \cdot \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}}.$$

Dabei seien die Zahlen $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$ *paarweise verschieden und* $m_i, n_j \in \mathbb{N}$, $c \in K^*$, $r, s \in \mathbb{N}_0$. *Dann gilt:*

$$\operatorname{ord}_P(f) = \begin{cases} m_i & \text{für } P = \alpha_i, \\ -n_j & \text{für } P = \beta_j, \\ (n_1 + \dots + n_s) - (m_1 + \dots + m_r) & \text{für } P = \infty, \\ 0 & \text{sonst.} \end{cases}$$

Beweis: Mit $u = \frac{1}{x}$ gilt

$$\begin{aligned} f &= c \cdot \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}} = \\ &= c \cdot \frac{u^{n_1+\dots+n_s} \cdot (1-\alpha_1 u)^{m_1} \dots (1-\alpha_r u)^{m_r}}{u^{m_1+\dots+m_r} \cdot (1-\beta_1 u)^{n_1} \dots (1-\beta_s u)^{n_s}}. \end{aligned}$$

Daraus kann man sofort ablesen:

$$\operatorname{ord}_{\alpha_i}(f) = m_i, \quad \operatorname{ord}_{\beta_j}(f) = -n_j, \quad \operatorname{ord}_{\infty}(f) = (n_1 + \dots + n_s) - (m_1 + \dots + m_r).$$

In allen anderen Punkten ist f definiert und nimmt einen von 0 verschiedenen Wert an, sodass die Ordnung 0 ist. ■

Das letzte Lemma hat eine erstaunliche Konsequenz:

SATZ. *Jede Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ hat nur endliche viele Null- und Polstellen. Es gilt*

$$\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0.$$

Mit Vielfachheiten gezählt, hat f also genau so viele Null- wie Polstellen.

Beweis: Das folgt sofort aus dem letzten Lemma, wenn man alle Ordnungen aufaddiert. ■

Beispiele:

$$\operatorname{ord}_0(x) = 1, \quad \operatorname{ord}_{\infty}(x) = -1.$$

Für $c \in K \setminus \{0\}$ gilt

$$\operatorname{ord}_c(x-c) = 1, \quad \operatorname{ord}_{\infty}(x-c) = \operatorname{ord}_{\infty}(\frac{1}{u} - c) = \operatorname{ord}_{\infty}(\frac{1}{u} \cdot (1-uc)) = -1.$$

Beispiel: Ist $p(x) \in K[x] \setminus \{0\}$ ein Polynom vom Grad m, so weiß man, dass p mit Vielfachheiten gezählt genau m Nullstellen hat. Betrachtet man p als Funktion auf $\mathbb{P}^1$, so folgt, dass p in ∞ einen Pol der Ordnung m hat.

FOLGERUNG. *Die einzigen Funktionen in $K(\mathbb{P}^1)$ ohne Polstellen sind die konstanten Funktionen. Anders ausgedrückt: Für $f \in K(\mathbb{P}^1) \setminus \{0\}$ gilt:*

$$\operatorname{ord}_P(f) \geq 0 \text{ für alle } P \in \mathbb{P}^1 \quad \Longleftrightarrow \quad f \in K^*.$$

Beweis: Ist f konstant, so ist nichts zu zeigen. Wir können annehmen, dass f nicht konstant ist. Sei $f = \frac{p(x)}{q(x)}$, wobei die Darstellung gekürzt sein soll. Ist $q(x)$ ein nichtkonstantes Polynom, so hat es eine Nullstelle β, d.h. $q(\beta) = 0$. Dann hat aber f eine Polstelle in β und es gilt $\operatorname{ord}_P(f) < 0$. Ist $f = p(x)$, so ist p nicht konstant. Es gibt also eine Nullstelle α. Dann ist $f(\alpha) = 0$. Dann hat aber f in ∞ eine Polstelle. ■

DEFINITION. *Sei $f \in K(\mathbb{P}^1)$ und $\lambda \in K$. Wir sagen, f nimmt den Wert λ in $P \in \mathbb{P}^1$ an, wenn gilt $f(P) = \lambda$.*
In diesem Fall sagen wir genauer: f nimmt den Wert λ in P mit Vielfachheit $\operatorname{ord}_P(f - \lambda)$ an, wenn $f \notin K$ gilt. (Im Fall $\lambda = 0$ ist diese Vielfachheit einfach die Nullstellenordnung.)

Beispiel: Wir betrachten

$$f = \frac{3x^2 - 2x + 5}{x^2 + 2}.$$

In $P = 1$ nimmt f den Wert 2 an: $f(1) = 2$. Mit welcher Vielfachheit? Es ist

$$\begin{aligned} f - 2 &= \frac{3x^2 - 2x + 5}{x^2 + 2} - 2 = \frac{(3x^2 - 2x + 5) - 2(x^2 + 2)}{x^2 + 2} = \\ &= \frac{x^2 - 2x + 1}{x^2 + 2} = (x-1)^2 \cdot \frac{1}{x^2 - 2}, \end{aligned}$$

also $\operatorname{ord}_1(f-2) = 2$, d.h. f nimmt den Wert 2 in 1 mit Vielfachheit 2 an.

SATZ. *Sei $f \in K(\mathbb{P}^1) \setminus K$ geschrieben als*

$$f = \frac{p(x)}{q(x)} \text{ mit teilerfremden Polynomen } p(x), q(x).$$

(Die Darstellung $f = \frac{p(x)}{q(x)}$ soll also gekürzt sein.) Für $\lambda \in K$ nimmt die Funktion f den Wert λ in genau

$$\max(\operatorname{grad}(p(x)), \operatorname{grad}(q(x)))$$

Punkten an, wenn man mit Vielfachheiten zählt, d.h.

$$\sum_{\substack{P \in \mathbb{P}^1 \\ f(P)=\lambda}} \operatorname{ord}_P(f-\lambda) = \max(\operatorname{grad}(p(x)), \operatorname{grad}(q(x))).$$

Dies ist auch gleich der (mit Vielfachkeit gezählten) Anzahl der Polstellen von f, d.h.

$$\sum_{\substack{P \in \mathbb{P}^1 \\ \operatorname{ord}_P(f)<0}} |\operatorname{ord}_P(f)| = \max(\operatorname{grad}(p), \operatorname{grad}(q)).$$

Beweis:

- Wir zählen zunächst die Polstellen von f. Wir schreiben wieder

$$\begin{aligned} f &= c \cdot \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}} = \\ &= c \cdot \frac{u^{n_1+\dots+n_s} \cdot (1-\alpha_1 u)^{m_1} \dots (1-\alpha_r u)^{m_r}}{u^{m_1+\dots+m_r} \cdot (1-\beta_1 u)^{n_1} \dots (1-\beta_s u)^{n_s}} = \\ &= c \cdot u^{\operatorname{grad}(q)-\operatorname{grad}(p)} \cdot \frac{(1-\alpha_1 u)^{m_1} \dots (1-\alpha_r u)^{m_r}}{(1-\beta_1 u)^{n_1} \dots (1-\beta_s u)^{n_s}}. \end{aligned}$$

  Im Endlichen sind die Polstellen von f die Punkte $\beta_1, \dots, \beta_s$, mit Vielfachheit gezählt also

$$n_1 + \dots + n_s = \operatorname{grad}(q(x)).$$

  Wir unterscheiden zwei Fälle:
  - **Fall** $\operatorname{grad}(p) > \operatorname{grad}(q)$**:** Dann ist $\operatorname{ord}_\infty(f) = \operatorname{grad}(q) - \operatorname{grad}(p) = -(\operatorname{grad}(p) - \operatorname{grad}(q))$, f hat in ∞ einen Pol der Ordnung $\operatorname{grad}(p) - \operatorname{grad}(q)$. Mit Vielfachheiten gezählt gibt es also

$$\operatorname{grad}(q) + (\operatorname{grad}(p) - \operatorname{grad}(q)) = \operatorname{grad}(p) = \max(\operatorname{grad}(p), \operatorname{grad}(q))$$

    Polstellen von f.
  - **Fall** $\operatorname{grad}(p) \leq \operatorname{grad}(q)$**:** Dann ist f in ∞ definiert. Die einzigen Polstellen liegen im Endlichen, ihre Anzahl ist

$$\operatorname{grad}(q) = \max(\operatorname{grad}(p), \operatorname{grad}(q)).$$

  Zusammengefasst:

$$\sum_{\substack{P \in \mathbb{P}^1 \\ \operatorname{ord}_P(f)<0}} |\operatorname{ord}_P(f)| = \max(\operatorname{grad}(p), \operatorname{grad}(q)).$$

- Die Funktion $f - \lambda$ hat die gleichen Polstellen wie f, weil dies gerade die Punkte sind, in denen f nicht definiert ist. Mit der Formel des letztes Satzes

$$\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0$$

angewandt auf $f-\lambda$ erhält man daher

$$\begin{aligned} 0 &= \sum_{P\in\mathbb{P}^1} \operatorname{ord}_P(f-\lambda) = \sum_{\substack{P\in\mathbb{P}^1\\ \operatorname{ord}_P(f-\lambda)>0}} \operatorname{ord}_P(f-\lambda) + \sum_{\substack{P\in\mathbb{P}^1\\ \operatorname{ord}_P(f-\lambda)<0}} \operatorname{ord}_P(f-\lambda) = \\ &= \sum_{\substack{P\in\mathbb{P}^1\\ f(P)=0}} \operatorname{ord}_P(f-\lambda) - \sum_{\substack{P\in\mathbb{P}^1\\ \operatorname{ord}_P(f-\lambda)<0}} |\operatorname{ord}_P(f-\lambda)| = \\ &= \sum_{\substack{P\in\mathbb{P}^1\\ f(P)=0}} \operatorname{ord}_P(f-\lambda) - \max(\operatorname{grad}(p),\operatorname{grad}(q)). \end{aligned}$$

Daraus folgt dann

$$\sum_{\substack{P\in\mathbb{P}^1\\ f(P)=\lambda}} \operatorname{ord}_P(f-\lambda) = \max(\operatorname{grad}(p),\operatorname{grad}(q)),$$

wie behauptet. ■

Beispiel: Wir betrachten

$$f = \frac{3x^2-2x+5}{x^2+2}.$$

Es ist

$$f = 3\cdot\frac{(x-\frac{1+\sqrt{-14}}{3})(x-\frac{1-\sqrt{-14}}{3})}{(x-\sqrt{-2})(x+\sqrt{-2})},$$

insbesondere ist die Darstellung gekürzt. f hat zwei Polstellen erster Ordnung, nämlich in $\pm\sqrt{-2}$, zwei Nullstellen erster Ordnung, nämlich in $\frac{1\pm\sqrt{-14}}{3}$. Wegen

$$f = \frac{3x^2-2x+5}{x^2+2} = \frac{3-2u+5u^2}{1+2u^2}$$

gilt $f(\infty)=3$. Mit welcher Vielfachheit wird der Wert 3 in ∞ angenommen? Es ist

$$f-3 = \frac{3-2u+5u^2}{1+2u^2} - 3 = \frac{(3-2u+5u^2)-3(1+2u^2)}{1+2u^2} = \frac{-2u-u^2}{1+2u^2} = u\cdot\frac{-2-u}{1+2u^2}.$$

Also $\operatorname{ord}_\infty(f-3)=1$, sodass der Wert 3 in ∞ mit Vielfachheit 1 angenommen wird. An welchem Punkt wird der Wert 3 sonst noch angenommen?

$$\begin{aligned} f-3 &= \frac{3x^2-2x+5}{x^2+2} - 3 = \frac{(3x^2-2x+5)-3(x^2+2)}{x^2+2} = \\ &= \frac{-2x-1}{x^2+2} = -\frac{1}{2}\cdot\frac{x+\frac{1}{2}}{x^2+2}. \end{aligned}$$

Also wird der Wert 3 noch im Punkt $-\frac{1}{2}$ angenommen.

3. Divisoren

Ein **Divisor** D der Kurve $\mathbb{P}^1$ ist eine formale ganzzahlige Linearkombination von endlich vielen Punkten auf $\mathbb{P}^1$:

$$D = \sum_{P\in\mathbb{P}^1} n_P[P] \quad \text{mit} \quad n_P\in\mathbb{Z} \quad \text{und} \quad \#\{P\in\mathbb{P}^1 : n_P\neq 0\} < \infty.$$

Beispiele: (für $K=\mathbb{C}$)

$D_1 = 2[1]-3[5]+3[\infty] = 2[(1:1)]-3[(1:5)]+3[(0:1)]$, $D_2=0$, $D_3 = 2[1+i]-3[\pi]+5[\infty]$.

(Die eckigen Klammern bei $[P]$ dienen dazu, die Punkte nicht mit Zahlen zu vermischen.)

Dabei soll gelten

$$\sum_{P\in\mathbb{P}^1} m_P[P] = \sum_{P\in\mathbb{P}^1} n_P[P] \quad\Longleftrightarrow\quad m_P = n_P \text{ für alle } P\in\mathbb{P}^1.$$

(Man kann also „Koeffizientenvergleich“ machen.)
Divisoren kann man addieren und subtrahieren:

$$\left(\sum_{P\in\mathbb{P}^1} m_P[P]\right) + \left(\sum_{P\in\mathbb{P}^1} n_P[P]\right) = \sum_{P\in\mathbb{P}^1} (m_P + n_P)[P]$$

und

$$\left(\sum_{P\in\mathbb{P}^1} m_P[P]\right) - \left(\sum_{P\in\mathbb{P}^1} n_P[P]\right) = \sum_{P\in\mathbb{P}^1} (m_P - n_P)[P].$$

Damit bilden die Divisoren eine abelsche Gruppe, die **Divisorengruppe** von $\mathbb{P}^1$:

$$\mathrm{Div}(\mathbb{P}^1) = \{\sum_{P\in\mathbb{P}^1} n_P[P] : n_P \in \mathbb{Z} \text{ und } \#\{P \in \mathbb{P}^1 : n_P \neq 0\} < \infty\}.$$

(In der Sprache der Algebra: $\mathrm{Div}(\mathbb{P}^1)$ ist die freie abelsche Gruppe, die von den Punkten von $\mathbb{P}^1$ erzeugt wird.)
Wir definieren den **Grad eines Divisors** durch

$$\mathrm{grad}(\sum_{P\in\mathbb{P}^1} n_P[P]) = \sum_{P\in\mathbb{P}^1} n_P.$$

Beispiele: Für die obigen Divisoren

$$D_1 = 2[1] - 3[5] + 3[\infty], \quad D_2 = 0, \quad D_3 = 2[1+i] - 3[\pi] + 5[\infty]$$

gilt

$$\mathrm{grad}(D_1) = 2, \quad \mathrm{grad}(D_2) = 0, \quad \mathrm{grad}(D_3) = 4.$$

Wir erhalten also eine Abbildung

$$\mathrm{grad} : \mathrm{Div}(\mathbb{P}^1) \to \mathbb{Z}.$$

Die Formel für die Addition von Divisoren zeigt sofort, dass die Grad-Abbildung additiv ist, d.h. ein Gruppenhomomorphismus ist.

Die **Divisoren vom Grad** 0 bilden eine Untergruppe in der Divisorengruppe:

$$\mathrm{Div}_0(\mathbb{P}^1) = \{D \in \mathrm{Div}(\mathbb{P}^1) : \mathrm{grad}(D) = 0\}.$$

Beispiel: $D = 3[\pi] - 7[i] + 4[\infty]$ ist ein Divisor vom Grad 0.
Die eigentliche Bedeutung der Divisoren kommt von den Hauptdivisoren: Sei $f \in K(\mathbb{P}^1) \setminus \{0\}$. Wir definieren den zu f gehörigen **Hauptdivisor** durch

$$\mathrm{div}(f) = \sum_{P\in\mathbb{P}^1} \mathrm{ord}_P(f)[P].$$

Da wir gesehen haben, dass eine von 0 verschiedene Funktion nur endlich viele Null- und Polstellen hat, ist $\mathrm{div}(f)$ wohldefiniert. (Ein Divisor D heißt **Hauptdivisor**, wenn es eine Funktion $f \in K(\mathbb{P}^1)\setminus\{0\}$ gibt mit $D = \mathrm{div}(f)$.) Der Divisor $\mathrm{div}(f)$ stellt also Informationen über die Null- und Polstellen der Funktion f zusammen.

Beispiele:

- Ist $\lambda \in K^*$, so hat λ als Element von $K(\mathbb{P}^1)$ weder Null- noch Polstellen, es gilt also
$$\mathrm{div}(\lambda) = 0.$$
- Die Funktion x hat einen Pol 1. Ordnung in ∞ und eine Nullstelle 1. Ordnung in 0. Daher ist
$$\mathrm{div}(x) = [0] - [\infty].$$
- Die Funktion $u = \frac{1}{x}$ hat einen Pol 1. Ordnung in 0 und eine Nullstelle 1. Ordnung in ∞:
$$\mathrm{div}(u) = [\infty] - [0].$$

- Wir hatten die Funktion
$$f = \frac{3x^2 - 2x + 5}{x^2 + 2} = 3 \cdot \frac{(x - \frac{1+\sqrt{-14}}{3})(x - \frac{1-\sqrt{-14}}{3})}{(x - \sqrt{-2})(x + \sqrt{-2})}$$
betrachtet. In ∞ ist wegen $f(\infty) = 3$ weder eine Null- noch eine Polstelle, sodass wir erhalten
$$\operatorname{div}(f) = [\frac{1+\sqrt{-14}}{3}] + [\frac{1-\sqrt{-14}}{3}] - [\sqrt{-2}] - [-\sqrt{-2}].$$

Wenn wir Zähler und Nenner einer rationalen Funktion f in Linearfaktoren zerlegen können, können wir sofort den zugehörigen Hauptdivisor aufschreiben:

SATZ. *Sei $f \in K(\mathbb{P}^1)$ mit*
$$f = c \cdot \frac{(x - \alpha_1)^{m_1} \dots (x - \alpha_r)^{m_r}}{(x - \beta_1)^{n_1} \dots (x - \beta_s)^{n_s}},$$
wo $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$ paarweise verschiedene Zahlen aus K sind und $m_1, \dots, m_r, n_1, \dots, n_s \in \mathbb{N}$, $r, s \in \mathbb{N}_0$, $c \in K^*$ gilt. Dann ist
$$\operatorname{div}(f) = ((n_1 + \dots + n_s) - (m_1 + \dots + m_r))[\infty] + m_1[\alpha_1] + \dots + m_r[\alpha_r] - n_1[\beta_1] - \dots - n_s[\beta_s].$$

Beweis: Wir hatten gezeigt:
$$\operatorname{ord}_P(f) = \begin{cases} m_i & \text{für } P = \alpha_i, \\ -n_j & \text{für } P = \beta_j, \\ (n_1 + \dots + n_s) - (m_1 + \dots + m_r) & \text{für } P = \infty, \\ 0 & \text{sonst.} \end{cases}$$
Daraus folgt die Behauptung. ■

SATZ. *Jeder Hauptdivisor hat Grad 0, d.h. für $f \in K(\mathbb{P}^1) \setminus \{0\}$ gilt*
$$\operatorname{grad}(\operatorname{div}(f)) = 0.$$

Achtung: Der Ausdruck $\operatorname{grad}(\operatorname{div}(f))$ hat nichts mit dem Gradienten und der Divergenz bei Vektorfeldern zu tun.

Beweis: Wegen
$$\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0$$
gilt
$$\operatorname{grad}(\operatorname{div}(f)) = \operatorname{grad}(\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f)[P]) = \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0,$$
wie behauptet. ■

LEMMA. *Für $f, g \in K(\mathbb{P}^1)^*$ gilt*
$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g) \quad \textit{und} \quad \operatorname{div}(\frac{1}{f}) = -\operatorname{div}(f).$$
Die Abbildung
$$K(\mathbb{P}^1)^* \to \operatorname{Div}_0(\mathbb{P}^1), \quad f \mapsto \operatorname{div}(f)$$
ist also ein Gruppenhomomorphismus.

Beweis: Es gilt
$$\begin{aligned} \operatorname{div}(fg) &= \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(fg)[P] = \sum_{P \in \mathbb{P}^1} (\operatorname{ord}_P(f) + \operatorname{ord}_P(g))[P] = \\ &= \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f)[P] + \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(g)[P] = \operatorname{div}(f) + \operatorname{div}(g), \end{aligned}$$
was zu zeigen war. ■

LEMMA. *Für $f, g \in K(\mathbb{P}^1)^*$ gilt*

$$\operatorname{div}(f) = 0 \quad \Longleftrightarrow \quad f \in K^*$$

und

$$\operatorname{div}(f) = \operatorname{div}(g) \quad \Longleftrightarrow \quad \text{es gibt ein } \lambda \in K^* \text{ mit } g = \lambda f.$$

Beweis:

- Ist $\operatorname{div}(f) = 0$, so hat f weder Null- noch Polstellen, ist also konstant, wie wir zuvor früher gesehen haben. Die Umkehrung ist klar.
- $\Longrightarrow$ Ist $\operatorname{div}(f) = \operatorname{div}(g)$, so folgt $\operatorname{div}(\frac{g}{f}) = 0$, nach dem ersten Teil ist $\frac{g}{f}$ konstant, also $\frac{g}{f} = \lambda$ für eine Zahl $\lambda \in K^*$. Dann ist $g = \lambda f$, wie behauptet.
  $\Longleftarrow$ Wegen $\operatorname{div}(\lambda) = 0$ folgt
  $$\operatorname{div}(g) = \operatorname{div}(\lambda f) = \operatorname{div}(\lambda) + \operatorname{div}(f) = \operatorname{div}(f).$$
  Damit ist alles gezeigt. ■

Bemerkung: Die Begriffe *Ordnung einer Funktion in einem Punkt*, *Uniformisierende*, *Divisor*, *Divisorengruppe*, *Hauptdivisor* lassen sich auch auf beliebigen nichtsingulären projektiven Kurven C einführen. Folgender Satz ist aber typisch für $\mathbb{P}^1$ und gilt für allgemeine Kurven nicht:

SATZ. *Jeder Divisor vom Grad 0 auf $\mathbb{P}^1$ ist ein Hauptdivisor. Genauer: Ist*

$$D = n_\infty[\infty] + m_1[\alpha_1] + \cdots + m_r[\alpha_r] - n_1[\beta_1] - \cdots - n_s[\beta_s],$$

wobei $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ paarweise verschiedene Zahlen aus K sind und $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbb{N}$, $r, s \in \mathbb{N}_0$ ein Divisor vom Grad 0, so hat die Funktion

$$f = \frac{(x-\alpha_1)^{m_1} \ldots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \ldots (x-\beta_s)^{n_s}}$$

den Divisor D, d.h. $\operatorname{div}(f) = D$.

Beweis: Natürlich können wir D wir im Satz schreiben. Da D Grad 0 haben soll, folgt

$$n_\infty = (n_1 + \cdots + n_s) - (m_1 + \cdots + m_r).$$

Nun betrachten wir die Funktion

$$f = \frac{(x-\alpha_1)^{m_1} \ldots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \ldots (x-\beta_s)^{n_s}}.$$

Wir haben zuvor gezeigt, dass gilt

$$\operatorname{div}(f) \quad = \quad ((n_1 + \cdots + n_s) - (m_1 + \cdots + m_r))[\infty] + m_1[\alpha_1] + \cdots + m_r[\alpha_r] - n_1[\beta_1] - \cdots - n_s[\beta_s].$$

Dann gilt aber offensichtlich $D = \operatorname{div}(f)$, was die Behauptung beweist. ■

Nochmals anders ausgedrückt: Auf $\mathbb{P}^1$ sind die Divisoren vom Grad 0 genau die Hauptdivisoren.

Beispiel: Der Divisor

$$D = 2[1] - 3[\pi] + 4[e] - 3[\sqrt{2}]$$

ist ein Divisor vom Grad 0. Ein zugehöriger Hauptdivisor $\operatorname{div}(f)$ wird gegeben durch

$$f = \frac{(x-1)^2(x-e)^4}{(x-\pi)^3(x-\sqrt{2})^3}.$$

DEFINITION. *Zwei Divisoren $D_1, D_2 \in \operatorname{Div}(\mathbb{P}^1)$ heißen* **linear äquivalent**, *in Zeichen $D_1 \sim D_2$, wenn sie sich nur um einen Hauptdivisor unterscheiden:*

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \text{es gibt eine Funktion } f \in K(\mathbb{P}^1)^* \text{ mit } D_1 = D_2 + \operatorname{div}(f).$$

Beispiel: Es ist $\operatorname{div}(x) = [0] - [\infty]$, also $[\infty] + \operatorname{div}(x) = [0]$, woraus

$$[0] \sim [\infty]$$

folgt.

LEMMA. *Die lineare Äquivalenz von Divisoren auf $\mathbb{P}^1$ ist eine Äquivalenzrelation.*

Beweis:

- $D \sim D$: Dies folgt aus $D = D + \operatorname{div}(1)$.
- $D_1 \sim D_2 \Longrightarrow D_2 \sim D_1$: Ist $D_1 \sim D_2$, so gibt es eine Funktion f mit $D_1 = D_2 + \operatorname{div}(f)$. Dann ist aber $D_2 = D_1 - \operatorname{div}(f) = D_1 + \operatorname{div}(\frac{1}{f})$, also $D_2 \sim D_1$.
- $D_1 \sim D_2, D_2 \sim D_3 \Longrightarrow D_1 \sim D_3$: Es gibt Funktionen f, g mit $D_1 = D_2 + \operatorname{div}(f)$ und $D_2 = D_3 + \operatorname{div}(g)$. Es folgt $D_1 = D_2 + \operatorname{div}(f) + \operatorname{div}(g) = D_2 + \operatorname{div}(fg)$, also $D_1 \sim D_3$. ■

Bemerkung: Man definiert die **Divisorenklassengruppe** von $\mathbb{P}^1$ als Faktorgruppe $\operatorname{Div}(\mathbb{P}^1)/\{\text{Hauptdivisoren}\}$. Sie mit mit $\operatorname{Pic}(\mathbb{P}^1)$ (Picard-Gruppe) bezeichnet. Für zwei Divisoren gilt

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \overline{D_1} = \overline{D_2} \text{ in } \operatorname{Pic}(\mathbb{P}^1).$$

Bemerkung: Die Definitionen der linearen Äquivalenz und der Picard-Gruppe verallgemeinern sich auf nichtsinguläre projektive Kurven. Auf $\mathbb{P}^1$ ist die lineare Äquivalenz aber einfach zu entscheiden:

SATZ. *Für $D_1, D_2 \in \operatorname{Div}(\mathbb{P}^1)$ gilt:*

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \operatorname{grad}(D_1) = \operatorname{grad}(D_2),$$

zwei Divisoren sind also genau dann linear äquivalent, wenn sie den gleichen Grad haben.

Beweis:

- $\Longrightarrow$ Sei $D_1 \sim D_2$. Dann existiert eine Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ mit $D_2 = D_1 + \operatorname{div}(f)$. Es folgt

  $$\operatorname{grad}(D_2) = \operatorname{grad}(D_1 + \operatorname{div}(f)) = \operatorname{grad}(D_1) + \operatorname{grad}(\operatorname{div}(f)) = \operatorname{grad}(D_1),$$

  da Hauptdivisoren Grad 0 haben. Dies beweist die Behauptung.
- $\Longleftarrow$ Sei umgekehrt $\operatorname{grad}(D_1) = \operatorname{grad}(D_2)$. Für den Divisor $D = D_2 - D_1$ gilt dann $\operatorname{grad}(D) = \operatorname{grad}(D_2) - \operatorname{grad}(D_1) = 0$. Da aber auf $\mathbb{P}^1$ jeder Divisor vom Grad 0 ein Hauptdivisor ist, gibt es eine Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ mit $D = \operatorname{div}(f)$, und damit

  $$D_2 = D_1 + D = D_1 + \operatorname{div}(f), \quad \text{also} \quad D_2 \sim D_1,$$

  wie behauptet. ■

Beispiel: Sind $\alpha_1, \alpha_2 \in K$, so gilt

$$[\alpha_1] + [\alpha_2] \sim 2[\infty],$$

da beide Divisoren gleichen Grad haben. Wir erhält man einen zugehörigen Hauptdivisor, d.h. eine Funktion f mit

$$[\alpha_1] + [\alpha_2] = 2[\infty] + \operatorname{div}(f)?$$

Wir setzen

$$f = (x - \alpha_1)(x - \alpha_2).$$

Dann ist

$$\operatorname{div}(f) = [\alpha_1] + [\alpha_2] - 2[\infty],$$

wie gewünscht.

4. Die Vektorräume $\mathcal{L}(D)$ und der Satz von Riemann-Roch für $\mathbb{P}^1$

Wir führen nun eine Ordnungsrelation für Divisoren ein:

DEFINITION. *Sind $D_1 = \sum m_P[P]$ und $D_2 = \sum n_P[P]$ zwei Divisoren auf $\mathbb{P}^1$, so definiert man*

$$D_1 \geq D_2 \iff m_P \geq n_P \text{ für alle } P \in \mathbb{P}^1.$$

(Dafür kann man natürlich auch $D_2 \leq D_1$ schreiben.) Man nennt einen Divisor D **effektiv**, *wenn $D \geq 0$ gilt.*

Beispiele: Es gilt

$$2[i] + 3[\pi] - [13] \geq [\pi] - [13] \geq -[13] \geq -5[13].$$

Der Divisor

$$3[\infty] + 4[\pi] + 7[13]$$

ist effektiv.

LEMMA. *Für Divisoren auf $\mathbb{P}^1$ gilt:*

- *$\geq$ ist eine Ordnungsrelation auf $\mathrm{Div}(\mathbb{P}^1)$.*
- *Jeder Divisor ist Differenz effektiver Divisoren.*
- *Jeder effektive Divisor hat Grad ≥ 0.*
- *Aus $D_1 \geq D_2$ folgt $\mathrm{grad}(D_1) \geq \mathrm{grad}(D_2)$.*
- *Aus $D_1 \geq D_2$ und $\mathrm{grad}(D_1) = \mathrm{grad}(D_2)$ folgt $D_1 = D_2$.*

Beweis:

- Die erste Eigenschaft folgt aus der entsprechenden für die ganzen Zahlen.
- Ist $D = \sum n_P[P]$, so kann man D so als Differenz effektiver Divisoren schreiben:

$$D = \sum_{\substack{P\in\mathbb{P}^1\\ n_P>0}} n_P[P] + \sum_{\substack{P\in\mathbb{P}^1\\ n_P<0}} n_P[P] = \left(\sum_{\substack{P\in\mathbb{P}^1\\ n_P>0}} n_P[P]\right) - \left(\sum_{\substack{P\in\mathbb{P}^1\\ n_P<0}} |n_P|[P]\right).$$

- Die dritte Eigenschaft folgt aus der vierten Eigenschaft.
- Ist $D_1 = \sum m_P[P]$ und $D_2 = \sum n_P[P]$, so ist $D_1 \geq D_2$ gleichwertig mit $m_P \geq n_P$ für alle P. Daraus folgt $\mathrm{grad}(D_1) = \sum m_P \geq \sum n_P = \mathrm{grad}(D_2)$, also die vierte Eigenschaft. Gilt zusätzlich $\mathrm{grad}(D_1) = \mathrm{grad}(D_2)$, also $\sum m_P = \sum n_P$, so folgt aus $m_P \geq n_P$ natürlich $m_P = n_P$ für alle Punkte P, also die fünfte Eigenschaft. ■

Welche effektiven Hauptdivisoren gibt es? D.h. für welche Funktionen $f \neq 0$ gilt $\mathrm{div}(f) \geq 0$, d.h. $\mathrm{ord}_P(f) \geq 0$ für alle $P \in \mathbb{P}^1$. Wir hatten zuvor gesehen, dass die einzigen Funktionen ohne Polstellen die Konstanten sind. Wir formulieren dies als Satz:

SATZ. *Für $f \in K(\mathbb{P}^1)$ haben wir die Äquivalenz:*

$$\mathrm{div}(f) \geq 0 \iff f \in K^* \iff \mathrm{div}(f) = 0.$$

Bemerkung: Was bedeutet $\mathrm{div}(f) \geq -n[P]$, wenn f eine Funktion, P ein Punkt und n eine natürliche Zahl ist? Es bedeutet, dass gilt

$$\mathrm{ord}_P(f) \geq -n \quad \text{und} \quad \mathrm{ord}_Q(f) \geq 0 \text{ für alle } Q \in \mathbb{P}^1 \setminus \{P\},$$

dass also f in P höchstens einen Pol n-ter Ordnung besitzt, sonst aber überall definiert ist. Wir schauen uns einen Spezialfall in folgendem Lemma an:

LEMMA. *Für eine Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ und $n \in \mathbb{N}_0$ gilt*

$$\mathrm{div}(f) \geq -n[\infty] \iff f \text{ ist ein Polynom vom Grad } \leq n.$$

Beweis:

- Es gelte $\operatorname{div}(f) \geq -n[\infty]$. Dann ist
$$\operatorname{ord}_\beta(f) \geq 0 \text{ für alle } \beta \in K \quad \text{und} \quad \operatorname{ord}_\infty(f) \geq -n.$$
Wir schreiben $f = \frac{p(x)}{q(x)}$ als Quotient gekürzter Polynome. Wäre $q(x)$ nichtkonstant, so gäbe es ein $\beta \in K$ mit $q(\beta) = 0$, β wäre eine Polstelle von f und $\operatorname{ord}_\beta(f) \leq -1$, im Widerspruch zu $\operatorname{ord}_\beta(f) \geq 0$. Also ist $q(x)$ konstant und o.E. $q(x) = 1$. Wir haben also $f = p(x)$. Sei m der Grad von $p(x)$:
$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_m x^m \text{ mit } p_m \neq 0.$$
Dann ist
$$f = p(x) = \frac{1}{u^m} \cdot (p_m + p_{m-1} u + \cdots + p_0 u^m) \quad \text{und} \quad \operatorname{ord}_\infty(f) = -m.$$
Aus $\operatorname{ord}_\infty(f) \geq -n$ folgt dann $m \leq n$, also die Behauptung.
- Die Umkehrung sieht man, wenn man den ersten Teil des Beweises rückwärts liest. ■

DEFINITION. *Für einen Divisor $D \subseteq \operatorname{Div}(\mathbb{P}^1)$ definiert man*
$$\mathcal{L}(D) = \{f \in K(\mathbb{P}^1)^* : D + \operatorname{div}(f) \geq 0\} \cup \{0\}.$$
($\mathcal{L}(D)$ ist eine Teilmenge des Funktionenkörpers $K(\mathbb{P}^1)$.) Ist $D = \sum_{P \in \mathbb{P}^1} n_P[P]$, so gilt
$$\mathcal{L}(D) = \{f \in K(\mathbb{P}^1)^* : \operatorname{ord}_P(f) \geq -n_P \text{ für alle } P \in \mathbb{P}^1\} \cup \{0\}.$$

Wir schreiben die letzte Darstellung in der Definition noch etwas ausführlicher: Ist $D = m_1[P_1] + \cdots + m_r[P_r] - n_1[Q_1] - \cdots - n_s[Q_s]$ mit $m_i, n_j \in \mathbb{N}$, so gilt für $f \in K(\mathbb{P}^1)^*$
$$\begin{aligned} f \in \mathcal{L}(D) \quad \Longleftrightarrow \quad & \operatorname{ord}_{P_1}(f) \geq -m_1, \ldots, \operatorname{ord}_{P_r}(f) \geq -m_r, \\ & \operatorname{ord}_{Q_1}(f) \geq n_1, \ldots, \operatorname{ord}_{Q_s}(f) \geq n_s, \\ & \operatorname{ord}_R(f) \geq 0 \text{ für alle } R \in \mathbb{P}^1 \setminus \{P_1, \ldots, P_r, Q_1, \ldots, Q_s\}, \end{aligned}$$
d.h. $\mathcal{L}(D)$ besteht genau aus den Funktionen, die in $P_1, \ldots, P_r$ höchstens einen Pol der Ordnung $m_1, \ldots, m_r$, in $Q_1, \ldots, Q_s$ mindestens eine Nullstelle der Ordnung $n_1, \ldots, n_s$ haben und sonst überall definiert sind.
Bemerkung: Die Definition
$$\mathcal{L}(D) = \{f \in K(\mathbb{P}^1)^* : D + \operatorname{div}(f) \geq 0\} \cup \{0\}$$
ist genau so gemacht, dass die folgende Menge von Divisoren
$$\{D + \operatorname{div}(f) : f \in \mathcal{L}(D) \setminus \{0\}\} \subseteq \operatorname{Div}(\mathbb{P}^1)$$
genau aus den effektiven Divisoren besteht, die linear äquivalent zu D sind.

Beispiel: Wir betrachten den Nulldivisor. Für eine Funktion $f \neq 0$ gilt:
$$f \in \mathcal{L}(0) \quad \Longleftrightarrow \quad \operatorname{div}(f) \geq 0 \quad \Longleftrightarrow \quad f \in K^*,$$
wobei wir die letzte Äquivalenz kurz zuvor gezeigt haben. Mit der 0 zusammen ergibt sich
$$\mathcal{L}(0) = K.$$

Beispiel: Mit dem vorangegangenen Lemma erhalten wir für $n \in \mathbb{N}$:
$$\begin{aligned} \mathcal{L}(n[\infty]) &= \{f \in K(\mathbb{P}^1)^* : \operatorname{div}(f) \geq -n[\infty]\} \cup \{0\} = \\ &= \{p_0 + p_1 x + \cdots + p_n x^n : p_0, p_1, \ldots, p_n \in K\} = \\ &= K + Kx + Kx^2 + \cdots + Kx^n. \end{aligned}$$
Da wir das Ergebnis noch benutzen werden, formulieren wir es als Satz:

SATZ. *Für $n \in \mathbb{N}_0$ gilt*
$$\begin{aligned} \mathcal{L}(n[\infty]) &= \{p_0 + p_1 x + \cdots + p_n x^n : p_0, p_1, \ldots, p_n \in K\} = \\ &= K + Kx + \cdots + Kx^n. \end{aligned}$$
$\mathcal{L}(n[\infty])$ ist der K-Vektorraum der Polynome vom Grad $\leq n$, eine K-Basis bilden die Monome $1, x, \ldots, x^n$. Insbesondere gilt $\dim \mathcal{L}(D) = n + 1$.

LEMMA. *Für einen Divisor $D \in \mathrm{Div}(\mathbb{P}^1)$ ist $\mathcal{L}(D)$ ein K-Vektorraum.*

Beweis:

- $0 \in \mathcal{L}(D)$: Dies gilt nach Definition von $\mathcal{L}(D)$.
- $\lambda \in K, f \in \mathcal{L}(D) \Longrightarrow \lambda f \in L(D)$: Ist $f \in \mathcal{L}(D) \setminus \{0\}$ und $\lambda \in K^*$, so folgt $D + \mathrm{div}(f) \geq 0$ und wegen $\mathrm{div}(\lambda f) = \mathrm{div}(f)$ auch $D + \mathrm{div}(\lambda f) \geq 0$, also $\lambda f \in \mathcal{L}(D)$.
- $f, g \in \mathcal{L}(D) \Longrightarrow f + g \in \mathcal{L}(D)$: Seien $f, g \in \mathcal{L}(D) \setminus \{0\}$. Ist $f + g = 0$, so gilt trivialerweise $f + g \in \mathcal{L}(D)$. Sei also $f + g \neq 0$. Schreiben wir $D = \sum n_P[P]$, so gilt
$$\mathrm{ord}_P(f) \geq -n_P \text{ und } \mathrm{ord}_P(g) \geq -n_P \text{ für alle } P \in \mathbb{P}^1.$$
Dies impliziert
$$\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g)) \geq -n_P,$$
und damit $f + g \in \mathcal{L}(D)$.

Dies beweist, dass $\mathcal{L}(D)$ ein K-Vektorraum ist. ■

LEMMA. *Für $D \in \mathrm{Div}(\mathbb{P}^1)$ und $f \in K(\mathbb{P}^1)^*$ gilt:*

- $\mathcal{L}(0) = K$.
- $\mathcal{L}(\mathrm{div}(f)) = K\frac{1}{f}$.
- $\mathcal{L}(D + \mathrm{div}(f)) = \frac{1}{f}\mathcal{L}(D)$.

Beweis:

- Dies haben wir bereits gezeigt.
- Für $g \in K(\mathbb{P}^1)^*$ gilt: $g \in \mathcal{L}(\mathrm{div}(f)) \iff \mathrm{div}(g) + \mathrm{div}(f) \geq 0 \iff \mathrm{div}(gf) \geq 0$, was äquivalent damit ist, dass gf konstant ist, d.h. $gf \in K$, also $g \in K\frac{1}{f}$. (Natürlich folgt die Eigenschaft auch aus (1) und (3).)
- Für $g \in K(\mathbb{P}^1)^*$ gilt:
$$\begin{aligned} g \in \mathcal{L}(D + \mathrm{div}(f)) &\iff D + \mathrm{div}(f) + \mathrm{div}(g) \geq 0 \iff \\ &\iff D + \mathrm{div}(fg) \geq 0 \iff \\ &\iff fg \in \mathcal{L}(D) \iff g \in \frac{1}{f}\mathcal{L}(D), \end{aligned}$$
was die Behauptung beweist. ■

Beispiel: Wir wollen für einen Punkt $P \in \mathbb{P}^1$ den K-Vektorraum $\mathcal{L}(-[P])$ bestimmen. Für $f \in K(\mathbb{P}^1)^*$ gilt:
$$f \in \mathcal{L}(-[P]) \iff \mathrm{div}(f) - [P] \geq 0 \iff \mathrm{div}(f) \geq [P].$$
f dürfte also keine Polstelle haben, müsste also konstant sein, andererseits müsste f aber in P eine Nullstelle haben. Das geht nicht, und daher folgt $\mathcal{L}(-[P]) = 0$.

Das Phänomen des letztes Satzes lässt sich leicht verallgemeinern:

SATZ. *Für $D \in \mathrm{Div}(\mathbb{P}^1)$ gilt die Implikation:*
$$\mathrm{grad}(D) < 0 \quad \Longrightarrow \quad \mathcal{L}(D) = 0.$$

Beweis: Angenommen, es gäbe eine Funktion $f \in \mathcal{L}(D) \setminus \{0\}$. Dann wäre $D + \mathrm{div}(f) \geq 0$, und damit $\mathrm{grad}(D + \mathrm{div}(f)) \geq 0$. Es würde
$$\mathrm{grad}(D) = \mathrm{grad}(D) + \mathrm{grad}(\mathrm{div}(f)) = \mathrm{grad}(D + \mathrm{div}(f)) \geq 0$$
folgen, im Widerspruch zur Voraussetzung $\mathrm{grad}(D) < 0$. Also muss $\mathcal{L}(D) = 0$ gelten. ■

Beschreibung von $\mathcal{L}(D)$ im Fall $\mathrm{grad}(D) \geq 0$: Wir schreiben
$$D = n_1[\alpha_1] + \cdots + n_r[\alpha_r] + n_\infty[\infty]$$

mit (beliebigen) ganzen Zahlen $n_1, \ldots, n_r, n_\infty$ und paarweise verschiedenen Zahlen $\alpha_1, \ldots, \alpha_r$ aus K. Wir definieren

$$f = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}.$$

Dann ist

$$\operatorname{div}(f) = n_1[\alpha_1] + \cdots + n_r[\alpha_r] - (n_1 + \cdots + n_r)[\infty]$$

und daher

$$D - \operatorname{div}(f) = (n_\infty + (n_1 + \cdots + n_r))[\infty] = \operatorname{grad}(D) \cdot [\infty].$$

Mit einem früheren Satz folgt

$$\begin{aligned} \mathcal{L}(D) &= \mathcal{L}(\operatorname{grad}(D)[\infty] + \operatorname{div}(f)) = \frac{1}{f}\mathcal{L}(\operatorname{grad}(D)[\infty]) = \\ &= \frac{1}{f}(K + Kx + \cdots + Kx^{\operatorname{grad}(D)}). \end{aligned}$$

Wir fassen das Ergebnis in einem Satz zusammen:

SATZ. *Ist*

$$D = n_1[\alpha_1] + \cdots + n_r[\alpha_r] + n_\infty[\infty]$$

ein Divisor vom Grad ≥ 0 *mit paarweise verschiedenen Zahlen* $\alpha_1, \ldots, \alpha_r$ *und ganzen Zahlen* $n_1, \ldots, n_r, n_\infty$, *definiert man*

$$f = \prod_{i=1}^{r} (x - \alpha_i)^{n_i},$$

so gilt

$$\mathcal{L}(D) = K \cdot \frac{1}{f} + K \cdot \frac{x}{f} + K \cdot \frac{x^2}{f} + \cdots + K \cdot \frac{x^{\operatorname{grad}(D)}}{f},$$

die Funktionen $\frac{x^i}{f}$ *mit* $i = 0, \ldots, \operatorname{grad}(D)$ *bilden also eine* K*-Basis von* $\mathcal{L}(D)$. *Insbesondere gilt*

$$\dim \mathcal{L}(D) = \operatorname{grad}(D) + 1.$$

Beispiel: Wir betrachten $D = [1] + [2] + [3]$. Der Vektorraum $\mathcal{L}(D)$ besteht aus den Funktionen, die in 1,2,3 höchstens jeweils einen Pol 1. Ordnung haben und sonst überall definiert sind. Wir bilden

$$f = (x-1)(x-2)(x-3).$$

Wegen $\operatorname{grad}(D) = 3$ bilden die Funktionen

$$\frac{1}{(x-1)(x-2)(x-3)}, \quad \frac{x}{(x-1)(x-2)(x-3)}, \quad \frac{x^2}{(x-1)(x-2)(x-3)}, \quad \frac{x^3}{(x-1)(x-2)(x-3)}$$

eine Basis von $\mathcal{L}(D)$.

Die Dimensionsaussagen für $\mathcal{L}(D)$ fassen wir nochmals zusammen:

SATZ (Riemann-Roch für $\mathbb{P}^1$). *Für einen Divisor* $D \in \operatorname{Div}(\mathbb{P}^1)$ *gilt*

$$\dim \mathcal{L}(D) = \begin{cases} 0 & \text{für } \operatorname{grad}(D) < 0, \\ \operatorname{grad}(D) + 1 & \text{für } \operatorname{grad}(D) \geq 0. \end{cases}$$

Beispiel: Für $n \in \mathbb{N}$ ist $\mathcal{L}(n[\infty])$ der Vektorraum der Polynome vom Grad $\leq n$. Eine Basis ist $1, x, x^2, \ldots, x^n$, die Dimension also $n + 1$, was mit $\operatorname{grad}(n[\infty]) + 1$ übereinstimmt.

Es gibt einen Satz von Riemann-Roch für nichtsinguläre projektive Kurven, der allerdings deutlich anspruchsvoller ist als der hier gezeigte Satz für $\mathbb{P}^1$.
Wir geben noch eine Darstellung für $\mathcal{L}(D)$ im Fall effektiver Divisoren an, die auf der Partialbruchzerlegung rationaler Funktionen beruht:

SATZ (Partialbruchzerlegung über einem algebraisch abgeschlossenen Grundkörper K). *Jede rationale Funktion $f \in K(x)^*$ hat eine (bis auf Summationsreihenfolge) eindeutige „Partialbruchzerlegung“*

$$\begin{aligned} f &= \left(\frac{b_{1,1}}{x-\alpha_1} + \frac{b_{1,2}}{(x-\alpha_1)^2} + \cdots + \frac{b_{1,n_1}}{(x-\alpha_1)^{n_1}}\right) + \cdots + \left(\frac{b_{r,1}}{x-\alpha_r} + \frac{b_{r,2}}{(x-\alpha_r)^2} + \cdots + \frac{b_{r,n_r}}{(x-\alpha_r)^{n_r}}\right) + \\ &\quad + c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m. \end{aligned}$$

Kürzer geschrieben:

$$f = \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{b_{i,j}}{(x-\alpha_i)^j} + \sum_{k=0}^{m} c_k x^k.$$

Dabei sind $\alpha_i, b_{i,j}, c_k \in K$, $n_i \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_r$ paarweise verschieden und $r, m \in \mathbb{N}_0$.

Beispiele:

$$\begin{aligned} \frac{1}{x^2-1} &= \frac{1}{(x-1)(x+1)} = \frac{\frac{1}{2}((x+1)-(x-1))}{(x-1)(x+1)} = \frac{\frac{1}{2}}{x-1} - \frac{\frac{1}{2}}{x+1}, \\ \frac{1}{x^2+1} &= \frac{1}{(x-i)(x+i)} = \frac{\frac{1}{2i}((x+i)-(x-i))}{(x-i)(x+i)} = \frac{\frac{1}{2i}}{x-i} - \frac{\frac{1}{2i}}{x+i}, \\ \frac{x^3}{x^2-1} &= \frac{\frac{1}{2}}{x-1} + \frac{\frac{1}{2}}{x-1} + x. \end{aligned}$$

Bemerkung: Wir betrachten $f \in K(\mathbb{P}^1)$ mit der Partialbruchzerlegung

$$f = \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{b_{i,j}}{(x-\alpha_i)^j} + \sum_{k=0}^{m} c_k x^k,$$

wobei $\alpha_i, b_{i,j}, c_k \in K$, $n_i \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_r$ paarweise verschieden und $r, m \in \mathbb{N}_0$ sind.
Wir betrachten die Polstellen der Summanden:

- $\frac{1}{(x-\alpha_i)^j}$ hat Ordnung $-j$ in α_i und ist sonst definiert.
- Daher: $\operatorname{ord}_{\alpha_i}(f) \geq -n_i$ mit Gleichheit, falls $b_{i,n_i} \neq 0$.
- x^k hat Ordnung $-k$ in ∞ und ist sonst definiert.
- Daher: $\operatorname{ord}_{\infty}(f) \geq -m$ mit Gleichheit, falls $c_m \neq 0$.
- In allen anderen Punkten gilt $\operatorname{ord}_P(f) \geq 0$.

Daraus ersieht man

$$f \in \mathcal{L}(n_1[\alpha_1] + \cdots + n_r[\alpha_r] + m[\infty]).$$

Durch Betrachtung der Partialbruchzerlegung ist auch umgekehrt leicht zu sehen, dass jedes Element aus $\mathcal{L}(n_1[\alpha_1] + \cdots + n_r[\alpha_r] + m[\infty])$ obige Gestalt hat. Wir fassen zusammen:

SATZ. *Seien $r, m \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_r \in K$ paarweise verschieden, $n_1, \ldots, n_r \in \mathbb{N}$, $n_\infty \in \mathbb{N}_0$. Dann gilt für den effektiven Divisor*

$$D = n_1[\alpha_1] + \cdots + n_r[\alpha_r] + n_\infty[\infty]$$

$$\mathcal{L}(D) = \left\{ \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{b_{i,j}}{(x-\alpha_i)^j} + \sum_{k=0}^{n_\infty} c_k x^k : b_{i,j}, c_k \in K \right\}.$$

Die Funktionen

$$\frac{1}{(x-\alpha_i)^j}, i = 1, \ldots, r, j = 1, \ldots, n_i, \quad x^k, k = 0, \ldots, n_\infty$$

bzw. ausgeschrieben

$$\frac{1}{x-\alpha_1}, \ldots, \frac{1}{(x-\alpha_1)^{n_1}}, \ldots, \frac{1}{x-\alpha_r}, \ldots, \frac{1}{(x-\alpha_r)^{n_r}}, 1, x, \ldots, x^{n_\infty}$$

bilden eine K-Basis von $\mathcal{L}(D)$. Insbesondere gilt $\dim \mathcal{L}(D) = \operatorname{grad}(D) + 1$.

Beispiel: Für $D = 2[3] + 3[2] + 5[\infty]$ ist

$$\frac{1}{x-3}, \frac{1}{(x-3)^2}, \frac{1}{x-2}, \frac{1}{(x-2)^2}, \frac{1}{(x-2)^3}, 1, x, x^2, x^3, x^4, x^5$$

eine K-Basis von $\mathcal{L}(D)$. Beim zuvor dargestellten Vorgehen bildet man

$$f = (x-3)^2(x-2)^3$$

und erhält dann wegen $\operatorname{grad}(D) = 10$ als K-Basis von $\mathcal{L}(D)$

$$\frac{1}{(x-3)^2(x-2)^3}, \quad \frac{x}{(x-3)^2(x-2)^3}, \quad \dots \quad \frac{x^{10}}{(x-3)^2(x-2)^3}.$$

5. Eine Anwendung in der Codierungstheorie

Beim Übertragen von Nachrichten auf elektronischem Weg können Fehler passieren. Was macht man, wenn z.B. die 0-1-Folge

`01001101011000010111010001101000011001010110110101100001011101000110100101101011`

gesendet wird, dafür aber

`00001001111000011011010001101000011001010011110100100001010101000110101101101011`

ankommt?
Die Idee der Codierungstheorie ist es, Redundanz einzufügen, sodass man trotz vorhandener Fehler auf die ursprüngliche Nachricht schließen kann.

Beispiel: Ersetzen wir 0 durch 000 und 1 durch 111, so wird beispielsweise die Folge 0110 zunächst in

$$000 \quad 111 \quad 111 \quad 000$$

übersetzt und dann gesendet. Erhält der Empfänger die Folge

$$010 \quad 111 \quad 011 \quad 000,$$

so liegt es nahe, dass

$$000 \quad 111 \quad 111 \quad 000$$

gemeint war; durch „Fehlerkorrektur“ erhält man also die ursprüngliche Nachricht. (Der „Code“ ist auch unter dem Namen Hamming-Code $[3, 1]$ bekannt.)
Ein $[n, k]$**-Code** C (über $\mathbb{F}_2$) ist ein k-dimensionaler Untervektorraum von $\mathbb{F}_2^n$, er wird gegeben durch eine $k \times n$-Matrix $M = (m_{ij}) \in \mathrm{M}(k \times n, \mathbb{F}_2)$. (Die Zeilen von M bilden eine Basis von C.)
Die zu übertragende Nachricht, die als 0-1-Folge gegeben ist, unterteilt man in eine Folge von Blöcken $(a_1 \dots a_k)$ der Länge k. Der Block $(a_1 \dots a_k)$ wird dann transformiert in

$$(a_1 \dots a_k) \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ \vdots & \vdots & & \vdots \\ m_{k1} & m_{k2} & \dots & m_{kn} \end{pmatrix} = (b_1\, b_2 \dots b_n)$$

und der neue Block $(b_1 \dots b_n)$ wird gesendet.
Beispiel: Der Hamming-Code $[7, 4]$ wird (beispielsweise) gegeben durch folgende Matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(SAGE: `codes.HammingCode(GF(2),3).generator_matrix()`). Je 4 Bits werden in 7 Bits umgewandelt:

```
0000 -> 0000000
0001 -> 0001111
0010 -> 0010110
0011 -> 0011001
0100 -> 0100101
0101 -> 0101010
0110 -> 0110011
0111 -> 0111100
1000 -> 1000011
1001 -> 1001100
1010 -> 1010101
```

```
1011 -> 1011010
1100 -> 1100110
1101 -> 1101001
1110 -> 1110000
1111 -> 1111111
```

Welche Eigenschaften soll ein guter Code haben?

- Gute Fehlerkorrektur.
- Hohe Informationsrate.
- Einfaches Codieren, einfaches Decodieren.

Wir werden die Situation etwas allgemeiner betrachten. Statt des Grundkörpers $\mathbb{F}_2$ werden wir einen allgemeinen Körper K zugrundelegen.
Codes: Ein $[n,k]$**-Code** C über einem Körper K ist ein k-dimensionaler Untervektorraum von K^n. Schreibt man eine Basis von C zeilenweise in eine Matrix, so erhält man eine $k \times n$-Matrix $M \in \mathrm{M}(k \times n, K)$, die auch Erzeugermatrix genannt wird. Eine Folge von k Zahlen aus K, also $(a_1 \dots a_k)$ wird dann zu $(b_1 \dots b_n)$ codiert mit

$$(b_1 \dots b_n) = (a_1 \dots a_k) \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & & \vdots \\ m_{k1} & \dots & m_{kn} \end{pmatrix} : \quad (a_1 \dots a_k) \longrightarrow (b_1 \dots b_n).$$

Hamming-Abstand: Auf K^n definiert man den **Hamming-Abstand** zweier Vektoren $v, w \in K^n$ (mit $v = (v_1, \dots, v_n)$, $w = (w_1, \dots, w_n)$) durch

$$d_{\text{Hamming}}(v,w) = \#\{i : v_i \neq w_i\}.$$

Der Hamming-Abstand gibt also an, an wievielen Stellen sich die Vektoren unterscheiden.

Ist $C \subseteq K^n$ ein $[n,k]$-Code, so definiert man den **Minimalabstand** $d(C)$ des Codes durch

$$d(C) = \min\{d_{\text{Hamming}}(v,w) : v, w \in C, v \neq w\}.$$

Zwei verschiedene Wörter des Codes unterscheiden sich also an mindestens $d(C)$ Stellen. Da C ein Untervektorraum von K^n ist, gilt auch

$$d(C) = \min\{d_{\text{Hamming}}(v,0) : v \in C \setminus \{0\}\}.$$

Man nennt den Code dann auch einen $[n,k,d(C)]$-Code.
Beispiel: Der oben erwähnte Hamming-Code $[7,4]$ über $\mathbb{F}_2$ ist ein $[7,4,3]$-Code.

Beispiel: Wir betrachten in $\mathbb{F}_2^4$ den $\mathbb{F}_2$-Untervektorraum

$$C = \{(x_1,x_2,x_3,x_4) \in \mathbb{F}_2^4 : x_1 + x_2 + x_3 + x_4 = 0\}.$$

Die Elemente von C kann man leicht auflisten:

$$(0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1), (0,1,1,0), (0,1,0,1), (0,0,1,1), (1,1,1,1).$$

Es ist $\dim(C) = 3$ und $d(C) = 2$. Also handelt es sich um einen $[4,3,2]$-Code über $\mathbb{F}_2$.

Goppa-Codes oder algebraisch-geometrische Codes: Goppa hat um 1975 bemerkt, dass man mit algebraischen Kurven interessante Codes konstruieren kann. Wir skizzieren zunächst die Idee:
Gegeben ist eine Kurve C, bei uns $\mathbb{P}^1$, ein Divisor D und Kurvenpunkte $P_1, \dots, P_n$. Dabei soll jede Funktion $f \in \mathcal{L}(D)$ in $P_1, \dots, P_n$ definiert sein. Dann ist

$$\alpha : \mathcal{L}(D) \to K^n, \quad f \mapsto (f(P_1), \dots, f(P_n))$$

eine K-lineare Abbildung. Also ist

$$C = \mathrm{Bild}(\alpha)$$

ein Code. Durch geeignete Parameterwahl kommt man zu interessanten Codes, worauf wir hier aber nicht eingehen wollen.

LEMMA. *Sei* $D = m_1[Q_1] + \dots + m_r[Q_r] \in \mathrm{Div}(\mathbb{P}^1)$ *ein Divisor.*

- *Ist $P \in \mathbb{P}^1 \setminus \{Q_1, \ldots, Q_r\}$, so ist jede Funktion $f \in \mathcal{L}(D)$ in P definiert.*
- *Für paarweise verschiedene Punkte $P_1, \ldots, P_n \in \mathbb{P}^1 \setminus \{Q_1, \ldots, Q_r\}$ gilt*

$$f(P_1) = \cdots = f(P_n) = 0 \quad \Longleftrightarrow \quad f \in \mathcal{L}(D - [P_1] - \cdots - [P_n]).$$

Beweis:

- Ist $f \in \mathcal{L}(D) \setminus \{0\}$, so gilt $\operatorname{div}(f) + D \geq 0$, also $\operatorname{ord}_{Q_j}(f) \geq -m_j$ für $j = 1, \ldots, r$ und $\operatorname{ord}_P(f) \geq 0$ für $P \in \mathbb{P}^1 \setminus \{Q_1, \ldots, Q_r\}$. Dies beweist die Behauptung.
- Es gilt für $f \in \mathcal{L}(D) \setminus \{0\}$:

$$\begin{aligned} f(P_1) = \cdots = f(P_n) = 0 &\iff \operatorname{ord}_{P_1}(f) \geq 1, \ldots, \operatorname{ord}_{P_n}(f) \geq 1 \iff \\ &\iff \operatorname{div}(f) \geq -m_1[Q_1] - \cdots - m_r[Q_r] + [P_1] + \cdots + [P_n] \iff \\ &\iff \operatorname{div}(f) \geq -D + [P_1] + \cdots + [P_n] \iff \\ &\iff \operatorname{div}(f) + D - [P_1] - \cdots - [P_n] \geq 0 \iff \\ &\iff f \in \mathcal{L}(D - [P_1] - \cdots - [P_n]). \end{aligned}$$

  Es folgt die Behauptung. ■

Satz. *Sei $D = m_1[Q_1] + \cdots + m_r[Q_r] \in \mathbb{P}^1$ ein Divisor vom Grad ≥ 0 und $P_1, \ldots, P_n \in \mathbb{P}^1 \setminus \{Q_1, \ldots, Q_r\}$ paarweise verschiedene Punkte mit $n > \operatorname{grad}(D)$. Dann ist*

$$\alpha : \mathcal{L}(D) \to K^n, \quad f \mapsto (f(P_1), \ldots, f(P_n))$$

eine injektive K-lineare Abbildung. $C = \operatorname{Bild}(\alpha)$ ist ein $[n, k, d]$-Code über K mit

$$k = \operatorname{grad}(D) + 1, \quad d = n - \operatorname{grad}(D).$$

(Es ist $k = \dim(C)$ die Dimension von C und $d = d(C)$ der Minimalabstand von C.)

Beweis:

- Das vorangegangene Lemma zeigt, dass die Abbildung α definiert ist. Die Linearität ist dann klar.
- Das Lemma zeigt:

$$\operatorname{Kern}(\alpha) = \mathcal{L}(D - [P_1] - \cdots - [P_n]).$$

  Nun gilt aber $\operatorname{grad}(D - [P_1] - \cdots - [P_n]) = \operatorname{grad}(D) - n < 0$, was $\mathcal{L}(D - [P_1] - \cdots - [P_n]) = 0$ und damit die Injektivität von α liefert.
- Es ist

$$k = \dim(C) = \dim(\operatorname{Bild}(\alpha)) = \dim(\mathcal{L}(D)) \overset{\text{RR}}{=} \operatorname{grad}(D) + 1.$$

- Sei $d = d(C)$. Dann gibt es eine Funktion $f \in \mathcal{L}(D) \setminus \{0\}$, sodass nach eventueller Umnummeriung der Punkte $P_1, \ldots, P_n$ gilt

$$f(P_1) \neq 0, \ldots, f(P_d) \neq 0, \quad f(P_{d+1}) = 0, \ldots, f(P_n) = 0.$$

  Es folgt

$$f \in \mathcal{L}(D - [P_{d+1}] - \cdots - [P_n]) \setminus \{0\},$$

  und damit

$$0 \leq \operatorname{grad}(D - [P_{d+1}] - \cdots - [P_n]) = \operatorname{grad}(D) - (n - d) = \operatorname{grad}(D) - n + d,$$

  also

$$d \geq n - \operatorname{grad}(D).$$

- Wir konstruieren nun eine Funktion, die zeigt, dass die letzte Ungleichung sogar eine Gleichheit ist. Der Divisor

$$D - [P_1] - \cdots - [P_{\operatorname{grad}(D)}]$$

  hat Grad 0, also gibt es eine Funktion

$$f \in \mathcal{L}(D - [P_1] - \cdots - [P_{\operatorname{grad}(D)}]) \setminus \{0\}.$$

  Nach dem Lemma gilt

$$f(P_1) = \cdots = f(P_{\operatorname{grad}(D)}) = 0,$$

und damit

$$d_{\text{Hamming}}(\alpha(f)) \leq n - \text{grad}(D).$$

Dies impliziert

$$d \leq n - \text{grad}(D).$$

Zusammen mit der Abschätzung aus dem letzten Punkt folgt

$$d = n - \text{grad}(D),$$

wie behauptet. ■

Beispiel: Als Grundkörper betrachten wir $\mathbb{F}_5$ (oder $\overline{\mathbb{F}}_5$). Wir wählen

$$P_1 = 1, \quad P_2 = 2, \quad P_3 = 3, \quad P_4 = 4, \quad D = [\infty].$$

Dann ist $n = 4$ und $\text{grad}(D) = 1$, also $n > \text{grad}(D)$. Wir brauchen eine Basis von $\mathcal{L}(D) = \mathcal{L}([\infty])$ und wählen $f_1 = 1$, $f_2 = x$. In der zum Code gehörigen Erzeugermatrix stehen dann die Zahlen $f_i(\alpha)$ mit $i = 1, 2$ und $\alpha \in \{1, 2, 3, 4\}$:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Nach unserem Satz hat der Code Dimension $k = \text{grad}(D) + 1 = 2$ und Minimalabstand $d(C) = n - \text{grad}(D) = 3$. Es handelt sich also um einen $[4, 2, 3]$-Code über $\mathbb{F}_5$.

```
00 -> 0000
10 -> 1111
20 -> 2222
30 -> 3333
40 -> 4444
01 -> 1234
11 -> 2340
21 -> 3401
31 -> 4012
41 -> 0123
02 -> 2413
12 -> 3024
22 -> 4130
32 -> 0241
42 -> 1302
03 -> 3142
13 -> 4203
23 -> 0314
33 -> 1420
43 -> 2031
04 -> 4321
14 -> 0432
24 -> 1043
34 -> 2104
44 -> 3210
```

(SAGE kennt den Code als `codes.ReedSolomonCode(GF(5),4,2)`.

Literatur: [**Geer-Lint**], [**Luetkebohmert**]

KAPITEL 6

Algebraische Varietäten - vertieft

Im ersten Teil der Vorlesung haben wir versucht, mit minimalen algebraischen Begriffen auszukommen. Im zweiten Teil der Vorlesung werden wir nun etwas mehr Algebra verwenden.

- Wir legen im Folgenden einen Körper K zugrunde. Sei $\overline{K}$ ein algebraischer Abschluss von K. Wir setzen voraus, dass $\overline{K}$ separabel über K ist, d.h. jedes irreduzible Polynom aus $K[x]$ zerlegt sich über $\overline{K}$ in der Form
$$f = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r)$$
mit paarweise verschiedenen Zahlen $\alpha_1,\dots,\alpha_r \in \overline{K}$. Ein solcher Körper heißt **vollkommener Körper** (engl. **perfect field**).
- Im Fall eines vollkommenen Körpers ist $\overline{K}$ galoissch über K. Mit G_K werde die Galoisgruppe von $\overline{K}$ über K bezeichnet. Es gilt:
$$K = \{a \in \overline{K} : \sigma a = a \text{ für alle } \sigma \in G_K\}.$$
- Beispiele vollkommener Körper: Algebraisch abgeschlossene Körper, Körper der Charakteristik 0 und endliche Körper.
- Beispiel eines Körpers, der nicht vollkommen ist: Der rationale Funktionenkörper in einer Variablen über einem endlichen Körper $\mathbb{F}_p$, also $\mathbb{F}_p(t) = \{\frac{g(t)}{h(t)} : g(t), h(t) \in \mathbb{F}_p[t]\}$ ist nicht vollkommen, da beispielsweise das Polynom $x^p - t$ zwar irreduzibel über dem Körper, aber nicht separabel ist.
- Der Polynomring $K[x_1,\dots,x_n]$ über einem Körper K ist ein **noetherscher Ring**, d.h. jedes Ideal ist endlich erzeugt.
- Ein Ideal $\mathfrak{p}$ eines kommutativen Rings R (mit Eins) heißt **Primideal**, wenn der Faktorring $R/\mathfrak{p}$ ein Integritätsring ist. Äquivalent dazu ist, dass $\mathfrak{p} \neq R$ und folgende Implikation gilt:
$$ab \in \mathfrak{p} \quad \Longrightarrow \quad a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}.$$
- Ein Ideal $\mathfrak{m}$ eines kommutativen Rings R (mit Eins) heißt **maximales Ideal**, wenn der Faktorring $R/\mathfrak{m}$ ein Körper ist.
- Die Galoisgruppe G_K operiert auf den Polynomen aus $\overline{K}[x_1,\dots,x_n]$: Für $f = \sum a_{i_1,\dots,i_n} x_1^{i_1}\dots x_n^{i_n}$ und $\sigma \in G_K$ sei
$$\sigma(f) = \sum \sigma(a_{i_1,\dots,i_n}) x_i^{i_1}\dots x_n^{i_n}.$$
Dann gilt:
$$K[x_1,\dots,x_n] = \{f \in \overline{K}[x_1,\dots,x_n] : \sigma f = f \text{ für alle } \sigma \in G_K\}.$$
Für $a_1,\dots,a_n \in \overline{K}$ gilt dann
$$\sigma(f(a_1,\dots,a_n)) = (\sigma(f))(\sigma(a_1),\dots,\sigma(a_n)).$$

1. Affine Varietäten

DEFINITION. *Der n-dimensionale affine Raum ist*
$$\mathbb{A}^n = \{P = (a_1,\dots,a_n) : a_i \in \overline{K}\}.$$
Die Menge der K-rationalen Punkte von $\mathbb{A}^n$ ist
$$\mathbb{A}^n(K) = \{P = (a_1,\dots,a_n) \in \mathbb{A}^n : a_i \in K\}.$$

Die Galoisgruppe G_K operiert auf $\mathbb{A}^n$ durch $\sigma(a_1,\dots,a_n)=(\sigma a_1,\dots,\sigma a_n)$. Dann gilt

$$\mathbb{A}^n(K)=\{P\in\mathbb{A}^n : \sigma P=P \text{ für alle } \sigma\in G_K\}.$$

DEFINITION. *Eine Teilmenge $V\subseteq\mathbb{A}^n$ heißt algebraische Menge in $\mathbb{A}^n$, falls es Polynome $f_1,\dots,f_r\in\overline{K}[x_1,\dots,x_n]$ gibt mit*

$$V=\{P\in\mathbb{A}^n : f_1(P)=\cdots=f_r(P)=0\}.$$

Man sagt, eine algebraische Menge V ist über K definiert, falls es Polynome $g_1,\dots,g_s\in K[x_1,\dots,x_n]$ gibt mit

$$V=\{P\in\mathbb{A}^n : g_1(P)=\cdots=g_s(P)=0\}.$$

Man schreibt dann auch V/K. In diesem Fall heißt

$$V(K)=V\cap\mathbb{A}^n=\{P\in K^n : g_1(P)=\cdots=g_s(P)=0\}$$

die Menge der K-rationalen Punkte von V.

Ist $V\subseteq\mathbb{A}^n$ über K definiert, d.h. $V=\{f_1=\cdots=f_r\}$ mit Polynomen $f_1,\dots,f_r\in K[x_1,\dots,x_n]$, so operiert G_K auf V, denn für $\sigma\in G_K$ gilt:

$$P\in V\Rightarrow f_i(P)=0\Rightarrow 0=\sigma(f_i(P))=f_i(\sigma(P))\Rightarrow\sigma(P)\in V.$$

Beispiele:

(1) Sei $f=-3y+2xy+3y^2$ und $g=4x+5y+x^2+xy$. Dann ist

$$X=\{f=g=0\}=\{(0,0),(-4,0),(\frac{-5+\sqrt{-35}}{2},\frac{8-\sqrt{-35}}{3}),(\frac{-5-\sqrt{-35}}{2},\frac{8+\sqrt{-35}}{3})\}.$$

Die Galoisgruppe $G_{\mathbb{Q}}$ operiert offensichtlich auf X.

(2) Sei $f=-3+3y+4x^2-5xy$ und $g=-3-3x+xy-5y^2$. Dann ist

$$X=\{f=g=0\}=\{(-2,-1)\}\cup\{(\alpha,4\alpha^2+\alpha-3) : 20\alpha^3-11\alpha^2-18\alpha+12=0\}.$$

(Die Galoisgruppe des Polynoms $20x^3-11x^2-18x+12$ ist die S_3.)

(3) Ist $X\subseteq\mathbb{A}^2$ eine über $\mathbb{Q}$ definierte algebraische Menge, und ist $(\sqrt{2},\sqrt{3})\in X$, so folgt

$$(\pm\sqrt{2},\pm\sqrt{3})\in X.$$

DEFINITION. *Sei $V\subseteq\mathbb{A}^n$ eine algebraische Menge. Dann heißt*

$$I(V)=\{f\in\overline{K}[x_1,\dots,x_n] : f(P)=0 \textit{ für alle } P\in V\}$$

das **Ideal von** *V. Weiter setzt man*

$$I(V/K)=I(V)\cap K[x_1,\dots,x_n].$$

Bemerkungen:

(1) Ist $V=\{f_1=\cdots=f_r=0\}$, so verschwinden natürlich auch alle Polynome aus dem Ideal $(f_1,\dots,f_r)$ auf V. Gibt es noch mehr Polynome? Der **Hilbertsche Nullstellensatz** besagt, dass

$$I(V)=\sqrt{(f_1,\dots,f_r)}$$

gilt. Dies setzt die Betrachtung über $\overline{K}$ voraus. Dabei ist

$$\sqrt{(f_1,\dots,f_r)}=\{f\in\overline{K}[x_1,\dots,x_n] : f^m\in(f_1,\dots,f_r) \text{ für ein } m\in\mathbb{N}\}$$

das Radikalideal von $(f_1,\dots,f_r)$. (Statt $\sqrt{(f_1,\dots,f_r)}$ findet man auch die Schreibweise $\mathrm{rad}((f_1,\dots,f_r))$.)

(2) Im Polynomring $\overline{K}[x_1,\dots,x_n]$ gilt

$$I(V/K)\overline{K}[x_1,\dots,x_n]\subseteq I(V).$$

Gleichheit gilt genau dann, wenn V über K definiert ist.

DEFINITION. *Eine nichtleere algebraische Menge $V \subseteq \mathbb{A}^n$ heißt* **(absolut) irreduzibel**, *falls sie nicht als echte Vereinigung weiterer algebraischer Mengen $V_1, V_2 \subseteq \mathbb{A}^n$ geschrieben werden kann, d.h. $V = V_1 \cup V_2$ impliziert $V = V_1$ oder $V = V_2$. (Die leere Menge wird nicht als irreduzibel betrachtet.) Fordert man, dass V, V_1, V_2 über K definiert sind, so nennt man V* **irreduzibel über** K.

Bemerkung: Sei $f \in K[x_1, \ldots, x_n]$ und $V = \{f = 0\} \subseteq \mathbb{A}^n$. Ist f über K irreduzibel, so ist V über K irreduzibel. Ist f über $\overline{K}$ irreduzibel, so ist V absolut irreduzibel.

Beispiel: $X = \{x^2 = 2y^2\}$ ist über $\mathbb{Q}$ irreduzibel, nicht aber absolut irreduzibel.

SATZ. *Jede algebraische Menge V ist Vereinigung von endlich vielen irreduziblen:*

$$V = V_1 \cup \cdots \cup V_r.$$

Fordert man noch $V_i \not\subseteq V_j$ für $i \neq j$, so ist diese Darstellung bis auf die Reihenfolge eindeutig. Die V_i's heißen **irreduzible Komponenten** *von V.*

Beispiel: Sei $V = \{f = 0\}$ mit $f \in \overline{K}[x_1, \ldots, x_n]$. Da $\overline{K}[x_1, \ldots, x_n]$ ein faktorieller Ring ist, hat man eine (bis auf Konstanten eindeutige) Zerlegung

$$f = f_1^{e_1} \ldots f_r^{e_r},$$

wo die f_i's irreduzible Polynome sind und $e_i \geq 1$. Dann gilt:

$$V = \{f = 0\} = \{f_1 = 0\} \cup \cdots \cup \{f_r = 0\}.$$

Die algebraischen Mengen $\{f_i = 0\}$ sind die irreduziblen Komponenten von V.

Bemerkung: Sei X über K definiert, über K irreduzibel, aber nicht absolut irreduzibel. Sei $V = \{f_1 = \cdots = f_r = 0\}$ eine irreduzible Komponente von X über $\overline{K}$ und für $\sigma \in G_K$

$$V_\sigma = \{\sigma f_1 = \cdots = \sigma f_r = 0\}.$$

Dann gilt

$$X = V_{\sigma_1} \cup \cdots \cup V_{\sigma_s}.$$

$W = V_{\sigma_1} \cap \cdots \cap V_{\sigma_s}$ ist über K definiert und $X(K) \subseteq W(K)$.

Beispiel: $V = \{3 - 3y + x^2 + xy + y^2 = 0\}$ ist über $\mathbb{Q}$ definiert und über $\mathbb{Q}$ irreduzibel. Über $\mathbb{Q}(\sqrt{-3})$ erhält man die Zerlegung

$$V = \{y = \frac{-1 + \sqrt{-3}}{2}x + \frac{3 + \sqrt{-3}}{2}\} \cup \{y = \frac{-1 - \sqrt{-3}}{2}x + \frac{3 - \sqrt{-3}}{2}\}.$$

Man sieht dann $V(\mathbb{Q}) = \{(-1, 2)\}$.

SATZ. *Sei $V \subseteq \mathbb{A}^n$ eine algebraische Menge. V ist genau dann (absolut) irreduzibel, wenn $I(V)$ ein Primideal in $\overline{K}[x_1, \ldots, x_n]$ ist.*

DEFINITION. *Eine (absolut) irreduzible Teilmenge von $\mathbb{A}^n$ heißt eine* **affine Varietät**.

DEFINITION. *Sei V eine über K definierte affine Varietät in $\mathbb{A}^n$. Dann heißt*

$$K[V] = K[x_1, \ldots, x_n]/I(V/K)$$

der **affine Koordinatenring von V (über K)**. *$K[V]$ ist ein Integritätsring. Sein Quotientenkörper $K(V)$ heißt der* **Funktionenkörper von** V/K.

Interpretation als Funktionen: Sei V eine affine Varietät in $\mathbb{A}^n$. Die Polynome aus $\overline{K}[x_1, \ldots, x_n]$ können wir als Funktionen $V \to \overline{K}$ betrachten. Für zwei Polynome f, g gilt:

$$\begin{aligned} & f \text{ und } g \text{ liefern die gleiche Funktion auf } V \quad \Longleftrightarrow \\ \Longleftrightarrow \quad & f - g \text{ verschwindet auf } V \quad \Longleftrightarrow \\ \Longleftrightarrow \quad & f - g \in I(V) \quad \Longleftrightarrow \quad f \equiv g \bmod I(V) \quad \Longleftrightarrow \\ \Longleftrightarrow \quad & f = g \text{ als Elemente von } \overline{K}[V]. \end{aligned}$$

Die Elemente aus $\overline{K}[V]$ können also als Funktionen auf V betrachtet werden.

DEFINITION. *Sei $V \subseteq \mathbb{A}^n$ eine Varietät. Dann wird die* **Dimension von** V *definiert als*

$$\dim V = \max\{n : V_0 \subset V_1 \subset \cdots \subset V_n = V, V_i \text{ irreduzibel}\}.$$

Bemerkung: Die Dimension von V berechnet sich auch als Transzendenzgrad von $\overline{K}(V)$ über $\overline{K}$.

Beispiele:

(1) $\overline{K}[\mathbb{A}^n] = \overline{K}[x_1, \ldots, x_n]$. $\mathbb{A}^n$ hat Dimension n.
(2) Sei $f \in \overline{K}[x_1, \ldots, x_n]$ ein irreduzibles Polynom. Dann ist $V = \{f = 0\}$ eine Varietät der Dimension $n - 1$. Außerdem gilt
$$\overline{K}[V] = \overline{K}[x_1, \ldots, x_n]/(f).$$

DEFINITION. *Sei $V \subseteq \mathbb{A}^n$ eine Varietät, $I(V) = (f_1, \ldots, f_r)$ und $P \in V$. Man sagt V ist* **nichtsingulär (oder glatt) in** P*, falls gilt*

$$\dim V = n - \operatorname{Rang} \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(P) & \ldots & \frac{\partial f_1}{\partial x_n}(P) \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial x_1}(P) & \ldots & \frac{\partial f_r}{\partial x_n}(P) \end{pmatrix}.$$

Ist V in jedem Punkt nichtsingulär, so heißt V **nichtsingulär**.

Beispiel: Sei $f(x, y) \in \overline{K}[x, y]$ ein irreduzibles Polynom. Dann ist $V = \{f = 0\}$ eine 1-dimensionale affine Varietät, eine Kurve. V ist genau dann nichtsingulär in $P \in V$, wenn

$$(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) \neq 0.$$

Dann ist $\frac{\partial f}{\partial x}(P)(x - x_P) + \frac{\partial f}{\partial y}(P)(y - y_P) = 0$ die Tangente in $P = (x_P, y_P)$.

Beispiel: $y^2 = x^2 + x^3$ und $y^2 = x^3$ sind jeweils singulär in $(0, 0)$.

DEFINITION. *Sei V eine affine Varietät und $P \in V$. Dann heißt*

$$\overline{K}[V]_P = \{\frac{f}{g} \in \overline{K}(V) : f, g \in \overline{K}[V], g(P) \neq 0\}$$

der **lokale Ring von** V **in** P.

Der lokale Ring von V in P besteht also aus den Funktionen des Funktionenkörpers, die in P definiert sind. Offensichtlich gilt:

$$\overline{K}[V] \subseteq \overline{K}[V]_P \subseteq \overline{K}(V).$$

Beispiele:

(1) Wir wissen bereits $K[\mathbb{A}^2] = K[x,y]$ und

$$K(\mathbb{A}^2) = K(x,y) = \{\frac{f(x,y)}{g(x,y)} : f,g \in K[x,y]\}.$$

Für $P = (2,-1)$ gilt dann

$$K[\mathbb{A}^2]_P = \{\frac{f(x,y)}{g(x,y)} : f,g \in K[x,y], g(2,-1) \neq 0\}.$$

(2) Sei $X = \{y^2 = x^3\} \subseteq \mathbb{A}^2$. Dann ist $K[X] = K[x,y]/(y^2 - x^3)$. Jedes Element aus $K[X]$ hat die Gestalt $a(x) + b(x)y$ mit Polynomen $a, b \in K[x]$. Wir betrachten die Funktion $f = \frac{y}{x}$. Sie ist definiert für alle $P \neq (0,0)$. Für f^2 gilt im Funktionenkörper:

$$f^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x,$$

also ist f^2 in allen Punkten definiert, auch in $(0,0)$.

2. Projektive Varietäten

DEFINITION. *Auf* $\mathbb{A}^{n+1} \setminus \{(0,\dots,0)\}$ *wird durch*

$$(x_0,\dots,x_n) \sim (y_0,\dots,y_n) \iff x_i = \lambda y_i \text{ für ein } \lambda \in \overline{K}^\times \text{ und alle } i$$

eine Äquivalenzrelation definiert. Die Äquivalenzklasse von $(x_0,\dots,x_n)$ *wird mit* $(x_0 : \cdots : x_n)$ *bezeichnet. Die* x_i*'s heißen homogene Koordinaten von* $(x_0 : \cdots : x_n)$*. Die Menge der Äquivalenzklassen heißt* n*-dimensionaler projektiver Raum (über* K*):*

$$\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = \{(x_0 : \cdots : x_n) : x_i \in \overline{K}, (x_0,\dots,x_n) \neq 0\}.$$

Die Menge der K*-rationalen Punkte von* $\mathbb{P}^n$ *ist*

$$\mathbb{P}(K) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n : x_i \in K\}.$$

Beispiel: Es gilt

$$\mathbb{P}^n(\mathbb{Q}) = \{(a_0 : \cdots : a_n) : a_i \in \mathbb{Z}, \mathrm{ggT}(a_0,\dots,a_n) = 1\}.$$

Bemerkung: Aus $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(K)$ folgt noch nicht $x_i \in K$, wie das Beispiel $(0 : \sqrt{2}) = (0 : 1) \in \mathbb{P}^1(\mathbb{Q})$ zeigt. Dies ändert sich, wenn man eine der homogenen Koordinaten zu 1 normiert. Ist $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\overline{K})$ und $x_i \neq 0$, so nennt man

$$K(P) = K(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i})(\subseteq \overline{K})$$

den minimalen Definitionskörper von P über K. Die Galoisgruppe operiert natürlich auch auf $\mathbb{P}^n(\overline{K})$ und man sieht schnell

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n : \sigma P = P \text{ für alle } \sigma \in G_K\}$$

und

$$K(P) = \text{ Fixkörper von } \{\sigma \in G_K : \sigma P = P\}.$$

DEFINITION. *Eine Teilmenge* $V \subseteq \mathbb{P}^n$ *heißt algebraische Teilmenge in* $\mathbb{P}^n$*, falls es homogene Polynome* $f_1,\dots,f_r \in \overline{K}[x_0,\dots,x_n]$ *gibt mit*

$$V = \{P \in \mathbb{P}^n : f_1(P) = \cdots = f_r(P) = 0\} = \{f_1 = \cdots = f_r = 0\}.$$

Man sagt, die algebraische Menge $V \subseteq \mathbb{P}^n$ *ist über* K *definiert, falls es Polynome* $g_1,\dots,g_s \in K[x_0,\dots,x_n]$ *gibt mit* $V = \{g_1 = \cdots = g_s = 0\}$*. In diesem Fall heißt*

$$V(K) = V \cap \mathbb{P}^n(K)$$

die Menge der K*-rationalen Punkte von* V*.*

Genau wie im affinen Fall definiert man, wann eine algebraische Teilmenge **irreduzibel** heißt.

DEFINITION. *Eine* **projektive Varietät** *ist eine irreduzible algebraische Menge in einem* $\mathbb{P}^n$.

Das Ideal $I(V)$ einer algebraischen Menge $V \subseteq \mathbb{P}^n$ ist das Ideal, das von allen homogenen Polynomen $f \in \overline{K}[x_0, \ldots, x_n]$ erzeugt wird, die auf V verschwinden. Dann gilt:

$$V \subseteq \mathbb{P}^n \text{ ist projektive Varietät } \iff I(V) \text{ ist Primideal.}$$

Wieder kann man jede algebraische Teilmenge des $\mathbb{P}^n$ in eine endliche Vereinigung von irreduziblen Komponenten zerlegen.

Zariski-Topologie:

- Sind $V = \{f_1 = \cdots = f_r = 0\}$ und $W = \{g_1 = \cdots = g_s = 0\}$ algebraische Mengen, so auch
$$V \cup W = \{f_1 g_1 = \cdots = f_1 g_s = \cdots = f_r g_1 = \cdots = f_r g_s = 0\}.$$
- Seien $V_i = \{f_{i1} = \cdots = f_{ir_i} = 0\}$, $i \in I$ algebraische Mengen. Nach dem Hilbertschen Basissatz ist das Ideal $(f_{ij} : i \in I, 1 \leq j \leq r_i)$ endlich erzeugt, d.h. es gibt Polynome $g_1, \ldots, g_s$ mit $(f_{ij} : i \in I, 1 \leq j \leq r_i) = (g_1, \ldots, g_s)$ und damit

$\cap_{i \in I} V_i = \{P \in \mathbb{P}^n : f_{ij}(P) = 0 \text{ für alle } i \in I \text{ und alle } j = 1, \ldots, r_i\} = \{g_1 = \cdots = g_s = 0\}$.

  Also ist auch $\cap_{i \in I} V_i$ eine algebraische Menge.
- Weiter sind $\emptyset = \{1 = 0\}$ und $\mathbb{P}^n = \{0 = 0\}$ algebraische Mengen.

Die algebraischen Teilmengen des $\mathbb{P}^n$ erfüllen damit die Axiome für die abgeschlossenen Teilmengen einer Topologie. Man nennt diese Topologie die Zariski-Topologie auf dem $\mathbb{P}^n$. (Das gleiche gilt natürlich auch auf dem $\mathbb{A}^n$.) Damit können wir jetzt topologische Begriffe verwenden. Teilmengen des $\mathbb{P}^n$ denken wir uns mit der induzierten Topologie versehen. Dass diese Topologie etwas ungewöhnlich ist, zeigen folgende Beispiele:

Beispiel: Sei $X \subseteq \mathbb{P}^n$ eine projektive Varietät und $U, V \subseteq X$ zwei offene nichtleere Teilmengen von X. Dann gilt $U \cap V \neq \emptyset$.
Beweis: Wäre $U \cap V = \emptyset$, so hätte man

$$X = (X \setminus U) \cup (X \setminus V).$$

$X \setminus U$ und $X \setminus V$ sind abgeschlossene Mengen von X, also algebraische Mengen des $\mathbb{P}^n$. Da X irreduzibel ist, folgt $X = X \setminus U$ oder $X = X \setminus V$, d.h. $U = \emptyset$ oder $V = \emptyset$, ein Widerspruch zur Voraussetzung. ■

Beispiel: Die abgeschlossenen Teilmengen des $\mathbb{P}^1$ sind $\emptyset$, $\mathbb{P}^1$ und alle endlichen Teilmengen.

Wir wollen nun den $\mathbb{P}^n$ betrachten. Sei $0 \leq i \leq n$ gegeben. Dann ist $H_i = \{x_i = 0\}$ abgeschlossen und $U_i = \mathbb{P}^n \setminus H_i = \{x_i \neq 0\}$ offen in $\mathbb{P}^n$. Für $(x_0 : \cdots : x_n) \in U_i$ gilt:

$$(x_0 : \cdots : x_{i-1} : x_i : x_{i+1} : \cdots : x_n) = (\frac{x_0}{x_i} : \cdots : \frac{x_{i-1}}{x_i} : 1 : \frac{x_{i+1}}{x_i} : \cdots : \frac{x_n}{x_i}).$$

Definiert man also

$$\phi_i : \mathbb{A}^n \to U_i, \quad (y_1, \ldots, y_n) \mapsto (y_1 : \cdots : y_{i-1} : 1 : y_{i+1} : \cdots : y_n)$$

und

$$\psi_i : U_i \to \mathbb{A}^n, \quad (x_0 : \cdots : x_{i-1} : x_i : x_{i+1} : \cdots : x_n) \mapsto (\frac{x_0}{x_i} : \cdots : \frac{x_{i-1}}{x_i} : \frac{x_{i+1}}{x_i} : \cdots : \frac{x_n}{x_i}),$$

so sind ϕ_i und ψ_i invers zueinander. Wir können also $\mathbb{A}^n$ als offene Teilmenge des $\mathbb{P}^n$ betrachten. Oft wählen wir $i = 0$, d.h. wir denken uns $\mathbb{A}^n \subset \mathbb{P}^n$ mit $(x_1, \ldots, x_n) \simeq (1 : x_1 : \cdots : x_n)$.

Ist $V \subseteq \mathbb{P}^n$ eine projektive algebraische Menge, gegeben durch

$$V = \{f_1(x_0, \ldots, x_n) = \cdots = f_r(x_0, \ldots, x_n) = 0\},$$

wo die f_i's homogene Polynome sind, so ist $V \cap \mathbb{A}^n$ eine affine algebraische Menge, gegeben durch die Gleichungen

$$V \cap \mathbb{A}^n = \{f_1(1, x_1, \ldots, x_n) = \cdots = f_r(1, x_1, \ldots, x_n) = 0\}.$$

Wichtiger ist die Umkehrung:

DEFINITION. *Ist $V \subseteq \mathbb{A}^n$ eine affine algebraische Menge, so denken wir uns V mit $V \subseteq \mathbb{A}^n \subset \mathbb{P}^n$ als Teilmenge des $\mathbb{P}^n$. Der topologische Abschluss $\overline{V}$ von V in $\mathbb{P}^n$ heißt der* **projektive Abschluss von** V.

Wie berechnet man den projektiven Abschluss? Dazu brauchen wir das Homogenisieren von Polynomen. Sei $f(x_1, \ldots, x_n) \in \overline{K}[x_1, \ldots, x_n]$ ein Polynom vom Grad d. Das homogenisierte Polynom ist dann

$$f^*(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}).$$

Man kann dies auch explizit ausschreiben: Ist

$$f = \sum_{i_1+\cdots+i_n \leq d} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

so ist

$$f^* = \sum_{i_0+i_1+\cdots+i_n = d} a_{i_1 \ldots i_n} x_0^{i_0} x_1^{i_1} \ldots x_n^{i_n}.$$

Damit gilt nun: Sei $V \subseteq \mathbb{A}^n$ eine algebraische Menge mit

$$I(V) = (f_1, \ldots, f_r).$$

Seien $g_1, \ldots, g_s \in \overline{K}[x_0, \ldots, x_n]$ homogene Polynome mit

$$(f^* : f \in I(V)) = (g_1, \ldots, g_s).$$

Dann ist

$$\overline{V} = \{g_1 = \cdots = g_s = 0\}.$$

Im Allgemeinen gilt nur

$$\overline{V} \subseteq \{f_1^* = \cdots = f_r^* = 0\}.$$

Beispiel: Für $V = \{(0,0)\} \subseteq \mathbb{A}^2$ gilt

$$I(V) = (x, y - x^2).$$

Die Homogenisierung von x und $y - x^2$ ist x_1 und $x_0 x_2 - x_1^2$ und

$$\{x_1 = 0, x_0 x_2 - x_1^2 = 0\} = \{(1:0:0), (0:1:0\} \supsetneq \overline{V} = \{(1:0:0)\}.$$

SATZ. (1) *Ist V eine affine Varietät, so ist $\overline{V}$ eine projektive Varietät und $V = \overline{V} \cap \mathbb{A}^n$. Ist V über K definiert, so auch $\overline{V}$.*

(2) *Ist W eine projektive Varietät, so ist entweder $W \cap \mathbb{A}^n = \emptyset$ oder $W \cap \mathbb{A}^n$ eine affine Varietät und $W = \overline{W \cap \mathbb{A}^n}$. Ist W über K definiert, so auch $W \cap \mathbb{A}^n$.*

Auf diese Weise definiert jede affine Varietät eindeutig eine projektive Varietät. Oft werden wir projektive Varietäten V durch affine Gleichungen angeben, weil dies etwas einfacher aussieht. Die Punkte $V \cap H_0$ heißen auch unendlich ferne Punkte der Varietät.

Die Dimension einer projektiven Varietät wird definiert wie im affinen Fall.

DEFINITION. *Sei V/K eine projektive Varietät. Wähle $\mathbb{A}^n \subseteq \mathbb{P}^n$ mit $V \cap \mathbb{A}^n \neq \emptyset$. Der* **Funktionenkörper von** V *wird definiert als*

$$K(V) = K(V \cap \mathbb{A}^n).$$

(Eine andere Wahl von $\mathbb{A}^n \subseteq \mathbb{P}^n$ liefert kanonisch isomorphe Körper.)

Bemerkung: Man kann den Funktionenkörper $K(V)$ einer projektiven Varietät auch noch etwas anders definieren, nämlich als Menge aller Quotienten $\frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}$ homogener Polynome gleichen Grades mit $g \notin I(V)$ und der Relation $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ genau dann, wenn $f_1 g_2 - f_2 g_1 \in I(V)$.

DEFINITION. *Sei V eine projektive Varietät und $P \in V$. Wähle $\mathbb{A}^n \subseteq \mathbb{P}^n$ mit $P \in \mathbb{A}^n$. (Dann ist $V \cap \mathbb{A}^n$ eine offene Umgebung von P in V.)*

(1) *P heißt singulärer Punkt von V, falls P singulärer Punkt von $V \cap \mathbb{A}^n$ ist; andernfalls nichtsingulär oder glatt.*
(2) *Der lokale Ring von V in $P \in V$ ist der lokale Ring von $V \cap \mathbb{A}^n$ in P. Er besteht aus allen Funktionen aus $\overline{K}(V)$, die in P definiert sind.*

Bemerkung: Ist $V = \{f(x_0, \ldots, x_n) = 0\} \subseteq \mathbb{P}^n$, wo f ein irreduzibles homogenes Polynom ist, so ist die Menge der Singularitäten von V gegeben durch

$$V_{\text{sing}} = \{f = \frac{\partial f}{\partial x_0} = \cdots = \frac{\partial f}{\partial x_n} = 0\}.$$

Für homogene Polynome gilt die Eulersche Relation

$$d \cdot f = \sum_{i=0}^{n} x_i \frac{\partial f}{\partial x_i},$$

wenn d der Grad von f ist. Hat also d nichts mit der Charakteristik von K zu tun, so kann man auf die Gleichung f in V_{sing} verzichten.

Der folgende Satz gibt einen fundamentalen Unterschied zwischen affinen und projektiven Varietäten an:

SATZ. (1) *Ist $V \subseteq \mathbb{A}^n$ eine affine Varietät und $f \in \overline{K}(V)$ eine Funktion, die in allen Punkten $P \in V$ definiert ist, dann ist $f \in \overline{K}[V]$.*
(2) *Ist $W \subseteq \mathbb{P}^n$ eine projektive Varietät und $g \in \overline{K}(V)$ eine Funktion, die in allen Punkten $P \in W$ definiert ist, dann gilt $g \in \overline{K}$.*

Beispiele:

(1) Eine Funktion f, die in allen Punkten von $\mathbb{A}^1$ definiert ist, ist eine Polynomfunktion: $f \in \overline{K}[\mathbb{A}^1] = \overline{K}[x]$.
(2) Eine Funktion f, die in allen Punkten von $\mathbb{P}^1$ definiert ist, ist konstant: $f \in \overline{K}$.

3. Produkte von Varietäten

Was sind die algebraischen Teilmengen von $\mathbb{P}^m \times \mathbb{P}^n$?

DEFINITION. *Ein Polynom $f \in \overline{K}[x_0, \ldots, x_m, y_0, \ldots, y_n]$ heißt bihomogen vom Grad (d, e) bzgl. $x_0, \ldots, x_m$ und $y_0, \ldots, y_n$, wenn es die Gestalt*

$$f = \sum_{i_0 + \cdots + i_m = d} \sum_{j_0 + \cdots + j_n = e} a_{i_0 \ldots i_m j_0 \ldots j_n} x_0^{i_0} \ldots x_m^{i_m} y_0^{j_0} \ldots y_n^{j_n}$$

hat. D.h. f ist homogen vom Grad d in den Variablen x_i und homogen vom Grad e in den Variablen y_j.

DEFINITION. *Auf $\mathbb{P}^m \times \mathbb{P}^n$ nennen wir eine Menge abgeschlossen oder algebraisch, falls sie Nullstellenmenge bihomogener Polynome $f_\ell(x, y)$ ist. Dies induziert eine Topologie, die wir wieder Zariski-Topologie nennen.*

Bemerkungen:

(1) Analog werden Produkte zwischen projektiven und affinen Varietäten definiert.
(2) Die Zariski-Topologie auf $\mathbb{P}^m \times \mathbb{P}^n$ ist nicht die Produkttopologie.

4. Abbildungen zwischen Varietäten

DEFINITION. *Seien V und W projektive Varietäten, $W \subseteq \mathbb{P}^n$. Eine* **rationale Abbildung** $\phi : V \to W$ *wird gegeben durch Funktionen $f_i \in \overline{K}(V)$, nicht alle 0, durch*

$$\phi = (f_0 : \cdots : f_n)$$

mit der Eigenschaft $F(f_0, \ldots, f_n) = 0$ für alle $F \in I(W)$. ϕ heißt definiert in $P \in V$, falls es eine Funktion $g \in \overline{K}(V)$ gibt mit der Eigenschaft:

- *Alle gf_i sind definiert in P,*
- *für mindestens ein i ist $(gf_i)(P) \neq 0$.*
- *Dann setzt man*

$$\phi(P) = ((gf_0)(P) : \cdots : (gf_n)(P)).$$

Sind V und W über K definiert, so heißt ϕ definiert über K, falls die $f_i \in K(V)$ gewählt werden können.

Beispiel: Wir betrachten $X \subseteq \mathbb{P}^2$ gegeben durch die Gleichung $2x^2 + 3y^2 - 5 = 0$, d.h.

$$X = \{2x_1^2 + 3x_2^2 = 5x_0^2\}.$$

Affine Koordinaten führen wir ein durch

$$(x_0 : x_1 : x_2) = (1 : x : y) = (u : 1 : v), \quad \text{d.h.} \quad x = \frac{x_1}{x_0}, \quad y = \frac{x_2}{x_0}, \quad u = \frac{x_0}{x_1}, \quad v = \frac{x_2}{x_1}.$$

Dann sind $x, y, u, v \in K(X)$ und $x = \frac{1}{u}, y = \frac{v}{u}$. Wir definieren die rationale Abbildung $\phi : X \to \mathbb{P}^1$ durch

$$\phi = (1 : \frac{y-1}{x-1}).$$

Wegen $\phi = (x - 1 : y - 1)$ ist ϕ sicher definiert in der offenen Menge $\{x_0 \neq 0\} \setminus \{(1 : 1 : 1)\}$. Wegen $\phi = (1 - u : v - u)$ ist ϕ auch in der offenen Menge $\{x_1 \neq 0\} \setminus \{(1 : 1 : 1)\}$ definiert. Es bleibt jetzt nur noch das Verhalten im Punkt $(1 : 1 : 1)$ zu untersuchen. Im Funktionenkörper $K(X)$ gilt $2x^2 + 3y^2 = 5$ und damit $3(y^2 - 1) = -2(x^2 - 1)$, was sofort

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

und damit

$$\phi = (1 : -\frac{2}{3} \cdot \frac{x+1}{y+1}) = (3(y+1) : -2(x+1))$$

liefert. Damit ist ϕ auch in $(1 : 1 : 1)$ definiert mit Wert $(1 : -\frac{2}{3})$.

Beispiel: Sei $X \subseteq \mathbb{P}^2$ definiert durch $y^2 = x^3$, d.h. $X = \{x_0 x_2^2 = x_1^3\}$. Wir definieren eine rationale Abbildung $\phi : X \to \mathbb{P}^1$ durch $\phi = (1 : \frac{y}{x})$. Schreibt man

$$\phi = (1 : \frac{y}{x}) = (x : y) = (x_1 : x_2),$$

dann sieht man, dass ϕ außerhalb des Punktes $(0, 0)$ definiert ist. Wir wollen untersuchen, was in diesem Punkt passiert.

- Zunächst ist schnell klar, dass gilt, dass sich jedes Element des Funktionenkörpers als $\frac{a(x)+b(x)y}{c(x)}$ schreiben lässt. Wählt man a, b, c teilerfremd, so ist diese Darstellung eindeutig.
- Sei $f = \frac{a+by}{c}$ gekürzt dargestellt. f ist genau dann in P definiert, falls $c(0) \neq 0$ ist.
- Angenommen, ϕ wäre auch in $(0, 0)$ definiert. Dann gäbe es ein g im Funktionenkörper, so dass g und $g\frac{y}{x}$ in $(0, 0)$ definiert sind und dort nicht beide den Wert 0 haben. Wir können also schreiben $g = \frac{a+by}{c}$ mit $c(0) \neq 0$. Dann hat man

  $$g\frac{y}{x} = \frac{ay + by^2}{xc} = \frac{x^3 b + ay}{xc}.$$

  Da dies in $(0, 0)$ definiert sein soll, ist $a(0) = 0$, d.h. $a = xd$ mit einem Polynom d. Dann gilt:

  $$g = \frac{xd + by}{c}, \quad g\frac{y}{x} = \frac{x^2 b + y}{c}.$$

  Beide sind in $(0, 0)$ definiert, aber beide nehmen den Wert 0 an, ein Widerspruch.

Also ist ϕ in $(0,0)$ nicht definiert.

Bemerkung: Seien V, W projektive Varietäten, die über K definiert, und $\phi : V \to W$ eine rationale Abbildung gegeben durch $\phi = (f_0 : \cdots : f_n)$. Dann operiert G_K auf ϕ durch $\sigma\phi = (\sigma f_0 : \cdots : \sigma f_n)$. Genau dann ist ϕ über K definiert, falls $\sigma\phi = \phi$ für alle $\sigma \in G_K$ gilt.

Bemerkung: Da wir uns die Elemente des Funktionenkörpers auch als Quotienten homogener Polynome gleichen Grades vorstellen können, können wir auch schreiben

$$\phi = (g_0(x_0, \ldots, x_m) : \cdots : g_n(x_0, \ldots, x_m)),$$

wo g_i homogene Polynome gleichen Grades sind, aber nicht alle in $I(V)$ liegen.

Beispiel: Wir betrachten die rationale Abbildung $\phi : \mathbb{P}^2 \to \mathbb{P}^1$, die durch $\phi = (x : y)$ gegeben ist. Schreiben wir $x = \frac{x_1}{x_0}, y = \frac{x_2}{x_0}$, so wird $\phi = (x_1 : x_2)$. ϕ ist in allen Punkten von $\mathbb{P}^2$ außer in $(1 : 0 : 0)$ definiert. Was passiert geometrisch? Die Geraden durch $(1 : 0 : 0)$ haben die Gestalt $x_2 = \lambda x_1$ oder $x_1 = 0$. Was macht ϕ mit den Punkten? Ein Punkt auf $x_2 = \lambda x_1$ wird abgebildet auf $(1 : \lambda)$, ein Punkt auf $x_1 = 0$ auf $(0 : 1)$. Es ist klar, dass ϕ in $(1 : 0 : 0)$ nicht definiert werden kann.

Beispiel: (Projektionen) Eine rationale Abbildung der Form

$$\mathbb{P}^n \to \mathbb{P}^{n-1}, \quad (x_0 : \cdots : x_n) \mapsto (x_0 : \cdots : x_{n-1})$$

nennt man Projektion.

LEMMA. *Sei $\phi : V \to W$ eine rationale Abbildung zwischen projektiven Varietäten. Dann ist $U = \{P \in V : \phi$ definiert in $P\}$ eine offene Teilmenge von V.*

Beweis: Sei $P \in U$ und $\phi = (f_0 : \cdots : f_n)$, wo f_i homogene Polynome sind, mit $f_j(P) \neq 0$. Dann ist ϕ dadurch auch in der offenen Umgebung $\{f_j \neq 0\} \cap V$ von P definiert, woraus sofort die Behauptung folgt. ■

DEFINITION.
(1) *Eine rationale Abbildung $\phi : V \to W$ zwischen projektiven Varietäten heißt* **Morphismus**, *wenn ϕ in allen Punkten von V definiert ist.*
(2) *Ein Morphismus $\phi : V \to W$ heißt Isomorphismus, falls es einen Morphismus $\psi : W \to V$ gibt, so dass $\phi\psi$ und $\psi\phi$ jeweils die Identität sind.*
(3) *Sind V und W über K definiert, so heißen V und W über K* **isomorph**, *falls über K definierte Morphismen $\phi : V \to W$ und $\psi : W \to V$ existieren, so dass $\phi\psi$ und $\psi\phi$ jeweils die Identität sind.*

Bemerkung: Da wir affine Varietäten projektiv abschließen können, ist klar, wie man rationale Abbildungen und Morphismen auch für affine Varietäten definiert.

Projektiver Koordinatenwechsel: Sei $T \in \mathrm{GL}_{n+1}(\overline{K})$. Dann induziert T eine lineare Abbildung des $\overline{K}^{n+1}$, die einen Automorphismus des $\mathbb{P}^n$ liefert. Man nennt dies einen Koordinatenwechsel. Zwei Teilmengen des $\mathbb{P}^n$ heißen projektive äquivalent, wenn sie durch einen Koordinatenwechsel auseinander hervorgehen.

Für die diophantische Geometrie ist folgender Satz wichtig:

SATZ. *Sind V und W über K definierte projektive Varietäten und $\phi : V \to W$ ein über K definierter Isomorphismus, so induziert ϕ eine Bijektion $V(K) \simeq W(K)$.*

Beweis: ϕ und ϕ^{-1} können also durch Polynome beschrieben werden, die Koeffizienten in K haben. Natürlich werden dann Punkte von $V(K)$ und $W(K)$ ineinander abgebildet. Da aber ϕ bijektiv ist, folgt die Behauptung. ■

Bemerkungen:

(1) Man könnte also eine Aufgabe der diophantischen Geometrie so formulieren: Klassifiziere über K-definierte projektive Varietäten bis auf K-Isomorphie und bestimme jeweils die K-rationalen Punkte.
(2) Ein erster Schritt dazu ist ein Ziel der algebraischen Geometrie: Klassifiziere projektive Varietäten bis auf Isomorphie, wobei hier alles über algebraisch abgeschlossenem Körper zu sehen ist. Allerdings ist auch diese Aufgabe noch zu schwierig.

Beispiel: Sei $X_n \subseteq \mathbb{P}^2$ definiert durch die affine Gleichung $2x^2+3y^2 = n$. Also $X_n = \{2x_1^2+3x_2^2 = nx_0^2\}$. Offensichtlich gilt

$$X_n(\mathbb{Q}) = \{(1:x:y) : 2x^2+3y^2 = n \text{ und } x,y \in \mathbb{Q}\}.$$

Man kann zeigen: $X_1(\mathbb{Q}) = \emptyset$ und $\#X_5(\mathbb{Q}) = \infty$, also sind X_1 und X_5 nicht über $\mathbb{Q}$ isomorph. Andererseits induziert der Koordinatenwechsel

$$\phi((x_0:x_1:x_2)) = (\sqrt{5}x_0 : x_1 : x_2)$$

einen Isomorphismus von X_1 mit X_5, der über $\mathbb{Q}(\sqrt{5})$ definiert ist.

Beispiel: Ist C eine über K durch das Polynom

$$f = a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$$

definierte nichtsinguläre Quadrik, die daher den Punkt $(1:0:0)$ enthält, so haben wir gesehen, dass durch

$$\phi((u:v)) = (a_3u^2 + a_4uv + a_5v^2 : -u(a_1u+a_2v) : -v(a_1u+a_2v))$$

und

$$\psi((x_0:x_1:x_2) = \begin{cases} (x_1:x_2), \text{ falls } (x_0:x_1:x_2) \neq (1:0:0), \\ (a_2:-a_1), \text{ falls } (x_0:x_2:x_2) = (1:0:0) \end{cases}$$

zwei zueinander inverse bijektive Abbildungen

$$\phi : \mathbb{P}^1 \to C \quad \text{und} \quad \psi : C \to \mathbb{P}^1$$

definiert werden. Natürlich ist ϕ ein Morphismus, da ϕ durch homogene Polynome vom Grad 2 definiert wird. Was ist mit ψ? Für $(x_0:x_1:x_2) \in C$ gilt

$$0 = a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = (a_1x_0 + a_3x_1 + a_4x_2)x_1 + (a_2x_0 + a_5x_2)x_2,$$

und damit

$$\begin{vmatrix} x_1 & x_2 \\ -a_2x_0 - a_5x_2 & a_1x_0 + a_3x_1 + a_4x_2 \end{vmatrix} = 0.$$

Daher ist

$$\psi((x_0:x_1:x_2)) = \begin{cases} (x_1:x_2), & \text{falls } (x_1,x_2) \neq (0,0), \\ (-a_2x_0 - a_5x_2 : a_1x_0 + a_3x_1 + a_4x_2), & \text{falls } (-a_2x_0 - a_5x_2, a_1x_0 + a_3x_1 + a_4x_2) \neq (0,0) \end{cases}$$

wohldefiniert, wobei die zweite Darstellung auch im Punkt $(1:0:0)$ definiert ist. Also ist auch ψ ein Morphismus. Daher erhalten wir über K definierte Isomorphismen

$$\phi : \mathbb{P}^1 \to C \quad \text{und} \quad \psi : C \to \mathbb{P}^1.$$

Beispiel: Ist C eine über K definierte nichtsinguläre projektive ebene Quadrik und gibt es einen Punkt $P \in C(K)$, so gibt es einen über K definierten Koordinatenwechsel α mit $\alpha(P) = (1:0:0)$. In den neuen Koordinaten werde die Kurve mit $\widetilde{C}$ bezeichnet. Dann liefert der Koordinatenwechsel einen Isomorphismus

$$\alpha : C \to \widetilde{C} \quad \text{mit} \quad \alpha(P) = (1:0:0).$$

Wie im vorangegangenen Beispiel findet man nun einen über K definierten Isomorphismus

$$\beta : \widetilde{C} \to \mathbb{P}^1.$$

Setzt man die Isomorphismen zusammen, so erhält man folgenden Satz:

SATZ. *Ist C eine über K definierte nichtsinguläre projektive ebene Quadrik und ist $C(K) \neq \emptyset$, so gibt es einen über K definierten Isomorphismus*

$$\phi : C \to \mathbb{P}^1.$$

Von fundamentaler Bedeutung ist folgender Satz, den wir nicht beweisen werden:

SATZ. *Ist X eine projektive Varietät und $\phi : X \to \mathbb{P}^n$ ein Morphismus, so ist $\phi(X)$ abgeschlossen, d.h. $\phi(X)$ lässt sich in $\mathbb{P}^n$ durch Gleichungen beschreiben.*

Dass dies Aussage im Allgemeinen für affine Varietäten nicht gilt, zeigt folgendes Beispiel:

Beispiel:

(1) Wir betrachten die affine Varietät $X = \{(x, y) \in \mathbb{A}^2 : xy = 1\}$ und den Morphismus $\phi : X \to \mathbb{A}^1$ mit $\phi((x, y)) = x$. Offensichtlich ist $\phi(X) = \mathbb{A}^1 \setminus \{0\}$ keine abgeschlossenen Teilmenge von $\mathbb{A}^1$.
(2) Dies wird auch nicht anders, wenn man $\phi : X \to \mathbb{P}^1$ mit $\phi((x, y)) = (1 : x)$ betrachtet. Dann ist $\phi(X) = \mathbb{P}^1 \setminus \{(1 : 0), (0 : 1)\}$, was auch keine abgeschlossene Teilmenge von $\mathbb{P}^1$ ist.
(3) Wir betrachten jetzt den projektiven Abschluss von X im $\mathbb{P}^2$: $Y = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 : x_1x_2 = x_0^2\}$. Wir haben die 2 Punkte $(0 : 1 : 0)$ und $(0 : 0 : 1)$ dazu bekommen. Die rationale Abbildung $\phi : Y \to \mathbb{P}^1$ mit

$$\phi = (1 : x) = (1 : \frac{x_1}{x_0}) = (x_0 : x_1) = (x_0^2 : x_0x_1) = (x_2 : x_0)$$

ist ein Morphismus, wie man an den verschiedenen Darstellungen sieht und $\phi((0 : 1 : 0)) = (0 : 1)$, $\phi((0 : 0 : 1)) = (1 : 0)$. Damit folgt sofort $\phi(Y) = \mathbb{P}^1$, insbesondere ist $\phi(Y)$ abgeschlossen.

Beispiel: Projektive ebene Quadriken werden definiert durch eine Gleichung

$$f_{(a_0,\ldots,a_5)} = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0.$$

Natürlich kann man die Koeffizienten $a_0, \ldots, a_5$ um einen Skalar abändern ohne zu Quadrik zu ändern. Die Menge der projektiven ebenen Quadriken wird also durch einen $\mathbb{P}^5$ parametrisiert:

$$\begin{array}{rcl} \mathbb{P}^5 & \longrightarrow & \{\text{projektive ebene Quadrik}\}, \\ (a_0 : a_1 : a_2 : a_3 : a_4 : a_5) & \mapsto & f_{(a_0,\ldots,a_5)} = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0. \end{array}$$

Im $\mathbb{P}^5$ der ebenen Quadriken gibt es die Teilmenge der reduziblen Quadriken:

$$R = \{(a_0 : \cdots : a_5) \in \mathbb{P}^5 : f_{(a_0,\ldots,a_5)} \text{ ist reduzibel}\}.$$

Wir haben gesehen, dass R eine algebraische Teilmenge von $\mathbb{P}^5$ ist:

$$R = \{4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_1^2a_5 - a_2^2a_3 = 0\}.$$

Wir wollen dies nochmals anders sehen: Eine Quadrik $f_{(a_0,\ldots,a_5)} = 0$ ist genau dann reduzibel, wenn es $b_0, b_1, b_2, c_0, c_1, c_2 \in \overline{K}$ gibt mit

$$\begin{array}{rcl} f & = & (b_0x_0 + b_1x_1 + b_2x_2)(c_0x_0 + c_1x_1 + c_2x_2) = \\ & = & b_0c_0x_0^2 + (b_0c_1 + b_1c_0)x_0x_1 + (b_0c_2 + b_2c_0)x_0x_2 + b_1c_1x_1^2 + (b_1c_2 + b_2c_1)x_1x_2 + b_2c_2x_2^2, \end{array}$$

also

$$a_0 = b_0c_0, \quad a_1 = b_0c_1 + b_1c_0, \quad a_2 = b_0c_2 + b_2c_0, \quad a_3 = b_1c_1, \quad a_4 = b_1c_2 + b_2c_1, \quad a_5 = b_2c_2.$$

Definieren wir also ϕ durch

$$\begin{array}{rcl} \mathbb{P}^2 \times \mathbb{P}^2 & \longrightarrow & \mathbb{P}^5, \\ ((b_0 : b_1 : b_2), (c_0 : c_1 : c_2)) & \mapsto & (b_0c_0 : b_0c_1 + b_1c_0 : b_0c_2 + b_2c_0 : b_1c_1 : b_1c_2 + b_2c_1 : b_2c_2), \end{array}$$

so ist ϕ ein Morphismus mit Bild R.

Beispiel: Wir betrachten nun im $\mathbb{P}^5$ der projektiven ebenen Quadriken die Teilmenge D der Doppelgeraden. Wir haben bereits gesehen, dass sich D durch Gleichungen beschreiben lässt:

$$D = \{4a_0a_3 - a_1^2 = 0, 4a_0a_5 - a_2^2 = 0, 4a_3a_5 - a_4^2 = 0, 2a_0a_4 - a_1a_2 = 0, 2a_1a_5 - a_2a$$

Wir geben noch eine andere Darstellung: Eine Quadrik $f_{(a_0,\ldots,a_5)} = 0$ ist genau dann eine Doppelgerade, wenn es $b_0, b_1, b_2 \in \overline{K}$ gibt mit

$$\begin{aligned} f &= (b_0x_0 + b_1x_1 + b_2x_2)^2 = \\ &= b_0^2x_0^2 + 2b_0b_1x_0x_1 + 2b_0b_2x_0x_2 + b_1^2x_1^2 + 2b_1b_2x_1x_2 + b_2^2x_2^2, \end{aligned}$$

also

$$a_0 = b_0^2, \quad a_1 = 2b_0b_1, \quad a_2 = 2b_0b_2, \quad a_3 = b_1^2, \quad a_4 = 2b_1b_2, \quad a_5 = b_2^2.$$

Definieren wir also ψ durch

$$\begin{aligned} \mathbb{P}^2 &\longrightarrow \mathbb{P}^5, \\ (b_0 : b_1 : b_2) &\mapsto (b_0^2 : 2b_0b_1 : 2b_0b_2 : b_1^2 : 2b_1b_2 : b_2^2), \end{aligned}$$

so ist ψ ein Morphismus mit Bild D. Man kann sich überlegen, dass ψ in Charakteristik $\neq 2$ ein Isomorphismus ist mit Umkehrabbildung

$$\psi^{-1}((a_0 : a_1 : a_2 : a_3 : a_4 : a_5)) = \begin{cases} (2a_0 : a_1 : a_2), & \text{falls } (2a_0, a_1, a_2) \neq 0, \\ (a_1 : 2a_3 : a_4), & \text{falls } (a_1, 2a_3, a_4) \neq 0, \\ (a_2 : a_4 : 2a_5), & \text{falls } (a_2, a_4, 2a_5) \neq 0. \end{cases}$$

Bevor wir weitermachen, geben wir noch zwei einfache Lemmas an:

LEMMA. *Jeder Morphismus ist stetig in der Zariski-Topologie.*

Beweis: Ein Morphismus $\phi : X \to Y$ wird lokal gegeben durch $\phi = (f_0 : \cdots : f_n)$ mit homogenen Polynomen gleichen Grades f_i. Eine abgeschlossene Menge in Y wird gegeben durch homogene Gleichungen $F_1 = \cdots = F_r = 0$. Das Urbild ist dann

$$F_1(f_0, \ldots, f_n) = \cdots = F_r(f_0, \ldots, f_n) = 0,$$

also wieder abgeschlossen. ■

LEMMA. *Sei $\phi : X \to Y$ ein Morphismus und X irreduzibel. Dann ist auch $\phi(X)$ irreduzibel.*

Beweis: Sei $\phi(X) = Z_1 \cup Z_2$ mit (in $\phi(X)$) abgeschlossenen Mengen Z_1, Z_2. Dann ist $X = \phi^{-1}(Z_1) \cup \phi^{-1}(Z_2)$, also gilt wegen der Irreduzibilität von X für ein i: $X = \phi^{-1}(Z_i)$ und damit $\phi(X) = Z_i$. ■

Trivialerweise folgt damit:

FOLGERUNG. *Ist X eine projektive Varietät und $\phi : X \to \mathbb{P}^n$ ein Morphismus, so ist $\phi(X)$ eine projektive Varietät.*

Wir beweisen jetzt noch einen Satz, den wir schon zitiert haben.

SATZ. *Sei X eine projektive Varietät und $f \in \overline{K}(X)$ eine Funktion, die auf ganz X definiert ist. Dann ist $f \in \overline{K}$.*

Beweis: f liefert eine Funktion $X \to \mathbb{A}^1 \subseteq \mathbb{P}^1$, also einen Morphismus $f : X \to \mathbb{P}^1$. Das Bild ist abgeschlossen, $\neq \mathbb{P}^1$, besteht also aus endlich vielen Punkten, also aus genau einem Punkt $a \in \mathbb{P}^1$, $a \in \mathbb{A}^1$. Also ist f konstant. ■

Eine etwas allgemeinere Formulierung obiger Aussage ist folgende:

SATZ. *Sei $\phi : V \to W$ ein Morphismus zwischen projektiven Varietäten. Dann ist ϕ eine abgeschlossene Abbildung, d.h. abgeschlossene Mengen werden in abgeschlossene abgebildet.*

Beweis: O.E. $V \subseteq \mathbb{P}^m$ und $W \subseteq \mathbb{P}^n$. Sei $Z \subseteq V$ abgeschlossen. Dann gibt es eine Zerlegung $Z = Z_1 \cup \cdots \cup Z_r$, wo die Z_i abgeschlossen und irreduzibel sind. Also sind die $Z_i \subseteq \mathbb{P}^m$ projektive Varietäten. ϕ induziert natürlich auch Morphismen $\phi : Z_i \to \mathbb{P}^n$. Also ist $\phi(Z_i)$ abgeschlossen und damit auch $\phi(Z) = \phi(Z_1) \cup \cdots \cup \phi(Z_r)$. ■

DEFINITION. *Ein Morphismus $\phi : V \to W$ zwischen projektiven Varietäten heißt eine Einbettung, falls ϕ einen Isomorphismus zwischen V und (der projektiven Varietät) $\phi(V)$ liefert.*

Beispiel: Wir definieren

$$\phi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3, \quad ((x_0 : x_1), (y_0 : y_1)) \mapsto (x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1).$$

ϕ ist ein Morphismus und $\phi(\mathbb{P}^1 \times \mathbb{P}^1) = Q = \{z_0z_3 = z_1z_2\}$. Wir wollen eine Umkehrabbildung finden. Dazu überlegen wir zunächst: Ist $z_0 = 1$, so o.E. $x_0 = y_0 = 1$ und $x_1 = z_2$, $y_1 = z_1$. Wegen

$$(z_0 : z_1) = (z_0z_3 : z_1z_3) = (z_1z_2 : z_1z_3) = (z_2 : z_3)$$

und

$$(z_0 : z_2) = (z_0z_3 : z_2z_3) = (z_1z_2 : z_2z_3) = (z_1 : z_3)$$

setzen wir an: $\psi : Q \to \mathbb{P}^1 \times \mathbb{P}^1$ mit

$$\psi = ((z_0 : z_2), (z_0 : z_1)) = ((z_0 : z_2), (z_2 : z_3)) = ((z_1 : z_3), (z_0 : z_1)) = ((z_1 : z_3), (z_2 : z_3)).$$

Offensichtlich ist auch ψ ein Morphismus und man rechnet schnell nach, dass $\phi\psi$ und $\psi\phi$ jeweils die Identität sind. Also ist $\mathbb{P}^1 \times \mathbb{P}^1$ isomorph zur Quadrik Q im $\mathbb{P}^3$.

Dieses Beispiel verallgemeinert sich wie folgt:

SATZ. *Definiert man $\phi : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$ durch*

$$((x_0 : \cdots : x_m), (y_0 : \cdots : y_n)) \mapsto (x_0y_0 : \cdots : x_0y_n : \cdots : x_my_0 : \cdots : x_my_n),$$

so ist ϕ eine Einbettung, die sogenannte Segre-Einbettung. Insbesondere ist $\mathbb{P}^m \times \mathbb{P}^n$ eine projektive Varietät.

Wir wollen nochmals rationale Abbildungen betrachten. Da rationale Abbildungen nicht überall definiert sein müssen, kann man nicht allgemein eine Komposition definieren.

DEFINITION. *Sei $\phi : V \to W$ eine rationale Abbildung mit maximaler Definitionsmenge U. Wir sagen, ϕ ist generisch surjektiv, falls $\phi(U)$ dicht in W liegt.*

Beispiel: Wir betrachten die rationale Abbildung $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ mit

$$\phi = (\frac{1}{x_0} : \frac{1}{x_1} : \frac{1}{x_2}) = (x_1x_2 : x_0x_2 : x_0x_1).$$

ϕ ist eine sogenannte quadratische Transformation der Ebene. ϕ ist generisch surjektiv und $\phi \circ \phi = id$. Was passiert geometrisch? ϕ ist nicht definiert in den 3 Punkten $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$. Die Gerade $x_0 = 0$ wird auf $(1 : 0 : 0)$ zusammengezogen, $x_1 = 0$ auf $(0 : 1 : 0)$, $x_2 = 0$ auf $(0 : 0 : 1)$.

Der folgende Satz Identitätssatz für rationale Abbildungen wird oft benutzt.

SATZ. *Seien $\phi_1, \phi_2 : X \to Y$ zwei rationale Abbildungen zwischen projektiven Varietäten mit maximaler Definitionsmenge U_1 und U_2. Stimmen ϕ_1 und ϕ_2 auf einer offenen Teilmenge $U \neq \emptyset$ überein, so gilt schon $\phi_1 = \phi_2$.*

Beweisidee: $U_1 \cap U_2 \cap \{\phi_1 \neq \phi_2\}$ ist eine offene Menge, $U \subseteq U_1 \cap U_2 \cap \{\phi_1 = \phi_2\}$ ebenso. Wir wissen, dass je zwei offene nichtleere Mengen einen nichtleeren Durchschnitt besitzen. Wegen $U \neq \emptyset$, folgt also $U_1 \cap U_2 \cap \{\phi_1 \neq \phi_2\} = \emptyset$, d.h. ϕ_1 und ϕ_2 stimmen auf $U_1 \cap U_2$ überein. Dann kann man aber ϕ_1 auch auf $U_1 \cup U_2$ fortsetzen. Also folgt $U_1 = U_2$ und damit die Behauptung. ■

Man hätte diesen Satz auch mit folgenden Lemma beweisen können.

LEMMA. *Ist X eine projektive Varietät und $f, g \in \overline{K}(X)$ zwei Funktionen, die auf einer offenen nichtleeren Menge U übereinstimmen, dann gilt schon $f = g$ (im Funktionenkörper).*

Beweis: Es genügt, $U \subseteq X \cap \mathbb{A}^n$ zu betrachten. Wir schreiben $f = \frac{f_1(x_1,\ldots,x_n)}{f_2(x_1,\ldots,x_n)}$ und $g = \frac{g_1(x_1,\ldots,x_n)}{g_2(x_1,\ldots,x_n)}$ als Quotient von Polynomen. Dann gilt auf U auch $f_1g_2 - f_2g_1 = 0$. Nun definiert $f_1g_2 - f_2g_1 \neq 0$ eine offene Menge in $X \cap \mathbb{A}^n$. Da je zwei offene nichtleere Mengen einen nichttrivialen Durchschnitt haben, muss $f_1g_2 - f_2g_1 \neq 0$ die leere Menge sein. Also gilt $f = g$ im Funktionenkörper. ■

DEFINITION. *Zwei projektive Varietäten heißen birational äquivalent über $\overline{K}$, falls es generisch surjektive rationale Abbildungen $\phi : V \to W$ und $\psi : W \to V$ gibt, so dass die rationalen Abbildungen $\phi\psi$ und $\psi\phi$ jeweils die Identität sind.*

Natürlich sind isomorphe projektive Varietäten auch birational äquivalent. Die birationale Äquivalenz ist aber i.a. eine gröbere Klassifizierung. Eine wesentliche Aufgabe der algebraischen Geometrie ist die Klassifizierung projektiver Varietäten bis auf birationale Äquivalenz.

Beispiel: Natürlich sind $\mathbb{A}^2$ und $\mathbb{A}^1 \times \mathbb{A}^1$ isomorph. Wie steht dies mit $\mathbb{P}^2$ und $\mathbb{P}^1 \times \mathbb{P}^1$? Wir definieren rationale Abbildungen

$$\phi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2, \quad ((x_0 : x_1), (y_0 : y_1)) \mapsto (1 : \frac{x_1}{x_0} : \frac{y_1}{y_0}) = (x_0y_0 : y_0x_1 : x_0y_1)$$

und

$$\psi : \mathbb{P}^2 \to \mathbb{P}^1 \times \mathbb{P}^1, \quad (z_0 : z_1 : z_2) \mapsto ((1 : \frac{z_1}{z_0}), (1 : \frac{z_2}{z_0})) = ((z_0 : z_1), (z_0 : z_2)).$$

Dann gilt $\psi\phi = id$ und $\phi\psi = id$, also sind $\mathbb{P}^1 \times \mathbb{P}^1$ und $\mathbb{P}^2$ birational äquivalent. Man kann zeigen, dass $\mathbb{P}^1 \times \mathbb{P}^1$ und $\mathbb{P}^2$ nicht isomorph sind: Auf $\mathbb{P}^1 \times \mathbb{P}^1$ gibt es Kurven, die sich nicht schneiden, z.B. $\{0\} \times \mathbb{P}^1$ und $\{1\} \times \mathbb{P}^1$, auf $\mathbb{P}^2$ schneiden sich dagegen je zwei Kurven in mindestens einem Punkt.

Beispiel: $X \subseteq \mathbb{P}^2$ werde definiert durch $y^2 = x^3$, d.h. $X = \{x_0x_2^2 = x_1^3\}$. Dann haben wir gesehen, dass $\phi : X \to \mathbb{P}^1$ mit $\phi = (1 : \frac{y}{x})$ eine rationale Abbildung ist, die im Punkt $(1 : 0 : 0)$ nicht definiert ist. Sei $\psi : \mathbb{P}^1 \to X$ mit $\psi = (1 : t^2 : t^3)$. Man rechnet nach, dass ψ ein Morphismus ist. Außerdem gilt: $\phi\psi = id$, $\psi\phi = id$, d.h. X ist birational äquivalent zu $\mathbb{P}^1$. Allerdings ist X nicht isomorph zu $\mathbb{P}^1$. (X hat eine Singularität.)

Die Beispiele deuten schon einen Sachverhalt an, den wir ohne Beweis angeben:

SATZ. *Seien X und Y birational äquivalente projektive Varietäten. Dann gibt es nichtleere offene Teilmengen $U_X \subseteq X$, $U_Y \subseteq Y$, die isomorph sind.*

Wir stellen nun noch eine Verbindung zur Algebra her: Seien $X \subseteq \mathbb{P}^m$ und $Y \subseteq \mathbb{P}^n$ projektive Varietäten.

- Haben wir auf $\mathbb{P}^m$ die Koordinaten x_i, auf $\mathbb{P}^n$ die Koordinaten y_j, so können wir uns die Funktionenkörper denken als $K(X) = K(x_1, \ldots, x_m)$ und $K(Y) = K(y_1, \ldots, y_n)$ mit Relationen zwischen den x_i's und den y_j's.
- Sei $\phi : X \to Y$ eine generisch surjektive (rationale) Abbildung. Dann liefert

  $$\phi^* : K(Y) \to K(X), \quad f \mapsto f \circ \phi$$

  einen Körperhomomorphismus, der K festlässt. Er ist dadurch festgelegt, dass man die $\phi^*(y_j)$'s kennt. ϕ^* ist (als Körperhomomorphismus) injektiv.
- Davon gilt nun auch die Umkehrung: Sei

  $$\alpha : K(Y) \to K(X)$$

  ein Körperhomomorphismus, der K in sich überführt. Sei $\alpha(y_i) = f_i(x_1, \ldots, x_n)$ mit $f_i \in K(X)$. Dann gibt es eine rationale Abbildung $\phi : X \to Y$ mit

  $$\phi = (1 : f_1 : \cdots : f_n).$$

- Wieso ist ϕ generisch surjektiv? Sei F ein Polynom mit $F(f_1,\dots,f_n)=0$, also $\alpha(F(y_1,\dots,y_n))=0$ und damit $F(y_1,\dots,y_n)=0$. Dies liefert $F\in I(Y)$, also eine Relation, die trivialerweise erfüllt sein muss. Daher ist ϕ generisch surjektiv.
- Was ist ϕ^*? Dazu bestimmen wir die Urbilder der Koordinatenfunktionen y_j. Wegen $\phi=(1:f_1:\dots:f_n)$ ist $\phi^*(y_j)=f_j$. Also $\phi^*(y_j)=\alpha(y_j)$. Da die y_j's den Funktionenkörper erzeugen, folgt $\phi^*=\alpha$.

Damit haben wir folgenden Satz bewiesen:

SATZ. *Für projektive Varietäten X und Y gibt es eine Bijektion*

$$\{\phi: X\to Y \text{ generisch surjektiv }\}\simeq\{\alpha:\overline{K}(Y)\to\overline{K}(X) \text{ Körperhomomorphismus mit } \alpha|_{\overline{K}}=id|_{\overline{K}}\}$$

vermöge $\alpha=\phi^*$.

Beispiel: Sei C eine irreduzible projektive Kurve. Jede rationale Abbildung $\phi: C\to\mathbb{P}^1$ ist gegeben durch $\phi=(f_0:f_1)$ mit $f_0,f_1\in\overline{K}(C)$. O.E. ist $f_0\neq 0$. Mit $f=\frac{f_1}{f_0}$ kann man dann auch $\phi=(1:f)$ schreiben. Es gibt zwei Möglichkeiten:

- ϕ ist konstant, d.h. $f\in\overline{K}$.
- ϕ ist nicht konstant, d.h. $f\in\overline{K}(C)\setminus\overline{K}$. Dann ist ϕ generisch surjektiv. Hat man auf $\mathbb{P}^1$ die Koordinaten $(1:t)$, so ist ϕ^* gegeben durch
$$\overline{K}(t)\to\overline{K}(C),\quad t\mapsto f.$$
Umgekehrt schaut hat natürlich auch jeder Körperhomomorphismus $\overline{K}(t)\to\overline{K}(C)$, der $\overline{K}$ festlässt, so aus.

Beispiel: Sei $F_n\subseteq\mathbb{P}^2$ gegeben durch $x^n+y^n=1$. Der Funktionenkörper von F_n ist
$$\overline{K}(F_n)=\overline{K}(x,y) \text{ mit } x^n+y^n=1.$$
Auf $\mathbb{P}^1$ wählen wir Koordinaten $(1:t)$. Dann ist der Funktionenkörper von $\mathbb{P}^1$ einfach $\overline{K}(t)$. Wir suchen eine nichtkonstante (also generisch surjektive) rationale Abbildung $\phi:\mathbb{P}^1\to F_n$.
Algebraische Interpretation: Wir suchen einen $\overline{K}$ festlassenden Körperhomomorphismus
$$\alpha:\overline{K}(x,y)\to\overline{K}(t) \text{ (mit })x^n+y^n=1.$$
$\alpha(x)$ und $\alpha(y)$ sind dann rationale Funktionen in t mit $(\alpha(x))^n+(\alpha(y))^n=1$. Da $\overline{K}$ fest bleibt, sind $\alpha(x)$ und $\alpha(y)$ nicht konstant. Wir setzen an $\alpha(x)=\frac{f}{h},\alpha(y)=\frac{g}{h}$ und erhalten dann die Bedingung $f^n+g^n=h^n$, wobei wir also f,g,h als paarweise teilerfremde Polynome in t annehmen können, die nicht alle konstant sind.
Geometrische Interpretation: Wir suchen Polynome f,g,h in t mit $\phi=(h:f:g)$. Da das Bild von ϕ in C liegen soll, muss gelten $f^n+g^n=h^n$. Wir können annehmen, dass f,g,h paarweise teilerfremd sind. Da ϕ nicht konstant sein soll, sollen f,g,h nicht alle konstant sein.
Behauptung: Für $n\geq 3$ und $char(K)=0$ gibt es keine solchen Polynome.
Beweis: Wir nehmen an, wir haben eine nichttriviale Relation $f^n+g^n=h^n$. Insbesondere sind alle $f,g,h\neq 0$. Differenzieren liefert $nf^{n-1}\cdot f'+ng^{n-1}\cdot g'=nh^{n-1}\cdot h'$. Wir schreiben dies in Matrizenform:
$$\begin{pmatrix} f & g & h\\ f' & g' & h'\end{pmatrix}\begin{pmatrix} f^{n-1}\\ g^{n-1}\\ -h^{n-1}\end{pmatrix}=0.$$
Als Grundkörper haben wir jetzt $\overline{K}(t)$. Sei
$$M=\begin{pmatrix} f & g & h\\ f' & g' & h'\end{pmatrix}.$$
Das Gleichungssytem $M\cdot X=0$ hat immer die Lösung
$$\left(\begin{vmatrix} g & h\\ g' & h'\end{vmatrix},\begin{vmatrix} h & f\\ h' & f'\end{vmatrix},\begin{vmatrix} f & g\\ f' & g'\end{vmatrix}\right).$$
1. Fall: Der Rang von M ist 1. Dann müssen obige Unterdeterminanten 0 sein. Also $fg'=f'g$ etc. Da f und g teilerfremd sind, folgt $f|f'$, was aus Gradgründen sofort $f'=0$ impliziert, also $f\in\overline{K}$. Genauso

folgt $f, g, h \in \overline{K}$, ein Widerspruch.
2. Fall: M hat Rang 2. Dann hat das Gleichungssystem $M \cdot X = 0$ einen 1-dimensionalen Lösungsraum, also gibt es teilerfremde Polynome $r(t), s(t)$ mit

$$f^{n-1} = \frac{r}{s} \begin{vmatrix} g & h \\ g' & h' \end{vmatrix}, \; g^{n-1} = \frac{r}{s} \begin{vmatrix} h & f \\ h' & f' \end{vmatrix}, \; -h^{n-1} = \frac{r}{s} \begin{vmatrix} f & g \\ f' & g' \end{vmatrix}.$$

Bringt man s auf die andere Seite, so sieht man sofort $r | f^{n-1}, g^{n-1}, h^{n-1}$, und da f, g, h teilerfremd sind: $r \in \overline{K}$, also o.E. $r = 1$. Jetzt folgt

$$f^{n-1} | (gh' - g'h),\; g^{n-1} | (hf' - h'f),\; h^{n-1} | (fg' - f'g).$$

Wir wollen jetzt die Grade vergleichen. Setzt man a, b, c für den Grad von f, g, h, so folgt

$$(n-1)a \leq b + c - 1, \quad (n-1)b \leq c + a - 1, \quad (n-1)c \leq a + b - 1,$$

oder auch

$$na, nb, nc \leq a + b + c - 1.$$

Setzt man $d = \max(a, b, c)$, so ist $d \geq 1$ und $nd \leq 3d - 1$, also $n \leq 2$, ein Widerspruch zu unserer Annahme. Damit ist die Behauptung bewiesen. ■
Bemerkung: Für $n = 1$ kann man $f = t, g = 1 - t, h = 1$ wählen, für $n = 2$:

$$f = 2t, \quad g = t^2 - 1, \quad h = t^2 + 1.$$

Aus den vorangegangenen Überlegungen folgt sofort:

SATZ. *Zwei projektive Varietäten V und W sind genau dann birational äquivalent über $\overline{K}$, falls die Funktionenkörper $\overline{K}(V)$ und $\overline{K}(W)$ über $\overline{K}$ isomorph sind.*

FOLGERUNG. *Jede projektive Varietät V der Dimension d ist birational äquivalent zu einer Hyperfläche $f = 0$ im $\mathbb{P}^{d+1}$. Ist V über K definiert, so kann auch $f = 0$ und die birationale Äquivalenz über K definiert werden.*

Beweis: Der Funktionenkörper $K(V)$ hat Transzendenzgrad d über K. Dann gibt es algebraisch unabhängige Elemente $t_1, \ldots, t_d \in K(V)$, so dass $K(V)$ eine endliche (algebraische) Erweiterung von $K(t_1, \ldots, t_d)$ ist. Da K als vollkommen vorausgesetzt wurde, kann man es so einrichten, dass $K(V)$ über $K(t_1, \ldots, t_d)$ separabel ist (Lang. S.365). Also gibt es ein $u \in K(V)$ mit $K(V) = K(t_1, \ldots, t_d, u)$. Außerdem besteht eine algebraische Relation $f(t_1, \ldots, t_d, u) = 0$ (Polynom mit Koeffizienten aus K), wobei das Polynom f irreduzibel gewählt werden kann. Der Funktionenkörper der Hyperfläche

$$f(x_1, \ldots, x_d, x_{d+1}) = 0$$

im $\mathbb{P}^{d+1}$ ist $\mathrm{Quot}(K[x_1, \ldots, x_{d+1}]/(f))$, also $K(V)$. Nach unserem Satz ist also V birational äquivalent zu der Hyperfläche $f = 0$. ■

FOLGERUNG. *Jede irreduzible projektive Kurve ist birational äquivalent zu einer ebenen Kurve $\{f(x_0, x_1, x_2) = 0\} \subseteq \mathbb{P}^2$.*

KAPITEL 7

Algebraische Kurven

Unter einer Kurve verstehen wir im Folgenden eine absolut irreduzible projektive Kurve C, die über einem vollkommenen Körper K definiert ist. Wir denken uns $C \subseteq \mathbb{P}^n$.

Sei also C eine Kurve. Wir haben dann den Funktionenkörper $\overline{K}(C)$ definiert. Für $P \in C$ haben wir den lokalen Ring von C in P definiert:

$$\mathcal{O}_{C,P} = \{f \in \overline{K}(C) : f \text{ ist definiert in } P\}.$$

Das maximale Ideal ist

$$\mathfrak{m}_{C,P} = \{f \in \mathcal{O}_{C,P} : f(P) = 0\}.$$

(Es gibt auch andere Bezeichnungen. [**Silverman**, S.17] schreibt $\overline{K}[C]_P$ für den lokalen Ring und M_P für das maximale Ideal.) Die Einheiten im lokalen Ring sind

$$\mathcal{O}^*_{C,P} = \{f \in \mathcal{O}_{C,P} : f(P) \neq 0\}.$$

Wir betrachten zunächst ein Beispiel:

Beispiel: Wir betrachten $\mathbb{P}^1$ und den Punkt $(1:2) \simeq 2$. Der Funktionenkörper ist $K(\mathbb{P}^1) = K(x)$. Jedes $f \in K(x) \setminus \{0\}$ hat eine eindeutige Darstellung $f = u(x) \cdot (x-2)^n$ mit $n \in \mathbb{Z}$, wo $u(x)$ in 2 definiert ist und $u(2) \neq 0$ gilt. n ist dann die Null- bzw. Polstellenordnung von f im Punkt 2.

Dieses Beispiel ist typisch für nichtsinguläre Punkte auf Kurven, wie folgender wichtige Satz besagt:

Satz. *Sei C eine Kurve und P ein nichtsingulärer Punkt auf C. Dann ist der lokale Ring $\mathcal{O}_{C,P}$ von C in P ein* **diskreter Bewertungsring**, *d.h. es gibt eine Funktion $t \in \mathcal{O}_{C,P}$ mit $t(P) = 0$, so dass sich jedes Element $f \neq 0$ des lokalen Rings eindeutig schreiben lässt als $f = ut^n$ mit einer Einheit $u \in \mathcal{O}^*_{C,P}$ und $n \geq 0$. t heißt eine* **Uniformisierende** *oder* **Ortsuniformisierende** *in P. Jedes Element $f \neq 0$ aus $\overline{K}(C)$ hat eine eindeutige Darstellung*

$$f = ut^n \text{ mit } u(P) \neq 0 \text{ und } n \in \mathbb{Z}.$$

Der Exponent n ist die **Ordnung von C in P** *wird mit $\operatorname{ord}_P(f)$ (oder auch $v_P(f)$) bezeichnet. Ist $\operatorname{ord}_P(f) > 0$, so sagt man, f hat in P eine* **Nullstelle**, *ist $\operatorname{ord}_P(f) < 0$, so sagt man, f hat in P eine* **Polstelle**.

Beweisidee:

- Der Einfachkeit halber beschränken wir uns auf den Fall $C \subseteq \mathbb{P}^2$. Nach Koordinatenwechsel können wir $P = (0,0) \in \mathbb{A}^2 \subseteq \mathbb{P}^2$ und $C \cap \mathbb{A}^2 = \{F(x,y) = 0\}$ annehmen. Wir betrachten die Taylorreihenentwicklung von F in $P = (0,0)$:

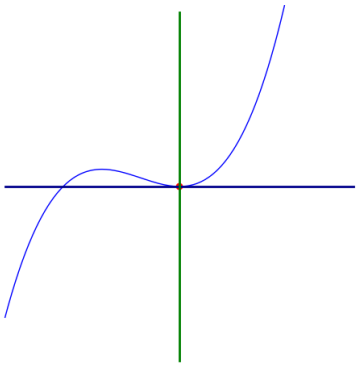
  $$F = ax + by + \text{ Terme mit Monomen vom Grad } \geq 2.$$

  Da C in P nichtsingulär sein soll, ist a oder $b \neq 0$. Nach einem weiteren Koordinatenwechsel können wir o.E. $b \neq 0$, auch $b = 1$ annehmen und dann

  $$F = y + ax + \text{ Terme mit Monomen vom Grad } \geq 2$$

  annehmen.

- Nochmals: $C \cap \mathbb{A}^2 = \{F(x,y) = 0\}$ mit $F = y + ax +$ Terme vom Grad ≥ 2.



- Wir klammern jetzt y überall aus und erhalten eine Darstellung
$$F = y(1 + A(x,y)) - B(x)x$$
mit Polynomen $A(x,y)$ und $B(x)$ und $A(0,0) = 0$. Im Funktionenkörper gilt also
$$y = \frac{B(x)x}{1 + A(x,y)} \quad \text{und} \quad \frac{B(x)}{1 + A(x,y)} \in \mathcal{O}_{C,P}.$$
- Nun ist $\overline{K}[C] = \overline{K}[x,y]/(F)$, das maximale Ideal des lokalen Rings wird also von x und y erzeugt: $\mathfrak{m}_{C,P} = (x,y)$. Mit unserer Relation folgt:
$$\mathfrak{m}_{C,P} = (x),$$
d.h. $\mathfrak{m}_{C,P}$ ist in $\mathcal{O}_{C,P}$ ein Hauptideal.
- Sei nun ein beliebiges Element $f \in \mathcal{O}_{C,P} \setminus \{0\}$ gegeben. Wir wollen zeigen, dass eine Funktion $u \in \mathcal{O}_{C,P}^*$ und ein $n \in \mathbb{N}_0$ existieren mit
$$f = u \cdot x^n.$$
Ist $f(P) \neq 0$, so ist f Einheit in P, wir wählen $u = f$ und $n = 0$ und sind fertig. Ist $f(P) = 0$, so ist $f \in \mathfrak{m}_{C,P} = (x)$, also gibt es $f_1 \in \mathcal{O}_{C,P}$ mit $f = f_1 \cdot x$. Nun kann man das gleiche Spiel mit f_1 machen, u.s.w. Man erhält $f_i = f_{i+1} \cdot x$, solange $f_i(P) = 0$ ist. Damit gilt
$$f = f_1 x = f_2 x^2 = \cdots = f_i x^i \quad \text{mit} \quad f_i \in \mathcal{O}_{C,P}.$$
- Warum muss dieser Prozess aufhören? Es ist $f_i = f_{i+1}x$, also $(f_i) \subsetneq (f_{i+1})$ und somit
$$(f) \subsetneq (f_1) \subsetneq (f_2) \subsetneq \ldots.$$
Der Hilbertsche Basissatz besagt nun, dass es keine unendlich echt aufsteigende Idealkette geben kann. Also bricht der Prozess ab und wir erhalten eine gewünschte Darstellung.
- Jedes Element hat also die Form $f = ux^n$ mit $u(P) \neq 0$, d.h. $u \in \mathcal{O}_{C,P}^*$, und $n \geq 0$.
- Zur Eindeutigkeit: Sei $ux^m = vx^n$ mit Einheiten u, v und $m \geq n \geq 0$. Dann ist $ux^{m-n} = v$ Einheit, also $m = n$ und $u = v$.
- Jedes Element $f \neq 0$ im Funktionenkörper lässt sich als Quotient von Polynomen, insbesondere als Quotient von Elementen aus $\mathcal{O}_{C,P}$ darstellen. Daraus folgt die letzte Behauptung. ■

Der Beweis zeigt, wie man in einem nichtsingulären Punkt an eine Ortsuniformisierende kommt. Wir formulieren dies nochmals als Satz:

SATZ. *Sei C eine absolut irreduzible Kurve und $C \cap \mathbb{A}^2 = \{F(x,y) = 0\}$ mit einem absolut irreduziblen Polynom $F(x,y)$. Sei $P = (a,b) \in C(\overline{K})$ ein nichtsingulärer Punkt von C.*

(1) *Sind $A, B \in \overline{K}$ mit $(A,B) \neq (0,0)$, sodass*
$$t = A(x-a) + B(y-b)$$
nicht die Tangente an C in P beschreibt, d.h. $(A : B) \neq (\frac{\partial F}{\partial x}(P) : \frac{\partial F}{\partial y}(P))$, so ist t eine Uniformisierende des lokalen Rings von C in P.

(2) *Ist* $\frac{\partial F}{\partial x}(P) \neq 0$*, so ist* $y - b$ *eine Uniformisierende in* $P = (a, b)$.
(3) *Ist* $\frac{\partial F}{\partial y}(P) \neq 0$*, so ist* $x - a$ *eine Uniformisierende in* $P = (a, b)$.

Bemerkung: Ist $C \subseteq \mathbb{P}^n$ und $P \in C \cap \mathbb{A}^n$, so kann man als Uniformisierende jede Linearform t wählen, wenn die Hyperebene $t = 0$ den Punkt P enthält, nicht aber die Tangente von C in P.

Bemerkung: Sei P ein nichtsingulärer Punkt auf der Kurve C. Die Funktion ord_P kann man dann als Funktion

$$\operatorname{ord}_P : \overline{K}(C) \to \mathbb{Z} \cup \{\infty\}$$

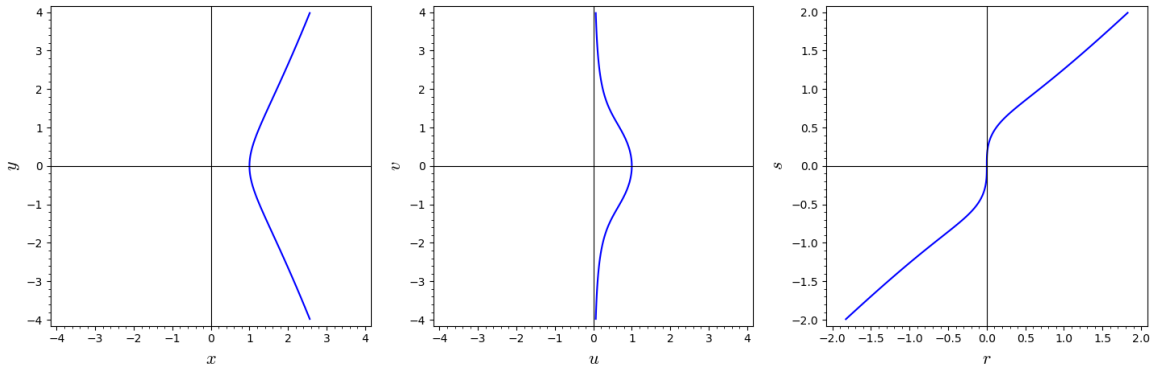
betrachten, wenn man noch $\operatorname{ord}_P(0) = \infty$ setzt. Man hat die folgenden Eigenschaften:

- $\operatorname{ord}_P(fg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g)$,
- $\operatorname{ord}_P(f + g) \geq \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$,
- ist $\operatorname{ord}_P(f) \neq \operatorname{ord}_P(g)$, so gilt $\operatorname{ord}_P(f + g) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$,
- ord_P ist surjektiv.

Es gilt:

$$\mathcal{O}_{C,P} = \{f \in \overline{K}(C)^* : \operatorname{ord}_P(f) \geq 0\}.$$

Beispiel: Sei $C \subseteq \mathbb{P}^2$ definiert durch $y^2 = x^3 - 1$, d.h. $C = \{x_0 x_2^2 = x_1^3 - x_0^3\}$.



Wir wollen für jeden Kurvenpunkt eine Uniformisierende bestimmen.

- *Im Endlichen:* Sei $(a, b) \in C$. Die Tangente ist $-3a^2(x - a) + 2b(y - b) = 0$. Ist $b \neq 0$, so ist $x - a$ uniformisierend, ist $b = 0$, so ist y uniformisierend:

$$t_P = \begin{cases} x - a & \text{für } P = (a, b) \text{ mit } b \neq 0, \\ y & \text{für } P = (a, 0). \end{cases}$$

- *Im Unendlichen:* Es gibt nur den Punkt $(0 : 0 : 1)$. Wir betrachten die Kurve in $U_2 = \{(r : s : 1) : r, s \in \overline{K}\}$ mit den affinen Koordinaten r, s. Der Punkt $(0 : 0 : 1)$ hat hier die Koordinaten $(r, s) = (0, 0)$. Die Kurve wird beschrieben durch die Gleichung

$$r = s^3 - r^3.$$

  Die Tangente in $(r, s) = (0, 0)$ ist offensichtlich $r = 0$, also können wir also Uniformisierende s wählen. Mit

$$(1 : x : y) = (r : s : 1) = (1 : \frac{s}{r} : \frac{1}{r})$$

  erhält man $x = \frac{s}{r}$ und $y = \frac{1}{r}$ bzw. $r = \frac{1}{y}$ und $s = \frac{x}{y}$.

Wir wollen jetzt die Null- und Polstellen der Funktion $f = y$ bestimmen.

- *Im Endlichen:* Hier hat y keine Polstelle. Es gibt 3 Nullstellen: $P_1 = (1, 0), P_2 = (\zeta, 0), P_3 = (\zeta^2, 0)$, wo $\zeta = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist. In allen 3 Punkten ist y uniformisierend, also $\operatorname{ord}_{P_i}(y) = 1$, d.h. in allen 3 Punkten hat y eine einfache Nullstelle.

- *Im Unendlichen:* Hier gibt es nur den Punkt $(0:0:1)$. Es ist $y = \frac{1}{r}$. Wir haben $r = s^3 - r^3$, s ist uniformisierend. Auch r hat eine Nullstelle. Wegen $r(1+r^2) = s^3$ gilt $r = \frac{1}{1+r^2}s^3$, also folgt sofort $\operatorname{ord}_{(0:0:1)}(r) = 3$ und daher $\operatorname{ord}_{(0:0:1)}(y) = -3$.

Beispiel: Die Kurve $\mathbb{P}^1$ hatten wir bereits früher behandelt. Wir hatten zerlegt

$$\mathbb{P}^1 = \{(1:a) : a \in \overline{K}\} \cup \{(0:1)\} \simeq \overline{K} \cup \{\infty\}.$$

Der Funktionenkörper von $\mathbb{P}^1$ ist $\overline{K}(x)$ mit $x = \frac{x_1}{x_0}$. In $a \in \overline{K}$ ist $x - a$ uniformisierend, in ∞ ist $u = \frac{1}{x}$ uniformisierend.
Jedes $f \in \overline{K}(x), f \neq 0$ hat eine eindeutige Zerlegung

$$f = c\prod_{i=1}^{r}(x-\alpha_i)^{e_i},$$

wobei $\alpha_1, \ldots, \alpha_r, c \in \overline{K}$, $e_i \in \mathbb{Z}$ und die Zahlen $\alpha_1, \ldots, \alpha_r$ paarweise verschieden sind. Dann gilt

$$\operatorname{ord}_{\alpha_i}(f) = e_i \quad \text{und} \quad \operatorname{ord}_{\alpha}(f) = 0 \text{ für } \alpha \in \overline{K} \setminus \{\alpha_1, \ldots, \alpha_r\}.$$

Was ist $\operatorname{ord}_{\infty}(f)$? Wir schreiben

$$f = \frac{a_m x^m + \cdots + a_0}{b_n x^n + \cdots + b_0} \text{ mit } a_m, b_n \neq 0.$$

Dann gilt

$$f = u^{n-m} \cdot \frac{a_m + a_{m-1}u + \cdots + a_0 u^m}{b_n + b_{n-1}u + \cdots + b_0 u^n}.$$

Der Bruch ist in ∞ definiert und hat den Wert $\frac{a_m}{b_n} \neq 0$. Also gilt $\operatorname{ord}_{\infty}(f) = n - m$.

Die Tatsache, dass der lokale Ring in einem nichtsingulären Punkt einer Kurve ein diskreter Bewertungsring ist, hat erstaunliche Konsequenzen:

Satz. *Sei C eine Kurve, Y eine projektive Varietät $\phi : C \to Y$ eine rationale Abbildung. Ist $P \in C$ ein nichtsingulärer Punkt von C, so ist ϕ in P definiert.*

Beweis: Sei $\phi = (f_0 : \cdots : f_n)$ mit $f_i \in \overline{K}(C)$. Sei t uniformisierend in P. Wir können o.E. $f_i \neq 0$ annehmen, sonst lassen wir die entsprechende Koordinate weg. Dann ist $f_i = u_i \cdot t^{e_i}$, wo u_i Einheit in P ist, also $u_i(P) \neq 0$, und damit

$$\phi = (u_0 t^{e_0} : u_1 t^{e_1} : \cdots : u_n t^{e_n}).$$

Sei o.E. $e_0 = \min(e_0, \ldots, e_n)$. Dann gilt

$$\phi = (u_0 : u_1 t^{e_1 - e_0} : \cdots : u_n t^{e_n - e_0})$$

und man sieht an dieser Darstellung, dass ϕ in P definiert ist. ■

Damit folgt unmittelbar:

Satz. *Ist C eine nichtsinguläre Kurve, Y eine projektive Varietät und $\phi : C \to Y$ eine rationale Abbildung, so ist ϕ schon ein Morphismus.*

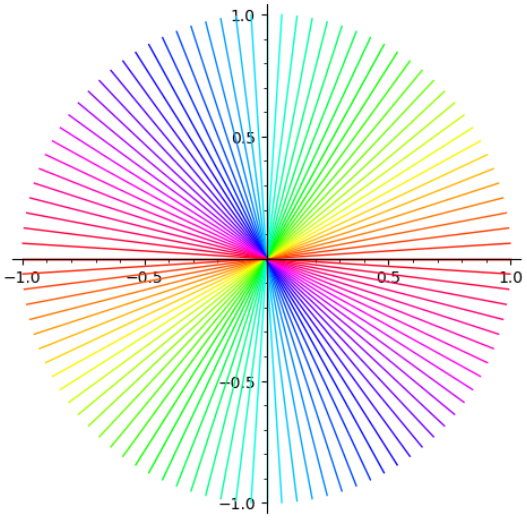
Satz. *Zwei birational äquivalente, nichtsinguläre, absolut irreduzible, projektive Kurven sind schon isomorph.*

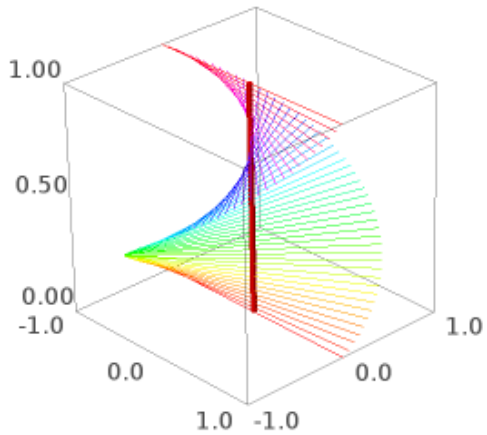
Was bedeutet das? In einer Äquivalenzklasse birational äquivalenter Kurven gibt es bis auf Isomorphie höchstens eine nichtsinguläre Kurve. Es stellt sich dann sofort die Frage: Ist jede Kurve birational äquivalent zu einer nichtsingulären Kurve? Wie findet man eine solche? Wir wissen bereits, dass jede Kurve zu einer ebenen Kurve birational äquivalent ist. Wir werden jetzt Singularitäten ebener Kurven durch „Aufblasen“ auflösen.

Vorbemerkung: Da Singularitäten ein lokales Phänomen sind, werden wir uns im folgenden auf die 2-dimensionale affine Darstellung beschränken.

Aufblasung von $\mathbb{A}^2$ in $(0,0)$:

- Sei
$$X = \{((x,y),(z_0:z_1)) \in \mathbb{A}^2 \times \mathbb{P}^1 : xz_1 = yz_0\}$$
und $\pi : X \to \mathbb{A}^2$ die Projektion auf die erste Komponente. Man nennt π bzw. X die Aufblasung von $\mathbb{A}^2$ in $P = (0,0)$.
- Wir betrachten einen Punkt $((x,y),(z_0:z_1)) \in X$:
  - **Fall $x \neq 0$:** Dann ist $z_1 = \frac{y}{x} z_0$ und
$$((x,y),(z_0:z_1)) = ((x,y),(z_0 : \frac{y}{x} z_0)) = ((x,y),(x:y)).$$
  - **Fall $y \neq 0$:** Dann ist $z_0 = \frac{x}{y} z_1$ und
$$((x,y),(z_0:z_1)) = ((x,y),(\frac{x}{y} z_1 : z_1)) = ((x,y),(x:y)).$$
  - **Fall $x = y = 0$:** Dann hat man keine Bedingung:
$$((0,0),(z_0:z_1)).$$
- Wir haben also
$$X = \{((x,y),(x:y)) : (x,y) \in \mathbb{A}^2 \setminus \{(0,0)\}\} \cup \{((0,0),(z_0:z_1)) : (z_0:z_1) \in \mathbb{P}^1\}.$$
Also gilt
$$\pi^{-1}((x,y)) = \{((x,y),(x:y))\} \text{ falls } (x,y) \neq (0,0),$$
$$\pi^{-1}((0,0)) = \{((0,0),(z_0:z_1)) : (z_0:z_1) \in \mathbb{P}^1\}.$$
Definiert man jetzt $E = \{((0,0),(z_0:z_1)) \in X : (z_0:z_1) \in \mathbb{P}^1\}$, so ist offensichtlich
$$E = \pi^{-1}((0,0)) \simeq \mathbb{P}^1.$$
Man nennt E den **exzeptionellen Divisor** oder die **exzeptionelle Faser**.
- Definiert man weiter $\phi : \mathbb{A}^2 \to X$ durch $(x,y) \mapsto ((x,y),(x:y))$, so ist ϕ definiert auf $\mathbb{A}^2 \setminus \{(0,0)\}$ und induziert einen Isomorphismus
$$X \setminus E \simeq \mathbb{A}^2 \setminus \{(0,0)\}.$$
- Überlegung: Die Punkte der Gerade $y = \lambda x$ werden durch ϕ abgebildet auf $((x,y),(1:\lambda))$. Die Gerade trifft also den exzeptionellen Divisor im Punkt $((0,0),(1:\lambda))$. Verschiedene Geraden treffen den exzeptionellen Divisor in verschiedenen Punkten.





Aufblasung zum Anklicken Was ist also passiert? Man ersetzt in $\mathbb{A}^2$ den Punkt $(0,0)$ durch eine projektive Gerade, man *bläst auf*. Vorstellung: Man zieht den Nullpunkt nach oben und nimmt dabei die Geraden $y = \lambda x$ mit.

- **Wie rechnet man mit der Aufblasung** $X = \{((x,y),(z_0:z_1)) \in \mathbb{A}^2 \times \mathbb{P}^1 : xz_1 = yz_0\}$**?** Wir betrachten die offene Überdeckung $X = \{z_0 \neq 0\} \cup \{z_1 \neq 0\}$:
  - **Fall** $z_0 \neq 0$**:** Sei $z = \frac{z_1}{z_0}$. Es ist
  $$\begin{aligned} X \cap \{z_0 \neq 0\} &= \{((x,y),(z_0:z_1)) : xz_1 = yz_0\} = \{((x,y),(1:z)) : xz = y\} = \\ &= \{((x,xz),(1:z))\} \simeq \{(x,z) \in \mathbb{A}^2\} \simeq \mathbb{A}^2. \end{aligned}$$
  In diesem affinen Teil bilden also x und $z = \frac{z_1}{z_0}$ affine Koordinaten, der exzeptionelle Divisor E ist hier gegeben durch die einzige Gleichung $x = 0$.
  - **Fall** $z_1 \neq 0$**:** Sei $t = \frac{z_0}{z_1} = \frac{1}{z}$. Es ist
  $$\begin{aligned} X \cap \{z_1 \neq 0\} &= \{((x,y),(z_0:z_1)) : xz_1 = yz_0\} = \{((x,y),(t:1)) : x = yt\} = \\ &= \{((yt,y),(t:1))\} \simeq \{(y,t) \in \mathbb{A}^2\} \simeq \mathbb{A}^2. \end{aligned}$$
  In diesem affinen Teil bilden also y und $t = \frac{z_0}{z_1}$ affine Koordinaten, des exzeptionelle Divisor E ist hier gegeben durch die einzige Gleichung $y = 0$.

  Wir können also Phänomene in den affinen Teilen $\{z_0 \neq 0\}$ und $\{z_1 \neq 0\}$ studieren. Oft kommt man mit einem Teil aus, denn
  $$\{z_0 = 0\} = \{((0,y),(0:1))\} \quad \text{und} \quad \{z_1 = 0\} = \{((x,0),(1:0))\}.$$
- Sei $C \subseteq \mathbb{A}^2$ eine Kurve, die den Punkt $(0,0)$ enthält. Natürlich gilt dann $E \subseteq \pi^{-1}(C)$, d.h. in $\pi^{-1}(C)$ ist der exzeptionelle Divisor immer enthalten. Daher definiert man das **eigentliche Urbild** $\widetilde{C}$ von C als
  $$\widetilde{C} = \overline{\pi^{-1}(C \setminus \{(0,0)\})},$$
  wo Überstreichen den Zariski-Abschluss bedeutet. Klar ist:
  $$\widetilde{C} \setminus E \simeq C \setminus \{(0,0\},$$
  d.h. C und $\widetilde{C}$ sind birational äquivalent. C und $\widetilde{C}$ unterscheiden sich also nur in den Punkten von $\widetilde{C} \cap E$. D.h. wenn man wissen will, wie Aufblasen C verändert, muss man nur die endlich vielen Punkte auf $\widetilde{C} \cap E$ betrachten.

Beispiel: Was passiert mit Geraden durch $(0,0)$? Wir betrachten als Beispiel eine Gerade G_λ, die durch die Gleichung $y = \lambda x$ gegeben wird (mit $\lambda \in \overline{K}$).

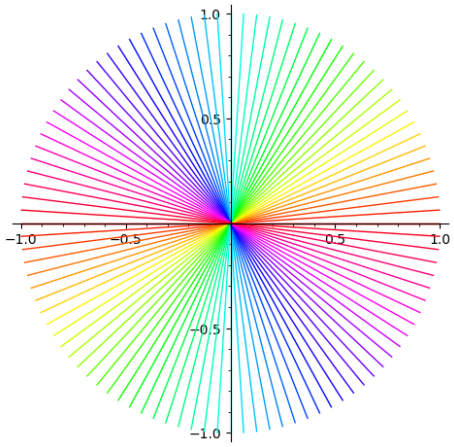
- Im affinen Teil $X \cap \{z_0 \neq 0\}$ verwenden wir die affinen Koordinaten x, z mit $y = xz$ und haben dann
  $$X \cap \{z_0 \neq 0\} = \{((x,xz),(1:z))\}.$$
  Die Gerade erhält die Gleichung
  $$xz = \lambda x, \quad \text{also} \quad x(z - \lambda) = 0.$$
  Da die exzeptionelle Faser durch $x = 0$ gegeben wird, wird das eigentliche Urbild der Geraden durch
  $$z - \lambda = 0$$
  gegeben, also
  $$X \cap \{z_0 \neq 0\} \cap \widetilde{G}_\lambda = \{(x,\lambda x),(1:\lambda) : x \in \overline{K}\}.$$
  $\widetilde{G}_\lambda$ schneidet die exzeptionelle Faser im Punkt $((0,0),(1:\lambda))$.
- Im affinen Teil $X \cap \{z_1 \neq 0\}$ verwenden wir die affinen Koordinaten y, t mit $x = yt$. Es ist
  $$X \cap \{z_1 \neq 0\} = \{(yt,y),(t:1)\}.$$
  Die Gerade erhält nun die Gleichung
  $$y = \lambda yt \quad \text{bzw.} \quad y(1 - \lambda t) = 0.$$
  Die exzeptionelle Faser wird durch $y = 0$ gegeben, das eigentliche Urbild der Geraden durch $1 - \lambda t = 0$. Daher ist
  $$X \cap \{z_1 \neq 0\} \cap \widetilde{G}_\lambda = \{((yt,y),(t:1)) : \lambda t = 1\}.$$

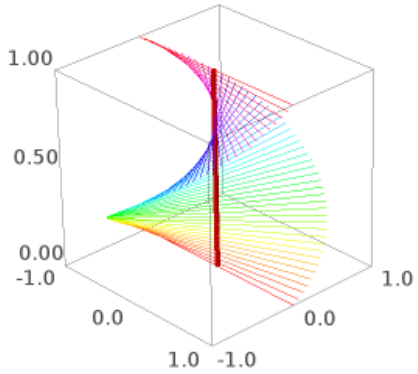
$\widetilde{G}_\lambda$ schneidet die exzeptionelle Faser im Punkt $((0,0),(\frac{1}{\lambda}:1))$, falls $\lambda \neq 0$ ist, sonst nicht. Dies liefert keine neue Information.

Als Ergebnis erhalten wir

$$\widetilde{G}_\lambda = \{((x,\lambda x),(1:\lambda)) \in X : x \in \overline{K}\}.$$

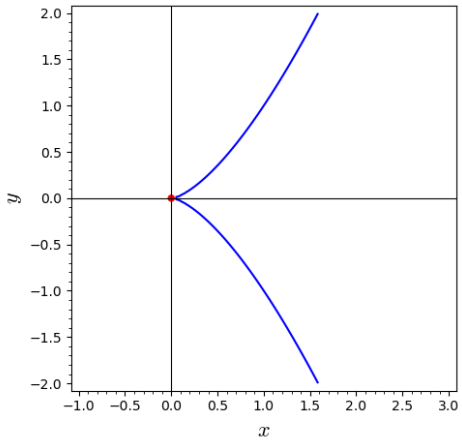
Verschiedene Geraden G_λ durch $(0,0)$ werden also beim Aufblasen „auseinandergezogen“.

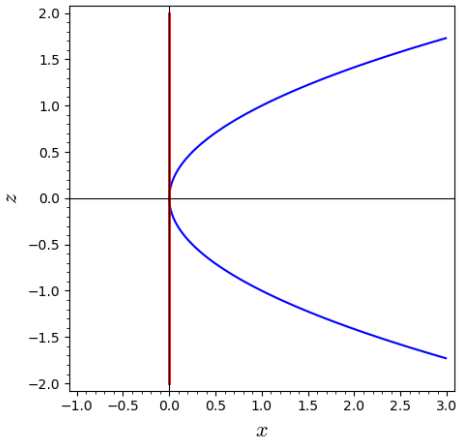




Beispiel: Die durch $y^2 = x^3$ definierte Kurve C hat eine Singularität in $(0,0)$. Wir blasen $\mathbb{A}^2$ in $(0,0)$ auf und wollen das eigentliche Urbild $\widetilde{C}$ von C bestimmen.

- Im affinen Teil
$$X \cap \{z_0 \neq 0\} = \{((x,xz),(1:z))\}$$
mit den affinen Koordinaten x, z setzen wir $y = xz$ in die Kurvengleichung ein:
$$0 = y^2 - x^3 = (xz)^2 - x^3 = x^2(z^2 - x).$$
Die exzeptionelle Faser wird durch $x = 0$ beschrieben, das eigentliche Urbild $\widetilde{C}$ von C durch
$$x = z^2.$$
Einziger Schnittpunkt der exzeptionellen Faser mit $\widetilde{C}$ ist der Punkt $(x,z) = (0,0)$, der nichtsingulär ist.





- Im affinen Teil
$$X \cap \{z_1 \neq 0\} = \{((yt,y),(t:1)\}$$
mit den affinen Koordinaten y, t setzen wir $x = yt$ in die Kurvengleichung ein:
$$0 = y^2 - x^3 = y^2 - y^3t^3 = y^2(1 - yt^3).$$

Das eigentliche Urbild $\widetilde{C}$ von C wird hier durch $1 = yt^3$ beschrieben, es schneidet die exzeptionelle Faser $y = 0$ nicht.

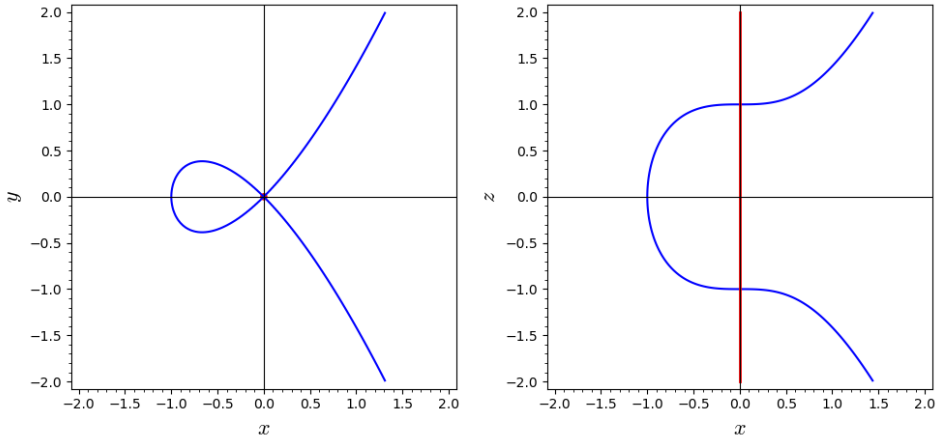
Ergebnis: $\widetilde{C}$ ist nichtsingulär und

$$X \cap \{z_0 \neq 0\} \cap \widetilde{C} = \{((x, xz), (1 : z)) : x = z^2\} \quad \text{und} \quad E \cap \widetilde{C} = \{((0, 0), (1 : 0))\}.$$

Wir haben also die Singularität von C durch Aufblasen aufgelöst.

Beispiel: $y^2 = x^2 + x^3$ definiert eine Kurve C, die in $(0, 0)$ singulär ist. Wir blasen $\mathbb{A}^2$ in $(0, 0)$ auf und bestimmen das eigentliche Urbild von C.

- Im affinen Teil
$$X \cap \{z_0 \neq 0\} = \{((x, xz), (1 : z))\}$$
mit den affinen Koordinaten x, z setzen wir $y = xz$ in die Kurvengleichung ein:
$$0 = y^2 - x^2 - x^3 = (xz)^2 - x^2 - x^3 = x^2(z^2 - 1 - x).$$
Die exzeptionelle Faser wird durch $x = 0$ beschrieben, das eigentliche Urbild $\widetilde{C}$ von C durch
$$x = z^2 - 1.$$
$\widetilde{C}$ schneidet die exzeptionelle Faser in den zwei Punkten $(x, z) = (0, \pm 1)$, also in
$$((0, 0), (1 : \pm 1)).$$
$\widetilde{C}$ ist in diesen Punkten nichtsingulär.



- Im affinen Teil
$$X \cap \{z_1 \neq 0\} = \{((yt, y), (t : 1))\}$$
mit den affinen Koordinaten y, t setzen wir $x = yt$ in die Kurvengleichung ein:
$$0 = y^2 - x^2 - x^3 = y^2 - y^2t^2 - y^3t^3 = y^2(1 - t^2 - yt^3).$$
Das eigentliche Urbild $\widetilde{C}$ von C wird durch die Gleichung
$$t^2 = 1 - yt^3$$
beschrieben. Die Schnittpunkte mit der exzeptionellen Faser sind die Punkte $(y, t) = (0, \pm 1)$, also
$$((0, 0), (\pm 1 : 1)).$$
Diese Punkte haben wir aber schon untersucht und müssen deshalb nicht weiter betrachtet werden.

Ergebnis: $\widetilde{C}$ ist nichtsingulär mit

$$\widetilde{C} \cap E = \{((0,0),(1:1)),((0,0),(1:-1))\}.$$

Wir haben also C durch Aufblasen desingularisiert. Denken wir uns $\widetilde{C}$ in der affinen Ebene mit den Koordinaten x, z gegeben durch $x = z^2 - 1$, so ist

$$\widetilde{C} = \{(x,z) \in \mathbb{A}^2 : x = z^2 - 1\} \xrightarrow{(x,z)\mapsto(x,xz)} C = \{(x,y) \in \mathbb{A}^2 : y^2 = x^2 + x^3\}$$

ein birationaler Morphismus und eingeschränkt auf $\widetilde{C} \setminus \{(0,1),(0,-1)\} \to C \setminus \{(0,0)\}$ ein Isomorphismus.

Sei C eine ebene Kurve. Wie löst man die Singularitäten von C auf? Sei C_0 die Aufblasung von C in einem singulären Punkt. Dann ist $\pi_0 : C_0 \to C$ ein birationaler Morphismus. Ist C_0 noch singulär, so blase man einen singulären Punkt von C_0 auf. Man kann dies lokal, also affin machen. Man erhält $\pi_1 : C_1 \to C_0$, etc.

$$\cdots \to C_n \overset{\pi_n}{\to} C_{n-1} \overset{\pi_{n-1}}{\to} C_{n-2} \to \cdots \to C_1 \overset{\pi_1}{\to} C_0 \overset{\pi_0}{\to} C,$$

wobei die π_i birationale Morphismen sind. Die entscheidende Tatsache ist nun, dass man durch diesen Prozess irgendwann bei einer nichtsingulären Kurve ankommt, was wir aber nicht beweisen werden. Durch Aufblasen kann man also eine ebene Kurve desingularisieren. (Einen Beweis findet man bei [**Hartshorne**, Proposition 3.8, S.390].) Damit erhält man schließlich:

Satz. *Zu jeder irreduziblen projektiven Kurve C gibt es eine nichtsinguläre irreduzible projektive Kurve $\widehat{C}$ und einen birationalen Morphismus $\pi : \widehat{C} \to C$. Die Kurve $\widehat{C}$ ist bis auf Isomorphie eindeutig bestimmt. Man sagt, $\widehat{C}$ ist ein nichtsinguläres Modell von C.*

Bemerkung: Wir haben den Aufblasprozess bisher nur affin 2-dimensional betrachtet. Man kann man auch allgemein einen Punkt im $\mathbb{P}^n$ aufblasen: Man nennt

$$X = \{((x_0 : x_1 : \cdots : x_n),(y_1 : \cdots : y_n)) \in \mathbb{P}^n \times \mathbb{P}^{n-1} : x_i y_j = x_j y_i \text{ für } i,j = 1,\ldots,n\}$$

zusammen mit der Projektion $\pi : X \to \mathbb{P}^n$ die Aufblasung von $\mathbb{P}^n$ im Punkt $(1:0:\cdots:0)$.

Wir wollen nochmals Morphismen zwischen glatten projektiven Kurven betrachten.

Beispiel: Sei $C \subseteq \mathbb{P}^2$ definiert durch $y^2 = x^3 - 1$ und $\phi : C \to \mathbb{P}^1$ durch $\phi = (1:y)$. Für $c \in \overline{K}$ gilt

$$\phi^{-1}((1:c)) = \{(1:x:c) \in C : x^3 = c^2 + 1\}.$$

Für $c \neq \pm i$ gibt es also genau 3 Urbilder von c. Außerdem gilt:

$$[\overline{K}(C) : \overline{K}(y)] = [\overline{K}(x,y) : \overline{K}(y)] = 3.$$

Dies ist nun ein ganz allgemeines Phänomen.

Sei $\phi : C_1 \to C_2$ ein Morphismus zwischen glatten projektiven Kurven. Wir wissen: ist ϕ nicht konstant, so ist ϕ surjektiv. Außerdem ist dann $\overline{K}(C_1)$ eine endliche algebraische Körpererweiterung von $\phi^*\overline{K}(C_2)$.

Definition. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen glatten projektiven Kurven. Dann heißt*

$$\operatorname{grad}(\phi) = [\overline{K}(C_1) : \phi^*\overline{K}(C_2)]$$

der **Grad von** *ϕ. Man sagt, ϕ ist* **separabel**, *wenn die Körpererweiterung $\overline{K}(C_1)|\phi^*\overline{K}(C_2)$ separabel ist.*

Um die Urbilder $\phi^{-1}(P)$ eines Punktes P richtig zu zählen, brauchen wir noch folgende Definition:

Definition. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus glatter projektiver Kurven und $P \in C_1$. Ist $t_{\phi(P)}$ eine Uniformisierende im Punkt $\phi(P)$, so heißt*

$$e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi(P)})$$

der **Verzweigungsindex** *von ϕ im Punkt P. (Wegen $(\phi^* t_{\phi(P)})(P) = t_{\phi(P)}(\phi(P)) = 0$ gilt immer $e_\phi(P) \geq 1$.) ϕ heißt* **verzweigt in** *P, falls $e_\phi(P) \geq 2$ gilt. Der Morphismus ϕ heißt* **unverzweigt**, *falls $e_\phi(P) = 1$ für alle $P \in C_1$ gilt.*

$e_\phi(P)$ zählt also, *wie oft* der Punkt P unter ϕ auf den Punkt $\phi(P)$ abgebildet wird. Dies wird noch deutlicher durch folgendes

Beispiel: Sei C eine glatte projektive Kurve und $f \in \overline{K}(C), f \notin \overline{K}$. Wir betrachten den Morphismus $\phi : C \to \mathbb{P}^1$ mit $\phi = (1 : f)$ und einen Punkt $P \in C$ mit $\phi(P) = Q$.
Fall $Q = (1 : a)$**:** In Q ist $x - a$ uniformisierend (mit $x = \frac{x_1}{x_0}$), also ist $\phi^*(x - a) = f - a$ und daher

$$e_\phi(P) = \text{ord}_P(f - a).$$

Ist $a = 0$, so ist $e_\phi(P) = \text{ord}_P(f)$ die Nullstellenordnung von f.
Fall $Q = (0 : 1)$**:** In Q ist $u = \frac{1}{x} = \frac{x_0}{x_1}$ uniformisierend, mit $\phi^*(\frac{1}{x}) = \frac{1}{f}$ gilt dann

$$e_\phi(P) = \text{ord}_P(\frac{1}{f}) = -\text{ord}_P(f).$$

Nun gilt der wichtige Satz, für dessen Beweis wir auf [**Silverman**, Proposition 2.6, S.23-24] verweisen:

Satz. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen glatten projektiven Kurven. Dann gilt:*

(1) *Für alle $Q \in C_2$ ist*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \text{grad}(\phi).$$

(2) *Ist ϕ separabel, so gibt es nur endlich viele Verzweigungspunkte, d.h. Punkte P mit $e_\phi(P) \geq 2$, insbesondere gilt für alle Punkte Q von C_2 mit nur endlich vielen Ausnahmen:*

$$\#\phi^{-1}(Q) = \text{grad}(\phi).$$

Jede nichtkonstante Funktion $f \in \overline{K}(C)$ liefert durch $\phi = (1 : f)$ einen Morphismus $\phi : C \to \mathbb{P}^1$, mit unserem letzten Beispiel folgt sofort:

Folgerung. *Ist C eine glatte Kurve und $f \in \overline{K}(C) \setminus \overline{K}$, so nimmt f jeden Wert gleich oft an, wenn man mit Vielfachheiten zählt.*

Es gibt also genauso viele Null- wie Polstellen, womit wir haben:

Folgerung. *Ist C eine glatte Kurve und $f \in \overline{K}(C)$, so gilt*

$$\sum_{P \in C} \text{ord}_P(f) = 0.$$

Bemerkungen:

- Später werden wir uns näher mit sogenannten **hyperelliptischen Kurven** beschäftigen. Im Wesentlichen werden diese dadurch charakterisiert, dass sie nichtsinguläre, absolut irreduzible, projektive Kurven C sind, die einen Morphismus

$$\phi : C \to \mathbb{P}^1 \quad \text{mit} \quad \text{grad}(\phi) = 2$$

besitzen. (Auch $\mathbb{P}^1$ und sogenannte **elliptische Kurven** besitzen einen Morphismus $\phi : C \to \mathbb{P}^1$ vom Grad 2, die aber nicht als hyperelliptische Kurven gezählt werden.)
- Wie kann man Kurven C beschreiben, die einen Morphismus $\phi : C \to \mathbb{P}^1$ vom Grad 2 besitzen? Sei $\phi : C \to \mathbb{P}^1$ ein Morphismus vom Grad 2. Als rationale Abbildung lässt sich ϕ schreiben als $\phi = (1 : \xi)$ mit $\xi \in \overline{K}(C) \setminus \overline{K}$. Verwenden wir wie üblich auf $\mathbb{P}^1$ die Koordinatenfunktion x, so ist $\phi^*(x) = \xi$. Dass ϕ Grad 2 hat, bedeutet, dass $\overline{K}(C)$ eine Körpererweiterung vom Grad 2 von $\phi^*\overline{K}(\mathbb{P}^1) = \phi^*\overline{K}(x) = \overline{K}(\xi)$ ist. Setzen zusätzlich voraus, dass die Charakteristik von K von 2 verwenden ist, so existiert ein $\eta \in \overline{K}(C)$ und ein Polynom separables Polynom $f(x) \in \overline{K}[x]$ mit

$$\overline{K}(C) = \overline{K}(\xi)(\eta) \quad \text{und} \quad \eta^2 = f(\xi).$$

(Dies entspricht der Aussage, dass die quadratischen Erweiterungen von $\mathbb{Q}$ in der Form $\mathbb{Q}(\sqrt{d})$ mit quadratfreien Zahlen $d \in \mathbb{Z} \setminus \{0,1\}$ geschrieben werden können.) Dann ist

$$\overline{K}(C) \simeq \mathrm{Quot}(\overline{K}[x,y]/(y^2 - f(x))),$$

C ist also birational äquivalent zu der durch

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

definierten Kurve, bei der der Morphismus nach $\mathbb{P}^1$ einfach durch $(x,y) \mapsto x$ gegeben wird.

Exkurs: Potenzreihenentwicklungen - Laurentreihenentwicklungen

LEMMA. *Sei t uniformisierend in einem Punkt P einer Kurve C. Zu $g \in K(C)^*$ mit $m = \mathrm{ord}_P(g)$ und $n \geq m$ gibt es dann Zahlen $c_m, c_{m+1}, \ldots, c_n \in K$ mit*

$$g \equiv \sum_{i=m}^{n} c_i t^i \bmod t^{n+1},$$

d.h.

$$g - \sum_{i=m}^{n} c_i t^i \in t^{n+1}\mathcal{O}_{C,P}.$$

Die Koeffizienten c_i sind eindeutig bestimmt.

Beweis:

- *Existenz:* Sei zunächst $g \in \mathcal{O}_{C,P}$. Definiere $c_0 = g(P)$. Dann lässt sich zerlegen

  $$g = c_0 + g_1 t,$$

  wo wieder $g_1 \in \mathcal{O}_{C,P}$ ist. Dies lässt sich iterieren: Definiere $c_i = g_i(P)$ und schreibe $g_i = c_i + g_{i+1}t$ mit $g_{i+1} \in \mathcal{O}_{C,P}$. So erhält man

  $$g = c_0 + g_1 t = c_0 + c_1 t + g_2 t^2 = c_0 + c_1 t + c_2 t^2 + g_3 t^3 = \cdots = c_0 + c_1 t + \cdots + c_n t^n + g_{n+1} t^{n+1}.$$

  Damit hat man die gewünschte Zerlegung erhalten.
  Ist $\mathrm{ord}_P(g) = -s < 0$, so entwickle man $t^s g \in \mathcal{O}_{C,P}$ modulo t^{n+1+s} und dividiere dann anschließend durch t^s.
- *Eindeutigkeit:* Es genügt die Eindeutigkeit für $g \in \mathcal{O}_{C,P}$ zu zeigen. Angenommen

  $$g - \sum_{0 \leq i \leq n} c_i t^i \in t^{n+1}\mathcal{O}_{C,P} \quad \text{und} \quad g - \sum_{0 \leq i \leq n} d_i t^i \in t^{n+1}\mathcal{O}_{C,P},$$

  dann ist auch

  $$\sum_{0 \leq i \leq n} (c_i - d_i) t^i \in t^{n+1}\mathcal{O}_{C,P},$$

  was nur sein kann, wenn alle $c_i = d_i$ sind. ■

Das vorangegangene Lemma deutet schon an, dass man einer Funktion des Funktionenkörpers $K(C)$ eine Potenzreihenentwicklung in einem Punkt P zuordnen kann. Kann man dies auch praktisch machen?

Sei eine Kurve C durch eine affine Gleichung $f(x,y) = 0$ gegeben zusammen mit einem nichtsingulären Kurvenpunkt $P = (a,b)$. (Den Funktionenkörper $K(C)$ kann man sich dann als $K(x,y)$ vorstellen, wo zwischen x und y die Beziehung $f(x,y) = 0$ gilt.) Die Tangente in P ist

$$\frac{\partial f}{\partial x}(a,b) \cdot (x-a) + \frac{\partial f}{\partial y}(a,b) \cdot (y-b) = 0.$$

Ist nun $\frac{\partial f}{\partial y}(a,b) \neq 0$, so ist $x - a = 0$ nicht die Tangente, also können wir $t = x - a$ als Uniformisierende in P verwenden. Nach dem vorangegangenen Lemma können wir jede Funktion $g \in K(C)^*$ in der Gestalt

$$g \equiv \sum_{i=m}^{n} c_i t^i \bmod t^{n+1}$$

entwickeln für beliebig große n. Da der Funktionenkörper $K(C)$ von x und y erzeugt wird, betrachten wir zunächst x und y. Nach Definition von t ist

$$x = a + t.$$

Wir suchen nun Zahlen $b_0, b_1, b_2, \dots$ mit

$$y \equiv \sum_{i=0}^{n} b_i t^i \bmod t^{n+1},$$

wobei wegen $y(P) = b$ natürlich $b_0 = b$ gilt.

Wir stellen hier ganz knapp ein paar Grundlagen zu Potenzreihen und Laurentreihen zusammen.

Man definiert den **Ring der formalen Potenzreihen** (in der Variablen t über dem Körper K) durch

$$K[[t]] = \left\{ \sum_{i \geq 0} a_i t^i : a_i \in K \right\}.$$

Es ist klar, wenn man addiert, multipliziert etc. Eine Potenzreihe $\sum_{i \geq 0} a_i t^i$ ist genau dann invertierbar, wenn $a_0 \neq 0$ gilt. Der Quotientenkörper $\mathrm{Quot}(K[[t]])$ wird mit den formalen Laurentreihen identifiziert:

$$K((t)) = \left\{ \sum_{i \geq n} a_i t^i, n \in \mathbb{Z}, a_i \in K \right\}.$$

Man definiert die Ordnung einer Potenz- bzw. Laurentreihe durch

$$\mathrm{ord}\,(\sum_{i \geq n} a_i t^i) = n, \text{ falls } a_n \neq 0.$$

Diese Ordnungsfunktion macht $K[[t]]$ zu einem vollständigen diskreten Bewertungsring.

LEMMA. *Sei $f(x,y) \in K[x,y]$, seien $a, b \in K$ mit $f(a,b) = 0$ und $\frac{\partial f}{\partial y}(a,b) \neq 0$. Sei t eine Variable über K. Beginnend mit $b_0 = b$ werden rekursiv Zahlen $b_0, b_1, b_2, \dots$ aus K wie folgt definiert: Sind $b_0, b_1, \dots, b_k$ bereits definiert, so sei c_{k+1} der Koeffizient des Polynoms $f(a + t, \sum_{i=0}^{k} b_i t^i) \in K[t]$ bei t^{k+1}, also*

$$f(a + t, \sum_{i=0}^{k} b_i t^i) = \dots + c_{k+1} t^{k+1} + \dots \in K[t]$$

Damit wird definiert

$$b_{k+1} = -\frac{c_{k+1}}{\frac{\partial f}{\partial y}(a,b)}.$$

Dann gilt:

(1) *Es ist*

$$f(a + t, \sum_{i=0}^{n} b_i t^i) \equiv 0 \bmod t^{n+1} \text{ für alle } n \geq 0.$$

(2) *Die Reihe $\sum_{i=0}^{\infty} b_i t^i \in K[[t]]$ existiert in $K[[t]]$ und erfüllt die Gleichung*

$$f(a + t, \sum_{i=0}^{\infty} b_i t^i) = 0,$$

d.h. $(a + t, \sum_{i=0}^{\infty} b_i t^i)$ ist eine Nullstelle des Polynoms $f(x,y)$ in $K[[t]]$.

Beweis:

(0) Wir schreiben in $K[x,y,z]$

$$f(x,y+z) = A_0(x,y) + A_1(x,y)\cdot z + A_2(x,y)\cdot z^2 + \dots.$$

Setzt man $z=0$, so erhält man $A_0(x,y) = f(x,y)$. Differenziert man nach z, so erhält man

$$\frac{\partial f}{\partial y}(x,y+z) = A_1(x,y) + A_2(x,y)\cdot 2z + \dots,$$

setzt man $z=0$ ein, so erhält man $A_1(x,y) = \frac{\partial f}{\partial y}(x,y)$. Insgesamt:

$$f(x,y+z) = f(x,y) + \frac{\partial f}{\partial y}(x,y)\cdot z + \text{ höhere Terme in } z.$$

(1) Wir zeigen durch Induktion, dass

$$f(a+t, \sum_{i=0}^{k} b_i t^i) \equiv 0 \bmod t^{k+1} \text{ für alle } k \geq 0$$

gilt.

- Der Induktionsanfang $k=0$ ist wegen
$$f(a,b_0) = f(a,b) = 0$$
trivialerweise richtig.
- Sei nun $k \geq 0$ und die Behauptung bereits für k gezeigt, d.h.
$$f(a+t, \sum_{i=0}^{k} b_i t^i) \equiv 0 \bmod t^{k+1}.$$
Wir können dann schreiben
$$f(a+t, \sum_{i=0}^{k} b_i t^i) = t^{k+1}(c_{k+1} + tg(t)).$$
Es folgt mit $z = b_{k+1}t^{k+1}$, wobei wir modulo t^{k+2} rechnen wollen:

$$\begin{aligned}
f(a+t, \sum_{i=0}^{k+1} b_i t^i) &= f(a+t, \sum_{i=0}^{k} b_i t^i + b_{k+1}t^{k+1}) = \\
&= f(a+t, \sum_{i=0}^{k} b_i t^i) + \frac{\partial f}{\partial y}(a+t, \sum_{i=0}^{k} b_i t^i)\cdot b_{k+1}t^{k+1} + t^{k+1+k+1}\cdot(\dots) = \\
&= t^{k+1}(c_{k+1} + \dots) + \frac{\partial f}{\partial y}(a+t, \sum_{i=0}^{k} b_i t^i)\cdot b_{k+1}t^{k+1} + \dots \equiv \\
&\equiv \left(c_{k+1} + b_{k+1}\cdot\frac{\partial f}{\partial y}(a,b)\right)\cdot t^{k+1} \equiv 0 \bmod t^{k+2}.
\end{aligned}$$

Dies beweist die Behauptung durch Induktion.

(2) Für alle $n \geq 0$ gilt

$$f(a+t, \sum_{i=0}^{n} b_i t^i) \equiv 0 \bmod t^{n+1},$$

d.h.

$$\text{ord}\left(f(a+t, \sum_{i=0}^{n} b_i t^i\right) \geq n+1.$$

Dann folgt

$$\lim_{n\to\infty} f(a+t, \sum_{i=0}^{n} b_i t^i) = 0.$$

Die Stetigkeit von $f(x,y)$ impliziert dann

$$f(a+t, \sum_{i=0}^{\infty} b_i t^i) = 0.$$

Dies ist die Behauptung. ■

SATZ. *Sei C eine absolut irreduzible, nichtsinguläre, projektive Kurve und $P \in C(K)$. In einer affinen Umgebung von P werde C durch die Gleichung $f(x,y) = 0$ beschrieben mit $P = (a,b)$, sodass $\frac{\partial f}{\partial y}(a,b) \neq 0$ gilt. Dann ist $t = x - a$ uniformisierend in P. Bestimmt man mit dem vorangegangenen Lemma*

$$\sum_{i=0}^{\infty} b_i t^i \quad \textit{mit} \quad f(a+t, \sum_{i=0}^{\infty} b_i t^i) = 0 \textit{ in } K[[t]],$$

so definiert

$$x \mapsto a + t, \quad y \mapsto \sum_{i=0}^{\infty} b_i t^i$$

eine Einbettung

$$K(C) \hookrightarrow K((t)),$$

wobei für $g \in K(C)$ gilt $\operatorname{ord}_P(g) = \operatorname{ord}(g)$.

KAPITEL 8

Divisoren auf nichtsingulären Kurven

Im Folgenden sei C eine nichtsinguläre, absolut irreduzible, projektive Kurve, die über einem vollkommenen Körper K definiert ist.

DEFINITION. (1) *Die* **Divisorengruppe** $\mathrm{Div}(C)$ *von C ist die freie abelsche Gruppe, die von den Punkten auf C erzeugt wird. Ein* **Divisor** $D \in \mathrm{Div}(C)$ *ist also eine formale Linearkombination*

$$D = \sum_{P \in C} n_P [P]$$

mit $n_P \in \mathbb{Z}$ und $n_P \neq 0$ für nur endlich viele Punkte von C. (Dabei dient die Schreibweise $[P]$ nur dazu, eine Verwechslung mit anderen Objekten auszuschließen.)

(2) *Der* **Grad** $\mathrm{grad}(D)$ *eines Divisors $D = \sum n_P[P]$ ist* $\mathrm{grad}(D) = \sum n_P$.

(3) *Die Divisoren vom Grad 0 bilden eine Untergruppe:*

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \mathrm{grad}(D) = 0\}.$$

(4) *Die Galoisgruppe G_K operiert auf* $\mathrm{Div}(C)$ *und* $\mathrm{Div}^0(C)$ *durch*

$$\sigma(\sum n_P[P]) = \sum n_P[\sigma P].$$

(5) *Man sagt, $D \in \mathrm{Div}(C)$ ist über K definiert, falls $\sigma D = D$ für alle $\sigma \in G_K$ gilt. Sei* $\mathrm{Div}_K(C)$ *bzw.* $\mathrm{Div}^0_K(C)$ *die Gruppe der Divisoren bzw. Divisoren vom Grad 0, die über K definiert sind.*

(6) *Ist $f \in \overline{K}(C)^*$, so heißt*

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)[P]$$

der zu f gehörige Hauptdivisor. Manchmal schreibt man statt $\mathrm{div}(f)$ *auch einfach* (f).

Beispiel: Wir betrachten $\mathbb{P}^1$ mit x als Koordinate im Endlichen und $u = \frac{1}{x}$ im Unendlichen. Ein $f \in \overline{K}(\mathbb{P}^1), f \neq 0$ hat eine eindeutige Zerlegung

$$f = c\frac{(x-a_1)^{m_1} \dots (x-a_r)^{m_r}}{(x-b_1)^{n_1} \dots (x-b_s)^{n_s}},$$

mit $m_i, n_j \geq 1$, alle a_i, b_j verschieden. Im Unendlichen ist $\mathrm{ord}_\infty(f) = (\sum_j n_j) - (\sum_i m_i)$ und damit folgt

$$\mathrm{div}(f) = \sum_i m_i[a_i] - \sum_j n_j[b_j] + (\sum_j n_j - \sum_i m_i)[\infty].$$

Insbesondere sieht man hier auch sofort $\mathrm{grad}(\mathrm{div}(f)) = 0$.

Beispiel: Wir betrachten die Kurve $C \subseteq \mathbb{P}^2$, die durch $y = x^2$ gegeben wird. Dann ist

$$[(\sqrt{2}, 2)] + [(-\sqrt{2}, 2)]$$

ein über $\mathbb{Q}$ definierter Divisor. Ist $\alpha^3 = 2$ und $\zeta = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel, so ist

$$[(\alpha, \alpha^2)] + [(\zeta\alpha, \zeta^2\alpha^2)] + [(\zeta^2\alpha, \zeta\alpha^2)]$$

ebenfalls über $\mathbb{Q}$ definiert.

LEMMA. *Seien $f, g \in \overline{K}(C)^*$. Dann gilt:*

(1) $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$, *die Hauptdivisoren bilden also eine Untergruppe.*

Datei: algku8.tex. Version vom 18.7.2021

(2) $\operatorname{div}(f) = 0 \iff f \in \overline{K}^*$.
(3) $\operatorname{div}(f) = \operatorname{div}(g) \iff f = cg$ *für ein* $c \in \overline{K}$.
(4) $\operatorname{grad}(\operatorname{div}(f)) = 0$, *d.h. Hauptdivisoren haben Grad* 0.

Beweis:

(1) Dies folgt sofort aus $\operatorname{ord}_P(fg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g)$.
(2) $\operatorname{div}(f) = 0$ heißt, f hat weder Pol- noch Nullstellen. Da ein nichtkonstantes $f \in \overline{K}(C)$ aber einen surjektiven Morphismus $\phi : C \to \mathbb{P}^1$ mit $\phi = (1 : f)$ liefert, ist klar, dass $\operatorname{div}(f) = 0$ mit $f \in \overline{K}(C)$ äquivalent ist.
(3) Es gilt $\operatorname{div}(f) = \operatorname{div}(g)$ genau dann, wenn $0 = \operatorname{div}(f) - \operatorname{div}(g) = \operatorname{div}(\frac{f}{g})$, woraus mit der letzten Aussage die Behauptung folgt.
(4) Aus dem letzten Abschnitt wissen wir: $\sum_P \operatorname{ord}_P(f) = 0$, also $\operatorname{grad}(\operatorname{div}(f)) = 0$. ■

Beispiel: Seien $e_1, e_2, e_3 \in \overline{K}$ paarweise verschieden, $\operatorname{char}(K) \neq 2$. Dann definiert $y^2 = (x - e_1)(x - e_2)(x - e_3)$ eine nichtsinguläre Kurve $C \subseteq \mathbb{P}^2$ mit einem unendlich fernen Punkt $P_\infty = (0 : 0 : 1)$. Sei $P_i = (e_i, 0)$. In P_1 ist $x - e_1 = 0$ Tangente, also y uniformisierend, außerdem $(x - e_2)(x - e_3)$ Einheit. Daher

$$2 = \operatorname{ord}_{P_1}(y^2) = \operatorname{ord}_{P_1}((x - e_1)(x - e_2)(x - e_3)) = \operatorname{ord}_{P_1}(x - e_1).$$

Da $x - e_1$ höchstens in P_1 eine Nullstelle hat, höchstens in P_∞ eine Polstelle hat, folgt

$$\operatorname{div}(x - e_1) = 2[P_1] - 2[P_\infty].$$

Analog

$$\operatorname{div}(x - e_2) = 2[P_2] - 2[P_\infty] \quad \text{und} \quad \operatorname{div}(x - e_3) = 2[P_3] - 2[P_\infty].$$

Daraus ergibt sich $\operatorname{div}(y^2) = 2[P_1] + 2[P_2] + 2[P_3] - 6[P_\infty]$, also

$$\operatorname{div}(y) = [P_1] + [P_2] + [P_3] - 3[P_\infty].$$

Definition. *Zwei Divisoren* $D_1, D_2 \in \operatorname{Div}(C)$ *heißen* **linear äquivalent**, $D_1 \sim D_2$, *wenn es einen Hauptdivisor* $\operatorname{div}(f)$ *gibt mit*

$$D_2 = D_1 + \operatorname{div}(f).$$

Die **Picardgruppe** *oder* **Divisorenklassengruppe** $\operatorname{Pic}(C)$ *ist der Quotient von* $\operatorname{Div}(C)$ *modulo der Untergruppe der Hauptdivisoren. Entsprechend definiert man*

$$\operatorname{Pic}^0(C) = \{\textit{Divisoren vom Grad } 0\}/\{\textit{Hauptdivisoren }\}.$$

Sei weiter

$$\operatorname{Pic}_K(C) = \{c \in \operatorname{Pic}(C) : \sigma c = c \textit{ für alle } \sigma \in G_K\}$$

und analog $\operatorname{Pic}^0_K(C)$.

Bemerkungen:

(1) $\operatorname{Pic}^0(C) = 0$ heißt, dass jeder Divisor vom Grad 0 Hauptdivisor ist. $\operatorname{Pic}^0(C)$ misst also, wieweit Divisoren vom Grad 0 von Hauptdivisoren abweichen. Man vergleiche die Funktion der Klassengruppe von Zahlkörpern.
(2) Da Hauptdivisoren Grad 0 haben, erhalten wir durch die Gradfunktion eine induzierte Abbildung $\operatorname{grad} : \operatorname{Pic}(C) \to \mathbb{Z}$. Der Kern ist $\operatorname{Pic}^0(C)$. Man kann dies auch mit der exakten Sequenz schreiben:
$$0 \to \operatorname{Pic}^0(C) \to \operatorname{Pic}(C) \to \mathbb{Z} \to 0.$$
Ist $P_0 \in C$, so definiert $(D_0, n) \mapsto D_0 + nP_0$ einen Isomorphismus von abelschen Gruppen
$$\operatorname{Pic}^0(C) \oplus \mathbb{Z} \simeq \operatorname{Pic}(C),$$
der von der Auswahl des Punktes P_0 abhängt.

Der folgende Satz gibt einen ersten Hinweis, wie wichtig $\operatorname{Pic}(C)$ für die Klassifikation von Kurven ist:

Satz. *Für eine Kurve* C *sind äquivalent:*

(1) $C \simeq \mathbb{P}^1$ *(über* $\overline{K}$*).*
(2) $\mathrm{Pic}^0(C) = 0$.
(3) *Es gibt ein* $f \in \overline{K}(C)$ *mit* $\mathrm{div}(f) = [P_1] - [P_2]$ *und* $P_1 \neq P_2$.

Beweis:

- $1 \Rightarrow 2$: Jeder Divisor D auf $\mathbb{P}^1$ vom Grad 0 kann in der Form
$$D = \sum_i m_i[\alpha_i] - \sum_j n_j[\beta_j] + (\sum_j n_j - \sum_i m_i)[\infty]$$
mit $m_i, n_j \geq 0$ geschrieben werden. Offensichtlich gilt nun für
$$f = \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}}$$
$\mathrm{div}(f) = D$, also ist D Hauptdivisor und damit $\mathrm{Pic}^0(C) = 0$.
- $2 \Rightarrow 3$: Wähle zwei verschiedene Punkte $P_1, P_2 \in C$. Dann hat der Divisor $[P_1] - [P_2]$ Grad 0, also gibt es eine Funktion f mit $\mathrm{div}(f) = [P_1] - [P_2]$.
- $3 \Rightarrow 1$: f induziert einen Morphismus $\phi : C \to \mathbb{P}^1$ mit $\phi = (1 : f)$ vom Grad
$$\mathrm{grad}(\phi) = \sum_{\substack{P \in C \\ f(P)=0}} \mathrm{ord}_P(f) = 1,$$
also ist ϕ ein Isomorphismus. (Alternativ: Es ist $\overline{K}(C) = \overline{K}(f) \simeq \overline{K}(\mathbb{P}^1)$ und damit $C \simeq \mathbb{P}^1$.) ■

Wir wollen jetzt wichtige Beispiele von Divisoren kennenlernen.

Hyperebenenschnitte: Sei $C \subseteq \mathbb{P}^n$ und C nicht in einem echten linearen Teilraum von $\mathbb{P}^n$ enthalten. Sei $\ell = a_0x_0 + \dots + a_nx_n = 0$ die Gleichung einer Hyperebene. Wir wollen den Divisor $\mathrm{div}(\ell)$ definieren, den Hyperebenenschnitt $\{\ell = 0\} \cap C$.
Sei $P \in C$. Ist $P \in U_i = \{x_i \neq 0\}$, so sei $n_P = \mathrm{ord}_P(\frac{\ell}{x_i})$. Ist P auch in U_j, so ist wegen $\mathrm{ord}_P(\frac{x_i}{x_j}) = 0$

$$\mathrm{ord}_P(\frac{\ell}{x_i}) = \mathrm{ord}_P(\frac{\ell}{x_i}) + \mathrm{ord}_P(\frac{x_i}{x_j}) = \mathrm{ord}_P(\frac{\ell}{x_j}),$$

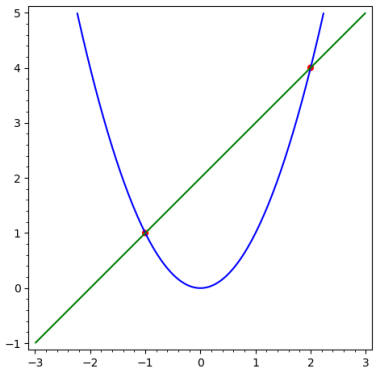
d.h. n_P ist wohldefiniert. Nun setzt man

$$\mathrm{div}(\ell) = \sum_{P \in C} n_P[P].$$

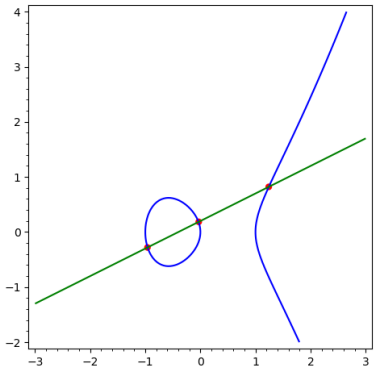
Ist $\ell' = 0$ eine andere Hyperebene, so ist $\frac{\ell}{\ell'}$ eine rationale Funktion auf C, und man sieht sofort, dass die Hyperebenenschnitte $\mathrm{div}(\ell)$ und $\mathrm{div}(\ell')$ linear äquivalent sind. Man nennt $\mathrm{grad}(\mathrm{div}(\ell))$ den **Grad der Kurve** C **im** $\mathbb{P}^n$.

Beispiele:

(1) Sei $C = \{x_0x_2 = x_1^2\} \subseteq \mathbb{P}^2$. Je zwei Punkte auf C bilden einen Hyperebenenschnitt.



(2) Für die Kurve C in affiner Darstellung $y^2 = x^3 - x$ bestehen die Hyperebenenschnitte aus 3 Punkten, die auf einer Geraden liegen.



Sei nun $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus glatter projektiver Kurven. Wir definieren

$$\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1), \quad [Q] \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)[P] \text{ und lineare Fortsetzung,}$$

$$\phi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2), \quad [P] \mapsto [\phi(P)] \text{ und lineare Fortsetzung.}$$

Beispiel: Interpretieren wir eine nichtkonstante Funktion $f \in \overline{K}(C)$ als $f : C \to \mathbb{P}^1$, so gilt

$$\mathrm{div}(f) = f^*([0] - [\infty]).$$

Satz. *Sei $\phi : C_1 \to C_2$ ein Morphismus glatter projektiver Kurven. Dann gilt*

(1) $\mathrm{grad}(\phi^* D) = \mathrm{grad}\phi \cdot \mathrm{grad}(D)$.
(2) $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$.
(3) $\mathrm{grad}(\phi_* D) = \mathrm{grad}(D)$.
(4) $\phi_* \circ \phi^* = \mathrm{grad}(\phi)$, *d.h. Multiplikation mit* $\mathrm{grad}(\phi)$ *auf* $\mathrm{Div}(C_2)$.

Der Beweis ergibt sich unmittelbar aus den Definitionen und früher erwähnten Eigenschaften.

KAPITEL 9

Differentialformen auf nichtsingulären Kurven

Sei wieder C eine nichtsinguläre, absolut irreduzible, projektive Kurve, die über einem vollkommenen Körper K definiert ist.

1. Rechnen mit Differentialformen

DEFINITION. *Der Raum Ω_C der meromorphen Differentialformen auf C ist der $\overline{K}(C)$-Vektorraum, der von Symbolen df mit $f \in \overline{K}(C)$ erzeugt wird, zusammen mit den Relationen*

$$d(f+g) = df + dg, \quad d(fg) = fdg + gdf, \quad dc = 0 \text{ für alle } c \in \overline{K}.$$

Jedes $\omega \in \Omega_C$ hat also eine Darstellung

$$\omega = \sum_{i=1}^{n} f_i dg_i \text{ mit } f_i g_i \in \overline{K}(C).$$

Wir üben etwas den Umgang mit den Differentialen: Seien $f, g \in \overline{K}(C)$.

- $d(f^2) = fdf + fdf = 2fdf$ und induktiv dann
$$d(f^n) = nf^{n-1}df \text{ für alle natürlichen Zahlen } n.$$
- Ist $f \neq 0$, so gilt:
$$0 = d(1) = d(f \cdot \frac{1}{f}) = fd(\frac{1}{f}) + \frac{1}{f}df,$$
woraus sofort
$$d(\frac{1}{f}) = -\frac{1}{f^2}df$$
folgt. Wie üblich erhält man dann
$$d(\frac{f}{g}) = \frac{gdf - fdg}{g^2}.$$
- Ist $F = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ein Polynom mit $a_i \in \overline{K}$, so können wir die formale Ableitung $F' = \sum i a_i x^{i-1}$ bilden. Setzt man f ein, so erhält man
$$dF(f) = d(\sum a_i f^i) = \sum i a_i f^{i-1} df = F'(f)df.$$
Ist G ein weiteres Polynom mit $G(f) \neq 0$, so ist
$$d(\frac{F(f)}{G(f)}) = \frac{F'(f)G(f) - F(f)G'(f)}{G(f)^2}df.$$

Beispiel: Wegen $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$ folgt aus den obigen Betrachtungen sofort, dass jedes $\omega \in \Omega_{\mathbb{P}^1}$ die Form
$$\omega = \frac{p(x)}{q(x)}dx$$
hat, mit Polynomen p und q.

SATZ. *Ω_C ist ein 1-dimensionaler $\overline{K}(C)$-Vektorraum.*

Beweisidee: Der Funktionenkörper $\overline{K}(C)$ kann erzeugt werden von Elementen x und y mit einer Relation $f(x,y)=0$. Wie oben überlegt man sich

$$\Omega_C = \overline{K}(C)dx + \overline{K}(C)dy.$$

Wir differenzieren jetzt die Relation $f(x,y)=0$:

$$0 = d0 = d(f(x,y)) = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy.$$

Ist $\frac{\partial f}{\partial y} \neq 0$, so folgt

$$dy = -\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}}dx,$$

und damit $\Omega_C = \overline{K}(C)dx$. Zu zeigen bliebe noch, dass $\Omega_C \neq 0$ gilt, worauf wir aber verzichten. ■

Bemerkung: Für $c \in \overline{K}$ gilt $dc = 0$. In Charakteristik p gilt außerdem $d(f^p) = 0$ für jede Funktion f.

Ohne Beweis geben wir folgenden Satz an, der die von uns benötigten Aussagen enthält:

SATZ. (1) *Ist* $\mathrm{char}(K) = 0$*, so gilt für* $f \in \overline{K}(C)$*:*

$$df = 0 \iff f \in \overline{K}.$$

(2) *Ist* $P \in C$ *und* t *uniformisierend in* P*, d.h.* $\mathrm{ord}_P(t) = 1$*, so ist* $dt \neq 0$*, insbesondere* $\Omega_C = \overline{K}(C)dt$*.*

Ist also t uniformisierend in $P \in C$ und $f \in \overline{K}(C)$, so gibt es eine Funktion $g \in \overline{K}(C)$ mit $df = gdt$. Wir schreiben dann auch manchmal $g = \frac{df}{dt}$. Ohne Beweis geben wir folgendes Lemma an:

LEMMA. *Ist* t *uniformisierend in* $P \in C$ *und* $f \in \overline{K}(C)$ *definiert in* P*, so ist* $\frac{df}{dt}$ *auch definiert in* P*.*

2. Kanonische Divisoren - das Geschlecht einer Kurve

DEFINITION. (1) *Ist* $\omega \in \Omega_C, \omega \neq 0$*,* $P \in C$ *und* t *uniformisierend in* P*, so gibt es eine Funktion* g *mit* $\omega = gdt$*. Man definiert*

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(g).$$

Man sagt, ω *ist holomorph oder regulär in* P*, falls* $\mathrm{ord}_P(\omega) \geq 0$ *ist.*

(2) *Der Divisor eines Differentials* $\omega \in \Omega_C$ *wird wie folgt definiert:*

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)[P].$$

Den Divisor eines Differentials nennt man auch einen **kanonischen Divisor***.*

Bemerkung: Man kann jetzt leicht zeigen, dass die Definition von $\mathrm{ord}_P(\omega)$ nicht von der Auswahl der Uniformisierenden in P abhängt.

Beispiel: $C = \mathbb{P}^1$ und $\omega = dx$. Was ist $\mathrm{div}(dx)$? Im Endlichen: In einem Punkt a ist $x-a$ uniformisierend, wegen $dx = d(x-a) = 1 \cdot d(x-a)$ gilt also $\mathrm{ord}_a(dx) = 0$. Im unendlich fernen Punkt ∞ ist $u = \frac{1}{x}$ uniformisierend, mit

$$dx = d(\frac{1}{u}) = -\frac{1}{u^2}du = (-1)u^{-2}du$$

gilt also $\mathrm{ord}_\infty(dx) = -2$, womit man schließlich erhält:

$$\mathrm{div}(dx) = -2[\infty] \quad \text{und} \quad \mathrm{grad}(\mathrm{div}(dx)) = -2.$$

LEMMA. *Für* $f \in \overline{K}(C) \setminus \{0\}$ *und* $\omega \in \Omega_C \setminus \{0\}$ *gilt*

$$\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega).$$

Beweis: Sei $P \in C$ und t uniformisierend in P. Dann gibt es eine Funktion g mit $\omega = g\,dt$. Mit $f\omega = fgdt$ folgt

$$\operatorname{ord}_P(f\omega) = \operatorname{ord}_P(fg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g) = \operatorname{ord}_P(f) + \operatorname{ord}_P(\omega).$$

Daraus ergibt sich

$$\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega),$$

wie behauptet. ■

SATZ. (1) *Je zwei kanonische Divisoren sind linear äquivalent.*

(2) *Ist ein Divisor linear äquivalent zu einem kanonischen Divisor, so ist er selbst ein kanonischer Divisor.*

Die kanonischen Divisoren bilden also eine ganze Äquivalenzklasse von Divisoren. Man nennt sie auch die **kanonische Klasse** *und schreibt dafür* k_C.

Beweis:

(1) Seien ω_1, ω_2 zwei von 0 verschiedene Differentialformen, so gibt es eine Funktion f mit $\omega_2 = f\omega_1$. Aus dem vorangegangenen Lemma folgt sofort

$$\operatorname{div}(\omega_2) = \operatorname{div}(f) + \operatorname{div}(\omega_1).$$

Also sind ω_1 und ω_2 linear äquivalent.

(2) Sei ein Divisor D linear äquivalent zu einem Divisor $\operatorname{div}(\omega)$ mit $\omega \in \Omega_C \setminus \{0\}$. Dann gibt es eine Funktion $f \neq 0$ mit $D = \operatorname{div}(f) + \operatorname{div}(\omega)$. Das vorangegangene Lemma impliziert $D = \operatorname{div}(f\omega)$, also ist D ein kanonischer Divisor, wie behauptet. ■

Beispiel: ($\operatorname{char}(K) \neq 2$) Wir betrachten die (nichtsinguläre) Kurve $C \subseteq \mathbb{P}^2$, die affin durch die Gleichung $y^2 = x^3 - x$ definiert wird, also $C = \{x_0x_2^2 = x_1^3 - x_0^2x_1\}$. Wir wollen den Divisor des Differentials $\omega = dx$ berechnen.

Im Endlichen: Sei $P_1 = (-1,0), P_2 = (0,0), P_3 = (1,0)$. Sei $P = (a,b) \in C$. Ist $P \neq P_i$, so ist $x - a$ uniformisierend, wegen $dx = d(x-a)$ also $\operatorname{ord}_P(\omega) = 0$. In P_i ist y uniformisierend. Wir differenzieren $y^2 = x^3 - x$ und erhalten

$$2ydy = (3x^2 - 1)dx \quad \text{und} \quad \omega = dx = \frac{2y}{3x^2-1}dy.$$

In P_i ist $3x^2 - 1$ Einheit, also gilt $v_{P_i}(\omega) = 1$.

Im Unendlichen: Es gibt nur den einen Punkt $P_\infty = (0:0:1)$. Wir wählen affine Koordinaten r, s mit $(r:s:1) = (x_0:x_1:x_2) = (1:x:y)$ und haben dann die Gleichung $r = s^3 - r^2s$. In P_∞ ist s uniformisierend und $\operatorname{ord}_{P_\infty}(r) = 3$. Zunächst gilt nun $\omega = dx = d(\frac{s}{r}) = \frac{1}{r}ds - \frac{s}{r^2}dr$. Durch Differenzieren der Gleichung $r = s^3 - r^2s$ erhält man $(1+2rs)dr = (3s^2 - r^2)ds$ und damit

$$\omega = dx = \frac{-2-4rs}{r(1+2rs)}ds,$$

woraus man sofort $\operatorname{ord}_{P_\infty}(\omega) = -3$ ablesen kann. Also gilt

$$\operatorname{div}(\omega) = [P_1] + [P_2] + [P_3] - 3[P_\infty].$$

Den gleichen Divisor hat die Funktion y: $\operatorname{div}(dx) = \operatorname{div}(y)$ und damit

$$\operatorname{div}(\frac{1}{y}dx) = 0.$$

Die kanonische Klasse ist also trivial: $k_C = 0$.

Zur Übung rechne man in gleicher Weise folgendes Beispiel:

Beispiel: ($\operatorname{char}(K) \neq 2$) Seien $e_1, e_2, e_3 \in \overline{K}$ paarweise verschieden und $C \subseteq \mathbb{P}^2$ gegeben durch die affine Gleichung $y^2 = (x-e_1)(x-e_2)(x-e_3)$. Man zeigt, dass C nichtsingulär und absolut irreduzibel ist. Mit $A = e_1 + e_2 + e_3$, $B = e_1e_2 + e_1e_3 + e_2e_3$ und $C = e_1e_2e_3$ können wir auch $y^2 = x^3 - Ax^2 + Bx - C$ schreiben bzw. projektiv $x_0x_2^2 = x_1^3 - Ax_0x_1^2 + Bx_0^2x_1 - Cx_0^3$. Wir wollen den kanonischen Divisor $\operatorname{div}(dx)$ berechnen. Sei $P_i = (e_i, 0)$ und $P_\infty = (0:0:1)$.

Im Endlichen: Ist $P = (a, b) \neq P_i$, so ist $x - a$ uniformisierend, wegen $dx = d(x - a)$ also $\operatorname{ord}_P(dx) = 0$. In P_i ist y uniformisierend. Wir differenzieren die Definitionsgleichung $y^2 = x^3 - Ax^2 + Bx - C$:

$$2ydy = (3x^2 - 2Ax + B)dx.$$

In P_i ist $(3x^2 - 2Ax + B)(P_i) = (e_i - e_j)(e_i - e_k) \neq 0$ (i, j, k paarweise verschieden), $3x^2 - 2Ax + B$ also Einheit und damit $\operatorname{ord}_{P_i}(dx) = 1$.
Im Unendlichen: Wir verwenden affine Koordinaten r, s mit $(r : s : 1) = (1 : x : y)$, also $x = \frac{s}{r}, y = \frac{1}{r}$. Die Gleichung lautet $r = s^3 - Ars^2 + Br^2s - Cr^3$. Die Tangente in P_∞ ist also $r = 0$, mithin s uniformisierend. Aus der Gleichung sieht man dann sofort $\operatorname{ord}_\infty(r) = 3$. Durch Differenzieren der Gleichung erhält man

$$(1 + 3Cr^2 - 2Brs + As^2)dr = (Br^2 - 2Ars + 3s^2)ds,$$

und daher mit $dx = d(\frac{s}{r}) = \frac{1}{r}ds - \frac{s}{r^2}dr$

$$dx = \frac{3Ars^2 - 3Br^2s + 3Cr^3 + r - 3s^3}{r^2(As^2 - 2Brs + 3Cr^2 + 1)}ds.$$

Nun gilt $\operatorname{ord}_\infty(r - 3s^3) = 3$, so dass sich $\operatorname{ord}_\infty(dx) = -3$ ergibt.
Insgesamt haben wir also

$$\operatorname{div}(dx) = [P_1] + [P_2] + [P_3] - 3[P_\infty].$$

Diesen Divisor kennen wir bereits: $\operatorname{div}(dx) = \operatorname{div}(y)$ und damit $\operatorname{div}(\frac{dx}{y}) = 0$. Die Differentialform $\frac{dx}{y}$ hat also weder Pol- noch Nullstellen. Außerdem gilt $k_C = 0$.

Die folgende Definition führt eine zentrale Invariante ein:

DEFINITION. *Das* **Geschlecht** *g (oder $g(C)$ oder g_C) einer Kurve C wird definiert durch die Formel*

$$2g - 2 = \operatorname{grad}(k_C),$$

wo k_C die kanonische Klasse bezeichnet.

Bemerkung: Da wir noch keine Aussagen über die Grade von kanonischen Divisoren haben, wissen wir bisher nur, dass für das Geschlecht einer Kurve

$$g(C) \in \frac{1}{2}\mathbb{Z}$$

gilt.

Beispiele:

(1) Wegen $\operatorname{grad}(k_{\mathbb{P}^1}) = -2$ hat $\mathbb{P}^1$ Geschlecht 0.
(2) Die vorhin betrachteten Kurven $y^2 = (x - e_1)(x - e_2)(x - e_3)$ (alle e_i's verschieden) haben $k_C = 0$, also Geschlecht 1.

3. Die Adjunktionsformel für ebene Kurven

Adjunktionsformel für glatte ebene Kurven:

- Sei $C \subseteq \mathbb{P}^2$ eine nichtsinguläre Kurve vom Grad d, d.h. gegeben durch ein Polynom $f(x, y) = 0$ bzw. homogen $x_0^d f(\frac{x_1}{x_0}, \frac{x_2}{x_0}) = 0$.
- Im Funktionenkörper gilt $f(x, y) = 0$, woraus folgt $\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy = 0$ und daher

$$\omega = \frac{dx}{\frac{\partial f}{\partial y}} = -\frac{dy}{\frac{\partial f}{\partial x}}.$$

- Wir betrachten ω im Endlichen, in einem Punkt $P = (a, b)$.
  Ist $\frac{\partial f}{\partial y}(P) \neq 0$, so ist $x - a$ uniformisierend und mit $d(x - a) = dx$ folgt $\operatorname{ord}_P(\omega) = 0$.
  Ist $\frac{\partial f}{\partial x}(P) \neq 0$, so ist $y - b$ uniformisierend und mit $d(y - b) = dy$ ergibt sich $\operatorname{ord}_P(\omega) = 0$.

- Im Unendlichen: Wir nehmen an, $(0:1:0)$ liegt nicht auf der Kurve, dann liegen alle unendlich fernen Punkte von C im affinen Teil $\{(r:s:1)\}$ und zwar auf $r=0$. Wegen $(1:x:y)=(r:s:1)=(1:\frac{s}{r}:\frac{1}{r})$ gilt im Funktionenkörper $x=\frac{s}{r}$ und $y=\frac{1}{r}$. Die Ableitung $\frac{\partial f}{\partial x}$ hat Grad $d-1$, also ist $g(r,s)=r^{d-1}\frac{\partial f}{\partial x}(\frac{s}{r},\frac{1}{r})$ ein Polynom in r und s. Mit $dy=d(\frac{1}{r})=-\frac{1}{r^2}dr$ erhalten wir
$$\omega=-\frac{dy}{\frac{\partial f}{\partial x}}=\frac{r^{d-3}dr}{g(r,s)}.$$
- Nun kann man erreichen, dass der Geradenschnitt (x_0) aus d verschiedenen Punkten besteht:
$$\mathrm{div}(x_0)=[P_1]+\cdots+[P_d].$$
Dann ist r uniformisierend in P_i und $\mathrm{ord}_{P_i}(\omega)=d-3$.
- Man erhält also
$$\mathrm{div}(\omega)=(d-3)[P_1]+\cdots+(d-3)[P_d]=(d-3)\mathrm{div}(x_0).$$
Insbesondere ist $\mathrm{grad}(k_C)=d(d-3)$.
- Aufgabe: Verifiziere die fürs Unendliche gemachten Aussagen durch explizites Ausrechnen.

Damit erhalten wir folgenden Satz:

SATZ. *Sei $C\subseteq\mathbb{P}^2$ eine nichtsinguläre Kurve vom Grad d. Ist h die Klasse eines Hyperebenenschnitts, so gilt für die kanonische Klasse*
$$k_C=(d-3)h,$$
also $\mathrm{grad}(k_C)=d(d-3)$ *und damit* $g(C)=\frac{(d-1)(d-2)}{2}$.

Beispiele: Ist C eine nichtsinguläre, absolut irreduzible, projektive, ebene Kurve vom Grad d, so gibt folgende Tabelle (im Fall $d\leq 6$) an, welches Geschlecht g die Kurve hat:

d	1	2	3	4	5	6
g	0	0	1	3	6	10

Was passiert, wenn eine ebene Kurve C Singularitäten hat? Durch Aufblasen erhalten wir eine nichtsinguläre birational äquivalente Kurve $\widetilde{C}$. Welches Geschlecht hat $\widetilde{C}$? Natürlich kann man dies bei einer konkret gegebenen Kurve ausrechnen, indem man den Divisor eines Differentials bestimmt. In vielen Fällen kann man aber auch obige Betrachtung modifizieren und erhält eine Aussage über das Geschlecht.

DEFINITION. *Ein Punkt $P=(x_0,y_0)$ einer ebenen Kurve $f(x,y)=0$ heißt einfacher Knoten oder gewöhnlicher Doppelpunkt, falls die Taylorreihenentwicklung in P folgende Gestalt hat:*
$$f=a(x-x_0)^2+b(x-x_0)(y-y_0)+c(y-y_0)^2+\ldots \qquad \text{mit } b^2-4ac\neq 0.$$

Nach Koordinatenwechsel sieht also die Taylorreihenentwicklung in einem einfachen Knoten wie folgt aus:
$$f=xy+\ldots$$

Damit gilt jetzt folgender Satz:

SATZ. *Sei $C\subseteq\mathbb{P}^2$ eine irreduzible projektive Kurve vom Grad d mit nur einfachen Knoten als Singularitäten, und zwar δ Stück. Ist $\widetilde{C}$ eine glattes Modell von C, so gilt*
$$g(\widetilde{C})=\frac{(d-1)(d-2)}{2}-\delta.$$

Beweisskizze: Wir können annehmen, dass alle Singularitäten im Endlichen liegen. $\widetilde{C}$ werde durch Aufblasung in den Singularitäten erhalten. Wir betrachten wieder das Differential

$$\omega = \frac{dx}{\frac{\partial f}{\partial y}} = -\frac{dy}{\frac{\partial f}{\partial x}}.$$

Wir müssen nur sehen, was in den singulären Punkten passiert. O.E. sei $P = (0,0)$ ein einfacher Knoten von C.

- Sei $f = xy + \sum_{i\geq 3} g_i(x,y)$, wo $g_i(x,y)$ homogen vom Grad i ist.
- Wir blasen $\mathbb{A}^2$ auf in $(0,0)$ und erhalten $X = \{((x,y),(z_0 : z_1)) \in \mathbb{A}^2 \times \mathbb{P}^1 : xz_1 = yz_0\}$. Die exzeptionelle Faser sei E, das eigentliche Urbild von C sei $\widetilde{C}$. Uns interessiert also, was in den Punkten $E \cap \widetilde{C}$ von $\widetilde{C}$ passiert. Dazu betrachten wir zwei affine Teile von X:
- $z_0 \neq 0$: Mit $z = \frac{z_1}{z_0}$ wird $y = xz$, als affine Koordinaten verwenden wir x, z. Einsetzen liefert

  $$f = x^2 z + \sum_{i\geq 3} g_i(x, xz) = x^2 z + \sum_{i\geq 3} x^i g_i(1, z),$$

  so dass hier das eigentliche Urbild $\widetilde{C}$ gegeben wird durch

  $$z + \sum_{i\geq 3} x^{i-2} g_i(1,z) = 0.$$

  $E \cap \widetilde{C} \cap \{z_0 \neq 0\}$ besteht nur aus dem Punkt $P_1 = ((0,0),(1:0))$.
- Der Punkt P_1 ist nichtsingulär auf $\widetilde{C}$ und x ist uniformisierend. Was passiert mit $\omega = dx/\frac{\partial f}{\partial y}$? Wir haben

  $$\frac{\partial f}{\partial y} = x + \sum_{i\geq 3} \frac{\partial g_i}{\partial y}(x,y) = x + \sum_{i\geq 3} \frac{\partial g_i}{\partial y}(x, xz),$$

  woraus sofort $\operatorname{ord}_{P_1}(\frac{\partial f}{\partial y}) = 1$ folgt, also

  $$\operatorname{ord}_{P_1}(\omega) = -1.$$
- Im affinen Teil $z_1 \neq 0$ findet man den Punkt $P_2 = ((0,0),(0:1))$ und analog $\operatorname{ord}_{P_2}(\omega) = -1$.
- Die Singularität erniedrigt also den Grad des kanonischen Divisors um 2, das Geschlecht erniedrigt sich also um 1, was wir zeigen wollten. ■

4. Die Riemann-Hurwitz-Formel

DEFINITION. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen glatten projektiven Kurven. Dann definieren wir*

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1} \text{ durch } \phi^*(\sum f_i dg_i) = \sum (\phi^* f_i) d(\phi^* g_i).$$

Da Ω_C ein 1-dimensionaler $\overline{K}(C)$-Vektorraum ist, ist $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ entweder injektiv oder identisch 0. Der folgende Satz gibt die wesentliche Charakterisierung.

SATZ. *$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ ist genau dann injektiv, wenn $\phi : C_1 \to C_2$ separabel ist.*

Wir werden diesen Satz nicht beweisen, geben aber ein Beispiel für das wesentliche Phänomen:

Beispiel: Hat K Charakteristik p und ist $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ gegeben durch $x \mapsto x^p$ oder $\phi = (1 : x^p)$, so gilt für das Differential $\omega = f(x)dx$:

$$\phi^*\omega = f(x^p)d(x^p) = f(x^p)px^{p-1}dx = 0,$$

also ist $\phi^* : \Omega_{\mathbb{P}^1} \to \Omega_{\mathbb{P}^1}$ in diesem Fall die 0-Abbildung.

Riemann-Hurwitz-Formel: Sei $\phi : C_1 \to C_2$ ein separabler Morphismus und ω eine Differentialform auf C_2. Wir wollen die Divisoren

$$\operatorname{div}(\phi^*\omega) \text{ und } \phi^*(\operatorname{div}(\omega))$$

vergleichen.

- Sei $P \in C_1$ und $Q = \phi(P)$. Sei s uniformisierend in Q, also $\omega = us^m ds$ mit $m = \operatorname{ord}_Q(\omega)$ und einer Einheit u.
- Sei t uniformisierend in P, $e = e_\phi(P)$ der Verzweigungsindex, also $\phi^*(s) = vt^e$ mit einer Einheit v. Dann gibt es auch eine in P definierte Funktion g mit $dv = gdt$.
- Wir betrachten $\phi^*\omega$ in P:

$$\begin{aligned}\phi^*\omega &= \phi^*(us^m)d(\phi^*s) = \phi^*u \cdot v^m \cdot t^{em} \cdot d(vt^e) = \\ &= \phi^*u \cdot v^m \cdot t^{em} \cdot (t^e dv + vd(t^e)) = \phi^*u \cdot v^m \cdot t^{em} \cdot (t^e gdt + evt^{e-1}dt) = \\ &= \phi^*u \cdot v^m \cdot t^{em} \cdot (t^e g + evt^{e-1})dt\end{aligned}$$

  Wir haben jetzt zwei Fälle:
  1. Fall: $e \neq 0$ in K: Dann gilt

$$\operatorname{ord}_P(\phi^*\omega) = me + e - 1 = e_\phi(P)\operatorname{ord}_Q(\omega) + (e_\phi(P) - 1).$$

  2. Fall: $e = 0$ in K: Dann ist

$$\operatorname{ord}_P(\phi^*\omega) > e_\phi(P)\operatorname{ord}_Q(\omega) + (e_\phi(P) - 1).$$

- Seien jetzt alle Verzweigungsindizes $e_\phi(P) \neq 0$ in K. Dann gilt also

$$\operatorname{ord}_P(\phi^*\omega) = e_\phi(P)\operatorname{ord}_{\phi(P)}(\omega) + (e_\phi(P) - 1),$$

  und damit

$$\begin{aligned}\operatorname{div}(\phi^*\omega) &= \sum_{P\in C_1} \operatorname{ord}_P(\phi^*\omega)[P] = \\ &= \sum_{P\in C_1} \big(e_\phi(P)\operatorname{ord}_{\phi(P)}(\omega)[P] + (e_\phi(P) - 1)[P]\big) = \\ &= \sum_{Q\in C_2} \sum_{P\in\phi^{-1}(Q)} e_\phi(P)\operatorname{ord}_Q(\omega)[P] + \sum_{P\in C_1} (e_\phi(P) - 1)[P] = \\ &= \sum_{Q\in C_2} \operatorname{ord}_Q(\omega) \left(\sum_{P\in\phi^{-1}(Q)} e_\phi(P)[P] \right) + \sum_{P\in C_1} (e_\phi(P) - 1)[P] = \\ &= \sum_{Q\in C_2} \operatorname{ord}_Q(\omega)\phi^*[Q] + \sum_{P\in C_1} (e_\phi(P) - 1)[P] = \\ &= \phi^*\Big(\sum_{Q\in C_2} \operatorname{ord}_Q(\omega)[Q]\Big) + \sum_{P\in C_1} (e_\phi(P) - 1)[P] = \\ &= \phi^*(\operatorname{div}(\omega)) + \sum_{P\in C_1} (e_\phi(P) - 1)[P].\end{aligned}$$

- In der letzten Formel berechnen wir noch die Grade und erhalten

$$2g(C_1) - 2 = \operatorname{grad}(\phi) \cdot (2g(C_2) - 2) + \sum_{P\in C_1} (e_\phi(P) - 1).$$

Damit erhalten wir folgenden Satz, der auch als **Riemann-Hurwitz-Formel** bezeichnet wird:

Satz (Riemann-Hurwitz). *Sei $\phi : C_1 \to C_2$ separabler Morphismus und alle Verzweigungsindizes $e_\phi(P) \neq 0$ in K. Ist ω ein von 0 verschiedenes Differential in C_2, so gilt*

$$\operatorname{div}(\phi^*\omega) = \phi^*(\operatorname{div}(\omega)) + \sum_{P\in C_1} (e_\phi(P) - 1)[P],$$

woraus sich für die Geschlechter der Kurven ergibt:

$$2g(C_1) - 2 = \operatorname{grad}(\phi)(2g(C_2) - 2) + \sum_{P\in C_1} (e_\phi(P) - 1).$$

Der Divisor $\sum_{P\in C_1}(e(_\phi(P) - 1)[P]$ heißt auch der **Verzweigungsdivisor von** ϕ.

KAPITEL 10

Der Satz von Riemann-Roch

Sei im Folgenden C eine nichtsinguläre, absolut irreduzible, projektive Kurve, die über einem vollkommenen Körper K definiert ist.

DEFINITION. *Für zwei Divisoren $D_1 = \sum m_P[P]$ und $D_2 = \sum n_P[P]$ auf C definiert man:*

$$D_1 \geq D_2 \quad \Longleftrightarrow \quad m_P \geq n_P \text{ für alle } P \in C.$$

Ein Divisor $D = \sum n_P[P] \in \mathrm{Div}(C)$ heißt **effektiv**, *falls $D \geq 0$ gilt, d.h. $n_P \geq 0$ für alle $P \in C$.*

Bemerkung: Für $D_1, D_2 \in \mathrm{Div}(C)$ gilt die Implikation

$$D_1 \geq D_2 \quad \Longrightarrow \quad \mathrm{grad}(D_1) \geq \mathrm{grad}(D_2).$$

Beispiel: Wie kann man ausdrücken, dass eine Funktion $f \in \overline{K}(C)^*$ höchstens in P_0 eine Polstelle hat, und zwar höchstens von der Ordnung n?
Die Bedingungen lauten: $\mathrm{ord}_{P_0}(f) \geq -n$ und $\mathrm{ord}_P(f) \geq 0$ für alle $P \neq P_0$. Dies ist offensichtlich gleichwertig mit $\mathrm{div}(f) = \sum \mathrm{ord}_P(f)P \geq -n[P_0]$, was man auch in der Form

$$\mathrm{div}(f) + n[P_0] \geq 0$$

schreiben kann.

DEFINITION. *Für $D \in \mathrm{Div}(C)$ sei*

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

Bemerkung: Sei $D = m_1[P_1] + \cdots + m_r[P_r] - n_1[Q_1] - \cdots - n_s[Q_s]$ mit paarweise verschiedenen Punkten $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ und $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbb{N}$. Für $f \in \overline{K}(C)^*$ gilt dann:

$$\begin{aligned}
f \in \mathcal{L}(D) \quad &\Longleftrightarrow \quad \mathrm{div}(f) + D \geq 0 \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \mathrm{div}(f) + m_1[P_1] + \cdots + m_r[P_r] - n_1[Q_1] - \cdots - n_s[Q_s] \geq 0 \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \mathrm{div}(f) \geq -m_1[P_1] - \cdots - m_r[P_r] + n_1[Q_1] + \cdots + n_s[Q_s] \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad \mathrm{ord}_{P_i}(f) \geq -m_i \text{ für } i = 1, \ldots, r, \quad \mathrm{ord}_{Q_j}(f) \geq n_j \text{ für } j = 1, \ldots, s \\
&\qquad\quad \text{und } \mathrm{ord}_P(f) \geq 0 \text{ für } P \in C \setminus \{P_1, \ldots, P_r, Q_1, \ldots, Q_s\}.
\end{aligned}$$

Zu $\mathcal{L}(D)$ gehören also die Funktionen, die in den Punkten P_i höchstens einen Pol der Ordnung m_i und in den Punkten Q_j mindestens eine Nullstelle der Ordnung n_j haben und in allen anderen Punkten definiert sind.

Beispiel: Was ist $\mathcal{L}(0)$, wo 0 hier den Nulldivisor bezeichnet? Ist $f \in \mathcal{L}(0) \setminus \{0\}$, so gilt $\mathrm{div}(f) \geq 0$, also hat f keine Polstellen. Dann muss aber f schon konstant sein. Damit haben wir

$$\mathcal{L}(0) = \overline{K}.$$

LEMMA. *$\mathcal{L}(D)$ ist ein $\overline{K}$-Vektorraum.*

Datei: algku10.tex. Version vom 18.7.2021

Beweis: Sei $D = \sum n_P[P]$, $f, g \in \mathcal{L}(D)$ und $c \in \overline{K}$. Wir wollen zeigen, dass gilt

$$f + g \in \mathcal{L}(D) \quad \text{und} \quad cf \in \mathcal{L}(D).$$

O.E. können wir uns auf den Fall $f \neq 0$, $g \neq 0$, $f+g \neq 0$, $c \neq 0$ beschränken. Dann gilt $\operatorname{ord}_P(f), \operatorname{ord}_P(g) \geq -n_P$ und damit

$$\operatorname{ord}_P(f+g) \geq \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g)) \geq -n \text{ und } \operatorname{ord}_P(cf) = \operatorname{ord}_P(f) \geq -n,$$

also $f + g \in \mathcal{L}(D)$ und $cf \in \mathcal{L}(D)$. ■

DEFINITION. *Wir setzen* $\ell(D) = \dim_{\overline{K}} \mathcal{L}(D)$.

Eine fundamentale Aufgabe ist die Bestimmung von $\mathcal{L}(D)$ und die von $\ell(D)$.

Beispiel: Im Fall $\mathbb{P}^1$ haben wir die Vektorräume $\mathcal{L}(D)$ bereits bestimmt. Zur Wiederholung betrachten wir $D = n[\infty]$ mit $n \in \mathbb{N}_0$. Dann ist

$$\mathcal{L}(n \cdot [\infty])] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_0, \ldots, a_n \in \overline{K}\}.$$

$\mathcal{L}(n[\infty])$ ist also der Vektorraum der Polynome vom Grad $\leq n$. Eine Basis ist $1, x, x^2, \ldots, x^n$, sodass insbesondere

$$\ell(n \cdot [\infty]) = n + 1 = \operatorname{grad}(n \cdot [\infty]) + 1$$

gilt.

SATZ. *Seien D und D' Divisoren auf C. Dann gilt:*

1. *Ist* $\operatorname{grad}(D) < 0$, *so ist* $\mathcal{L}(D) = 0$ *und* $\ell(D) = 0$.
2. *Sind D und D' linear äquivalent, so gilt* $\mathcal{L}(D) \simeq \mathcal{L}(D')$ *und insbesondere* $\ell(D) = \ell(D')$. *Genauer: Ist* $D' = D + \operatorname{div}(f)$, *so gilt* $\mathcal{L}(D') = \frac{1}{f}\mathcal{L}(D)$.
3. *Ist* $D \leq D'$, *so* $\mathcal{L}(D) \subseteq \mathcal{L}(D')$ *und* $\ell(D) \leq \ell(D')$.
4. *Sei* $P \in C$ *und* $D \in \operatorname{Div}(C)$. *Gilt* $\mathcal{L}(D) \subsetneq \mathcal{L}(D + [P])$ *und ist* $f \in \mathcal{L}(D + [P]) \setminus \mathcal{L}(D)$, *so gilt bereits* $\mathcal{L}(D + [P]) = \mathcal{L}(D) + \overline{K}f$.
5. *Ist* $P \in C$, *so gilt* $\ell(D) \leq \ell(D + [P]) \leq \ell(D) + 1$.
6. *Für* $\operatorname{grad}(D) \geq 0$ *gilt* $\ell(D) \leq \operatorname{grad}(D) + 1$.

Beweis:

(1) Wäre $\mathcal{L}(D) \neq 0$, so gäbe es ein $f \in \mathcal{L}(D) \setminus \{0\}$. Dann wäre $D + \operatorname{div}(f) \geq 0$, also würde

$$\operatorname{grad}(D) = \operatorname{grad}(D) + \operatorname{grad}(\operatorname{div}(f)) = \operatorname{grad}(D + \operatorname{div}(f)) \geq 0$$

folgen, ein Widerspruch zur Voraussetzung.

(2) Sei $D' = D + \operatorname{div}(f)$. Dann gilt für $g \in \overline{K}(C)^*$:

$$\begin{aligned} g \in \mathcal{L}(D') &\iff D' + \operatorname{div}(g) \geq 0 \iff D + \operatorname{div}(f) + \operatorname{div}(g) \geq 0 \iff \\ &\iff D + \operatorname{div}(fg) \geq 0 \iff fg \in \mathcal{L}(D) \iff g \in \frac{1}{f}\mathcal{L}(D), \end{aligned}$$

also $\mathcal{L}(D') = \frac{1}{f}\mathcal{L}(D)$, woraus die Behauptung folgt.

(3) Sei $D \leq D'$ und $f \in \mathcal{L}(D) \setminus \{0\}$. Dann gilt $D' + \operatorname{div}(f) \geq D + \operatorname{div}(f) \geq 0$, also $f \in \mathcal{L}(D')$. D.h. $\mathcal{L}(D) \subseteq \mathcal{L}(D')$.

(4) Wir nehmen an, es existiert eine Funktion f mit $f \in \mathcal{L}(D+[P]) \setminus \mathcal{L}(D)$. Sei $D = n[P] + \ldots$, d.h. n ist die Multiplizität von D in P. Sei t uniformisierend in P. Dann ist $\operatorname{ord}_P(f) \geq -(n+1)$, aber $\operatorname{ord}_P(f) \not\geq -n$, und daher $\operatorname{ord}_P(f) = -(n+1)$. Dann ist $\operatorname{ord}_P(ft^{n+1}) = 0$, also $(ft^{n+1})(P) \neq 0$. Ist jetzt $g \in \mathcal{L}(D+[P])$, so gilt $\operatorname{ord}_P(gt^{n+1}) \geq 0$, also gibt es eine Konstante c mit $(gt^{n+1})(P) = c(ft^{n+1})(P)$, was $\operatorname{ord}_P(gt^{n+1} - cft^{n+1}) \geq 1$ und somit $\operatorname{ord}_P(g - cf) \geq -n$ liefert. Also gilt $g - cf \in \mathcal{L}(D)$ und damit $g \in \mathcal{L}(D) + \overline{K}f$ wie behauptet.

(5) Dies folgt sofort aus der letzten Aussage.

(6) Wir können $\mathrm{grad}(D) \geq 0$ und $\mathcal{L}(D) \neq 0$ voraussetzen. Dann gibt es ein f mit $D + \mathrm{div}(f) \geq 0$. Also ist $D' = D + \mathrm{div}(f)$ effektiv und $\ell(D') = \ell(D)$. Wir können uns also auf effektive Divisoren beschränken: $D' = [P_1] + \cdots + [P_n]$. Mit Hilfe der letzten Aussage ergibt sich

$$\ell([P_1] + \cdots + [P_n]) \leq \ell([P_1] + \cdots + [P_{n-1}]) + 1 \leq \cdots \leq \ell(0) + n = n + 1,$$

was zu zeigen war. ■

Beispiel: Wir betrachten $C = \mathbb{P}^1$ und einen Divisor

$$D = \sum_{\alpha \in \overline{K}} n_\alpha [\alpha] + n_\infty [\infty] \quad \text{mit} \quad \mathrm{grad}(D) \geq 0,$$

wobei natürlich $\{\alpha \in \overline{K} : n_\alpha \neq 0\}$ endlich sein soll. Für die Funktion

$$f = \prod_{\alpha \in \overline{K}} (x - \alpha)^{n_\alpha}$$

gilt dann

$$\mathrm{div}(f) = \sum_{\alpha \in \overline{K}} n_\alpha [\alpha] - (\sum_{\alpha \in \overline{K}} n_\alpha)[\infty].$$

Mit der zweiten Formel des vorangegangenen Satzes folgt

$$\begin{aligned} \mathcal{L}(D) &= \mathcal{L}(\mathrm{div}(f) + ((\sum_{\alpha \in \overline{K}} n_\alpha) + n_\infty)[\infty]) = \mathcal{L}(\mathrm{div}(f) + \mathrm{grad}(D)[\infty]) = \\ &= \frac{1}{f} \mathcal{L}(\mathrm{grad}(D)[\infty]) = \\ &= \frac{1}{f} \left(\overline{K} + \overline{K} x + \overline{K} x^2 + \cdots + \overline{K} x^{\mathrm{grad}(D)} \right). \end{aligned}$$

Also ist

$$\frac{1}{f}, \quad \frac{x}{f}, \quad \frac{x^2}{f}, \quad \cdots \quad \frac{x^{\mathrm{grad}(D)}}{f}$$

eine Basis von $\mathcal{L}(D)$, und insbesondere $\ell(D) = \mathrm{grad}(D) + 1$.
Ohne Beweis geben wir jetzt folgenden fundamentalen Satz an:

Satz (Riemann-Roch). *Ist C eine Kurve vom Geschlecht g und K_C ein kanonischer Divisor, so gilt für alle Divisoren $D \in \mathrm{Div}(C)$:*

$$\ell(D) = \mathrm{grad}(D) + 1 - g + \ell(K_C - D).$$

Beispiel: Im Fall $C = \mathbb{P}^1$ war $g = 0$ und $K_C = \mathrm{div}(dx) = -2[\infty]$ ein kanonischer Divisor. Der Satz von Riemann-Roch besagt dann

$$\ell(D) = \mathrm{grad}(D) + 1 + \ell(-2[\infty] - D).$$

Ist $\mathrm{grad}(D) \geq 0$, so ist $\mathrm{grad}(-2[\infty] - D) < 0$, also $\ell(-2[\infty] - D) = 0$, was zu

$$\ell(D) = \mathrm{grad}(D) + 1 \text{ für } \mathrm{grad}(D) \geq 0$$

führt. Diese Aussage haben wir bereits zuvor erhalten, wobei wir außerdem eine Basis für $\mathcal{L}(D)$ bestimmt haben.

Bemerkung: Wir wissen bereits, dass gilt

$$\mathcal{L}(0) = \overline{K}, \quad \text{und damit} \quad \ell(0) = 1.$$

Setzen wir dies in Riemann-Roch ($\ell(D) = \mathrm{grad}(D) + 1 - g + \ell(K_C - D)$) ein, so erhalten wir

$$1 = \ell(0) = \mathrm{grad}(0) + 1 - g + \ell(K_C - 0) = 1 - g + \ell(K_C),$$

und damit

$$\ell(K_C) = g.$$

Insbesondere bedeutet dies, dass das Geschlecht g eine ganze Zahl ≥ 0 ist.
Setzen wir jetzt $D = K_C$ in Riemann-Roch ein, so erhalten wir

$$g = \ell(K_C) = \operatorname{grad}(K_C) + 1 - g + \ell(K_C - K_C) = \operatorname{grad}(K_C) + 1 - g + 1,$$

also

$$\operatorname{grad}(K_C) = 2g - 2.$$

Über diese Formel hatten wir zuvor das Geschlecht einer Kurve definiert. Wir fassen nochmals zusammen:

FOLGERUNG.

$$\ell(K_C) = g \quad \textit{und} \quad \operatorname{grad}(K_C) = 2g - 2.$$

Bemerkung: Sei $K_C = \operatorname{div}(\omega)$ mit einer Differentialform ω. Dann gilt für $f \in \overline{K}(C), f \neq 0$:

$$f \in \mathcal{L}(K_C) \iff \operatorname{div}(f) + \operatorname{div}(\omega) \geq 0 \iff \operatorname{div}(f\omega) \geq 0,$$

also

$$\mathcal{L}(K_C) \simeq \{\text{holomorphe Differentialformen auf } C\}.$$

Man deutet daher $\mathcal{L}(K_C)$ oft auch als $\overline{K}$-Vektorraum der holomorphen Differentialformen auf C.

Der Satz von Riemann-Roch

$$\ell(D) = \operatorname{grad}(D) + 1 - g + \ell(K_C - D)$$

berechnet zunächst nicht $\ell(D)$ in Abhängigkeit von $\operatorname{grad}(D)$, denn ein Korrekturterm $\ell(K_C - D)$ ist erforderlich. Gilt aber $\operatorname{grad}(K_C - D) < 0$, d.h. $\operatorname{grad}(D) > 2g - 2$, so ist $\ell(K_C - D) = 0$ und Riemann-Roch ergibt $\ell(D) = \operatorname{grad}(D) + 1 - g$. Damit haben wir gezeigt:

FOLGERUNG. *Für einen Divisor $D \in \operatorname{Div}(C)$ gilt*

$$\operatorname{grad}(D) > 2g - 2 \quad \Rightarrow \quad \ell(D) = \operatorname{grad}(D) + 1 - g.$$

Beispiele:

$g = 0$	$\operatorname{grad}(D) \geq -1$	$\Longrightarrow$	$\ell(D) = \operatorname{grad}(D) + 1$
$g = 1$	$\operatorname{grad}(D) \geq 1$	$\Longrightarrow$	$\ell(D) = \operatorname{grad}(D)$
$g = 2$	$\operatorname{grad}(D) \geq 3$	$\Longrightarrow$	$\ell(D) = \operatorname{grad}(D) - 1$
$g = 3$	$\operatorname{grad}(D) \geq 5$	$\Longrightarrow$	$\ell(D) = \operatorname{grad}(D) - 2$

Beispiel: Sei $P \in C$. Für alle $n \geq 2g - 1$ gilt $\ell(n[P]) = n + 1 - g$, d.h. es gibt Funktionen, die nur in P eine Polstelle haben.

Beispiel: Sei $C \subseteq \mathbb{P}^2$ definiert durch die affine Gleichung $y^2 = (x - e_1)(x - e_2)(x - e_3)$ mit drei verschiedenen Zahlen $e_1, e_2, e_3 \in \overline{K}$ (in Charakteristik $\neq 2$). Die Kurve C hat genau einen Punkt im Unendlichen, nämlich $\infty = (0 : 0 : 1)$. Es gilt

$$\operatorname{ord}_\infty(x) = -2, \quad \operatorname{ord}_\infty(y) = -3.$$

Wir haben $K_C = \operatorname{div}(\frac{dx}{y}) = 0$ berechnet, sodass C Geschlecht $g = 1$ hat.
Was ist $\mathcal{L}(n[\infty])$ für $n \geq 1$? Riemann-Roch liefert

$$\ell(n[\infty]) = \operatorname{grad}(n[\infty]) + 1 - g + \ell(K_C - n[\infty]) = n + \ell(-n[\infty]) = n.$$

Da die Funktionen x und y außerhalb von ∞ definiert sind, da wir $\operatorname{ord}_\infty(x) = -2$ und $\operatorname{ord}_\infty(y) = -3$ wissen, können wir leicht die Räume $\mathcal{L}(n[\infty])$ gut beschreiben. (y^2 kann dabei als Linearkombination von $1, x, x^2, x^3$ dargestellt werden.)

$$\begin{aligned}
\mathcal{L}([\infty]) &= \overline{K} \\
\mathcal{L}(2[\infty]) &= \overline{K} + \overline{K}x \\
\mathcal{L}(3[\infty]) &= \overline{K} + \overline{K}x + \overline{K}y \\
\mathcal{L}(4[\infty]) &= \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 \\
\mathcal{L}(5[\infty]) &= \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy \\
\mathcal{L}(6[\infty]) &= \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy + \overline{K}x^3
\end{aligned}$$

Induktiv sieht man schnell, dass

$$1, x, x^2, , x^2, \ldots, x^{[\frac{n}{2}]}, y, xy, x^2y, \ldots, x^{[\frac{n-3}{2}]}y$$

eine Basis von $\mathcal{L}(n[\infty])$ ist.

Bemerkung: Es gibt Verfahren, wie man explizit eine Basis von $\mathcal{L}(D)$ bestimmen kann.

Für uns ist folgende Aussage von Bedeutung:

SATZ. *Ist $D \in \mathrm{Div}_K(C)$ ein über K definierter Divisor, so besitzt $\mathcal{L}(D)$ eine Basis aus $K(C)$.*

Beweis: Es genügt zu zeigen: Jedes Element aus $\mathcal{L}(D)$ ist Linearkombination von Elementen von $\mathcal{L}(D) \cap K(C)$. Sei also $f \in \mathcal{L}(D) \setminus \{0\}$. Dann gibt es eine endliche galoissche Körpererweiterung L von K mit $f \in L(C)$. Sei $G = \mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$ (mit $\sigma_1 = \mathrm{id}_L$) und $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L. Wir definieren

$$g_i = \sigma_1(\alpha_i f) + \cdots + \sigma_n(\alpha_i f).$$

Da g_i invariant unter G ist, folgt $g_i \in K(C)$. Aus $f \in \mathcal{L}(D)$ folgt $\mathrm{div}(f) + D \geq 0$, und damit wegen $\mathrm{div}(\sigma_i(f)) = \sigma_i(\mathrm{div}(f))$ und $\sigma_i(D) = D$ auch $\mathrm{div}(\sigma_i(f)) + D \geq 0$, also $\sigma_i(f) \in \mathcal{L}(D)$, und damit auch $g_i \in \mathcal{L}(D)$. Insgesamt gilt $g_i \in \mathcal{L}(D) \cap K(C)$. Nun haben wir

$$\begin{pmatrix} g_1 \\ \ldots \\ g_n \end{pmatrix} = \begin{pmatrix} \sigma_1\alpha_1 & \sigma_2\alpha_1 & \ldots & \sigma_n\alpha_1 \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_1\alpha_n & \sigma_2\alpha_n & \ldots & \sigma_n\alpha_n \end{pmatrix} \begin{pmatrix} \sigma_1 f \\ \ldots \\ \sigma_n f \end{pmatrix}.$$

Die Matrix werde mit M bezeichnet. Dann ist $\det(M)^2$ die/eine Diskriminante von L über K, also $\neq 0$. Mithin ist $f = \sigma_1 f$ $\overline{K}$-Linearkombination von $g_1, \ldots, g_n$, was wir zeigen wollten. ■

Beispiel: Wir betrachten die Quadrik $Q \subseteq \mathbb{P}^2$, die affin durch die Gleichung

$$y + ax^2 + bxy + cy^2 = 0$$

mit $a \neq 0$ definiert wird. (Wegen $a \neq 0$ ist die Kurve nichtsingulär - in jeder Charakteristik.) Der Grad ist 2, also hat Q Geschlecht 0. Wir haben den K-rationalen Punkt $P = (0, 0)$ und wollen $\mathcal{L}([P])$ bestimmen. Nach Riemann-Roch ist $\ell([P]) = 2$. Natürlich ist $\overline{K} \subseteq \mathcal{L}([P])$.
Im Endlichen: Im Funktionenkörper gilt $ax^2 = -y(1 + bx + cy)$. Wir betrachten folgende Funktion f und geben verschiedene Darstellungen an:

$$f = \frac{x}{y} = -\frac{1}{a} \cdot \frac{1 + bx + cy}{x}.$$

f hat höchstens für $x = y = 0$ eine Polstelle, also in P. Andererseits ist x uniformisierend in P, also sieht man aus der zweiten Darstellung $\mathrm{ord}_P(f) = -1$.
Im Unendlichen: Wir haben projektiv $x_0x_2 + ax_1^2 + bx_1x_2 + cx_2^2 = 0$, also im Unendlichen die Punkte mit $x_0 = 0$ und $ax_1^2 + bx_1x_2 + cx_2^2 = 0$. Für sie gilt $x_2 \neq 0$. Wir führen also affine Koordinaten r, s mit $(r : s : 1) = (x_0 : x_1 : x_2) = (1 : x : y) = (\frac{1}{y} : \frac{x}{y} : 1)$ ein. Also ist $f = s$, insbesondere hat f keine Polstelle im Unendlichen.
Also hat f genau eine Polstelle, nämlich in P, woraus sofort

$$\mathcal{L}([P]) = \overline{K} + \overline{K}\frac{x}{y}$$

folgt. Wir behandeln den Spezialfall

$$y + 2x^2 + 3xy + 4y^2 = 0 \quad \text{über} \quad \mathbb{F}_{11}$$

mit SAGE:

```
Proj.<x0,x1,x2>=ProjectiveSpace(GF(11),2)
f=x0*x2+2*x1^2+3*x1*x2+4*x2^2
C=Curve(f,Proj)
P=C.point([1,0,0])
D=C.divisor([(1,P)])
L=C.riemann_roch_basis(D)
```

SAGE liefert als Basis von $\mathcal{L}(D)$

$$1, \quad \frac{3x_0 + x_2}{x_1},$$

während wir zuvor $\mathcal{L}([P]) = \overline{K} + \overline{K}\,\frac{x_1}{x_2}$ erhalten haben. Tatsächlich überprüft man, dass gilt

$$\frac{3x_0 + x_2}{x_1} = 2 + 5 \cdot \frac{x_1}{x_2},$$

sodass die Ergebnisse übereinstimmen. (Mir ist nicht klar, ob man mit SAGE im Funktionenkörper rechnen kann.)

LEMMA. *Ist D ein Divisor vom Grad d und $d \geq g_C$, so gibt es Punkte $P_1, \ldots, P_d \in C$ mit $D \sim [P_1] + \cdots + [P_d]$. D.h. Divisoren mit einem Grad $\geq g_C$ sind linear äquivalent zu effektiven Divisoren. (Die Punkt $P_1, \ldots, P_d$ müssen nicht paarweise verschieden sein.)*

Beweis: Mit Riemann-Roch gilt

$$\ell(D) = \operatorname{grad}(D) + 1 - g_C + \ell(K_C - D) \geq d + 1 - g_C \geq 1,$$

also gibt es ein $f \in \mathcal{L}(D) \setminus \{0\}$. Es folgt $D + \operatorname{div}(f) \geq 0$. Schreibt man $D + \operatorname{div}(f) = [P_1] + \cdots + [P_d]$, so folgt die Behauptung. ■

LEMMA. *Sei $P_0 \in C$ fest gewählt. Dann ist*

$$\phi : C^g \to \operatorname{Pic}^0(C), \quad (P_1, \ldots, P_g) \mapsto \textit{Klasse von } [P_1] + \cdots + [P_g] - g[P_0]$$

surjektiv. (C^g meint hier einfach das g-fache mengentheoretische Produkt von C.)

Beweis: D_0 sei ein Divisor vom Grad 0, der eine Klasse in $\operatorname{Pic}^0(C)$ repräsentiert. Zu $D_0 + g[P_0]$ existieren nach dem letzten Lemma Punkte $P_1, \ldots, P_g$ mit $D_0 + g[P_0] \sim [P_1] + \cdots + [P_g]$, was $D_0 \sim [P_1] + \cdots + [P_g] - g[P_0]$ und damit die Behauptung zeigt. ■

Konstruktion von rationalen Abbildungen: Sei D ein Divisor auf C mit $\ell(D) \geq 2$. Sei $f_0, \ldots, f_r$ eine $\overline{K}$-Basis von $\mathcal{L}(D)$. Dann definieren wir $\phi_D : C \to \mathbb{P}^r$ durch

$$\phi_D = (f_0 : \cdots : f_r).$$

(Wählt man eine andere Basis von $\mathcal{L}(D)$, so bedeutet dies einen Basiswechsel in $\mathbb{P}^r$.)
Gilt $\mathcal{L}(D) = \mathcal{L}(D - [P])$ für einen Punkt P, so können wir $D - [P]$ statt D betrachten. Wir setzen also voraus

$$\mathcal{L}(D - [P]) \neq \mathcal{L}(D), \text{ d.h. } \ell(D - [P]) = \ell(D) - 1$$

für alle Punkte P. (Man nennt ein solches D basispunktfrei.)
Sei $P \in C$ und t_P uniformisierend in P. Sei n_P die Multiplizität des Divisors D in P, also $D = n_P[P] + \ldots$. Dann ist $\operatorname{ord}_P(f_i t_P^{n_P}) \geq 0$ und $= 0$ für mindestens einen Index i und

$$\phi_D(P) = ((f_0 t_P^{n_P})(P) : \cdots : (f_r t_P^{n_P})(P)).$$

Wir untersuchen, wann ϕ_D injektiv ist. Es gilt:

$$\begin{aligned}
\phi_D(P) \neq \phi_D(Q) \quad &\iff \quad \text{es gibt eine Hyperebene } H = \{a_0x_0 + \cdots + a_rx_r = 0\} \text{ mit } \phi_D(P) \in H, \phi_D(Q) \notin H \\
&\iff \quad \text{es gibt } a_0, \ldots, a_r \text{ nicht alle 0 mit } (\sum a_i f_i t_P^{n_P})(P) = 0, (\sum a_i f_i t_Q^{n_Q})(Q) \neq 0 \\
&\iff \quad \text{es gibt } a_0, \ldots, a_r \text{ nicht alle 0 mit } \sum a_i f_i \in \mathcal{L}(D - [P]), \sum a_i f_i \notin \mathcal{L}(D - [P] - [Q]) \\
&\iff \quad \mathcal{L}(D - [P] - [Q]) \neq \mathcal{L}(D - [P]) \\
&\iff \quad \ell(D - [P] - [Q]) = \ell(D - [P]) - 1 = \ell(D) - 2
\end{aligned}$$

Es stellt sich heraus, dass die letzte Bedingung sogar die Bedingung dafür ist, dass ϕ_D eine Einbettung ist. (Etwas ausführlicher wird dies bei [**Hulek**, S.161-162] behandelt, genauer bei [**Hartshorne**, S.307-308].)

SATZ. *Genau dann ist ϕ_D eine Einbettung, d.h. $\phi_D(C)$ ist isomorph zu C, wenn für alle $P, Q \in C$ gilt:*

$$\ell(D - [P] - [Q]) = \ell(D) - 2.$$

In diesem Fall ist $\mathrm{grad}(D)$ *der Grad von $\phi_D(C)$ in $\mathbb{P}^r$ mit $r = \ell(D) - 1$. Man nennt einen solchen Divisor D dann auch* **sehr ampel**.

Noch eine Bemerkung zum Grad von $\phi_D(C)$: Ist $D = n_1[P_1] + \cdots + n_r[P_r]$, so kann man nach Koordinatenwechsel $\mathrm{ord}_{P_i}(f_0) = -n_i$ annehmen. Damit hat f_0 dann $n_1 + \cdots + n_r = \mathrm{grad}(D)$ Polstellen, also ebensoviele Nullstellen. Die Nullstellen liefern den Schnitt von $\phi_D(C)$ mit der Hyperebene $x_0 = 0$, woraus sich die Behauptung ergibt.

SATZ. *Gilt* $\mathrm{grad}(D) \geq 2g + 1$*, so ist D sehr ampel, d.h. ϕ_D liefert eine Einbettung $C \simeq \phi_D(C) \subseteq \mathbb{P}^r$.*

Beweis: Seien $P, Q \in C$ beliebige Punkte. Wegen $\mathrm{grad}(K_C) = 2g - 2$ gilt

$$\mathrm{grad}(D) \geq 2g + 1 > \mathrm{grad}(K_C) \quad \text{und} \quad \mathrm{grad}(D - [P] - [Q]) \geq 2g - 1 > \mathrm{grad}(K_C),$$

also $\mathrm{grad}(K_C - D) < 0$ und $\mathrm{grad}(K_C - (D - [P] - [Q])) < 0$, sodass Riemann-Roch

$$\ell(D) = \mathrm{grad}(D) + 1 - g$$

und

$$\ell(D - [P] - [Q]) = \mathrm{grad}(D - [P] - [Q]) + 1 - g = \mathrm{grad}(D) + 1 - g - 2 = \ell(D) - 2$$

liefert. Mit dem vorangegangenen Satz folgt die Behauptung. ■

Beispiele:

(1) $C = \mathbb{P}^1$: Für $n \geq 1$ hat $\mathcal{L}(n[\infty])$ als Basis $1, x, x^2, \ldots, x^n$. Also ist

$$\phi_{n[\infty]} = (1 : x : \cdots : x^n).$$

Das Bild ist die sogenannte **rationale Normkurve vom Grad** n im $\mathbb{P}^n$:

$$\phi_{n[\infty]}(\mathbb{P}^1) = \{(x_0^n : x_0^{n-1}x_1 : \cdots : x_1^n) : (x_0 : x_1) \in \mathbb{P}^1\}.$$

(2) Die Kurve C mit $y^2 = x^3 - x$ hat Geschlecht 1 und den unendlich fernen Punkt $P = (0 : 0 : 1)$. Es ist $\mathrm{ord}_P(x) = -2$, $\mathrm{ord}_P(y) = -3$. Wie sieht $\phi_{4[P]}$ aus? $\mathcal{L}(4[P])$ hat als Basis $1, x, y, x^2$, also: $\phi_{4[P]} : C \to \mathbb{P}^3$ mit

$$\phi_{4[P]} = (1 : x : y : x^2).$$

Das Bild ist eine Kurve vom Grad 4 in $\mathbb{P}^3$. Verwendet man in $\mathbb{P}^3$ die homogenen Koordinaten z_0, z_1, z_2, z_3, so gelten folgende Gleichungen für das Bild:

$$z_1^2 = x^2 = z_0 z_3, \quad z_2^2 = y^2 = x \cdot x^2 - x = z_1 z_3 - z_1 z_0,$$

nochmals:

$$\phi_{4[P]}(C) \subseteq \{z_1^2 = z_0 z_3, z_2^2 = z_1 z_3 - z_1 z_0\}.$$

Man kann zeigen, dass diese Gleichungen das Bild sogar beschreiben.

(3) Ist C eine Kurve vom Geschlecht 2 und wählt man 5 Punkte $P_1, \ldots, P_5$, so ist $D = [P_1] + \cdots + [P_5]$ wegen $\mathrm{grad}(D) = 5 \geq 2 \cdot 2 + 1$ sehr ampel. Wegen $\mathrm{grad}(D) = 5$ und $\ell(D) = 4$ liefert ϕ_D eine Einbettung von C in $\mathbb{P}^3$ als Kurve vom Grad 5.

Beispiel: Wir betrachten über $\mathbb{F}_7$ die durch

$$f = x_0^3 + 2x_1^3 + 3x_2^3$$

definierte projektive ebene Kurve. C ist nichtsingulär (und absolut irreduzibel), hat als ebene Kubik daher Geschlecht 1. Es gibt 9 Punkte, die über $\mathbb{F}_7$ definiert sind, nämlich

$$(1:1:3), (1:2:3), (1:4:3), (1:1:5), (1:2:5), (1:4:5), (1:1:6), (1:2:6), (1:4:6).$$

Die Hesse-Kurve zu C wird durch $x_0 x_1 x_2 = 0$ definiert. Daraus sieht man, dass C keinen Wendepunkt hat, der über $\mathbb{F}_7$ definiert ist.
Wir betrachten den Punkt $P = (1 : 1 : 6)$ und den Divisor $3[P]$, der wegen $\mathrm{grad}(3[P]) = 3 = 2 \cdot 1 + 1$ sehr ampel ist. Riemann-Roch liefert $\ell(3[P]) = 3$. Wir bestimmen eine Basis von $\mathcal{L}(3[P])$ mit SAGE:

```
Proj.<x0,x1,x2>=ProjectiveSpace(GF(7),2)
f=x0^3+2*x1^3+3*x2^3
C=Curve(f,Proj)
P=C.point([1,1,-1])
D=C.divisor([(3,P)])
f0,f1,f2=C.riemann_roch_basis(D)
```

SAGE liefert als Basis von $\mathcal{L}(3[P])$:

$$\begin{aligned} f_0 &= \frac{5x_0^3+x_0^2x_1+4x_0x_1^2+x_1^3+x_0^2x_2-x_0x_1x_2-x_0x_2^2}{2x_0^2x_1+3x_0^2x_2+x_1x_2^2}, \\ f_1 &= \frac{-x_0^3+x_0^2x_1+x_0x_1^2+x_0^2x_2-x_0x_1x_2+x_1^2x_2+2x_0x_2^2}{2x_0^2x_1+3x_0^2x_2+x_1x_2^2}, \\ f_2 &= 1. \end{aligned}$$

Wir betrachten die zugehörige Abbildung $\phi = \phi_{3[P]} = (f_0 : f_1 : f_2)$, wobei wir mit dem Nenner durchmultipliziert haben:

$$\begin{aligned} f_0 &= 5x_0^3+x_0^2x_1+x_0^2x_2+4x_0x_1^2-x_0x_1x_2-x_0x_2^2+x_1^3, \\ f_1 &= -x_0^3+x_0^2x_1+x_0^2x_2+x_0x_1^2-x_0x_1x_2+2x_0x_2^2+x_1^2x_2, \\ f_2 &= 2x_0^2x_1+3x_0^2x_2+x_1x_2^2. \end{aligned}$$

Da der Divisor $3[P]$ sehr ampel vom Grad 3 ist, ist die Bildkurve $\phi(C)$ eine Kurve vom Grad 3, die isomorph zu C ist. Mit SAGE bestimmen wir eine Gleichung $g = 0$ für die Bildkurve, wobei wir bequemlichkeitshalber neue Koordinaten y_0, y_1, y_2 für die Bildkurve verwenden:

```
R.<x0,x1,x2,y0,y1,y2>=PolynomialRing(GF(7),order='lex')
f=x0^3+2*x1^3+3*x2^3
f0=-2*x0^3+x0^2*x1+x0^2*x2-3*x0*x1^2-x0*x1*x2-x0*x2^2+x1^3
f1=-x0^3+x0^2*x1+x0^2*x2+x0*x1^2-x0*x1*x2+2*x0*x2^2+x1^2*x2
f2=2*x0^2*x1+3*x0^2*x2+x1*x2^2
I=R*(f,y0-f0,y1-f1,y2-f2)
g=(I.groebner_basis())[-1]
```

Wir erhalten

$$g = y_0^3 - y_0^2y_1 + 3y_0^2y_2 + 5y_0y_1^2 + 3y_0y_2^2 + y_1^3 - y_1^2y_2 + 5y_1y_2^2 + y_2^3.$$

Wir berechnen die zu $g = 0$ gehörige Hesse-Kurve; sie ist gegeben durch das Polynom.

$$h = 4y_0^3 + 2y_0^2y_2 + 2y_0y_1^2 + 5y_0y_1y_2 + y_1^3 + 4y_1y_2^2 + 2y_2^3.$$

Man findet, dass $\phi(C)$ (natürlich) auch 9 Punkte hat, die über $\mathbb{F}_7$ definiert sind, nämlich

$$(0:1:3), (1:3:0), (1:6:1), (1:5:2), (1:2:3), (1:4:3), (1:6:3), (1:6:5), (1:0:6).$$

Man stellt außerdem fest, dass alle 9 Punkte Wendepunkte sind. (Damit ist C über $\mathbb{F}_7$ isomorph zu $\phi(C)$, aber nicht projektiv äquivalent zu $\phi(C)$.)

Beispiel: Wir betrachten über $\mathbb{F}_7$ die durch

$$f = x_0^2 + 2x_1^2 + 3x_2^2$$

definierte projektive ebene Quadrik C. Die Kurve ist nichtsingulär und hat daher 8 über $\mathbb{F}_7$ definierte Punkte:

$$(0:1:2), (0:1:5), (1:0:3), (1:0:4), (1:2:2), (1:2:5), (1:5:2), (1:5:5).$$

Wir betrachten den Divisor

$$D = [(1:2:5)] + 2[(1:5:2)]$$

vom Grad 3. Eine Basis des Vektorraums $\mathcal{L}(D)$ berechnen wir mit SAGE:

```
Proj.<x0,x1,x2>=ProjectiveSpace(GF(7),2)
f=x0^2+2*x1^2+3*x2^2
C=Curve(f,Proj)
P1=C.point([1,2,5])
P2=C.point([1,5,2])
D=C.divisor([(1,P1),(2,P2)])
f0,f1,f2,f3=C.riemann_roch_basis(D)
```

Wir erhalten

$$\begin{aligned} f_0 &= \frac{x_0x_1}{3x_0^2+x_0x_1+x_1^2+x_0x_2}, \\ f_1 &= \frac{3x_0^2+x_0x_2}{3x_0^2+x_0x_1+x_1^2+x_0x_2}, \\ f_2 &= \frac{x_1^2}{3x_0^2+x_0x_1+x_1^2+x_0x_2}, \\ f_3 &= \frac{x_1x_2}{3x_0^2+x_0x_1+x_1^2+x_0x_2}. \end{aligned}$$

Die zugehörige Abbildung in den $\mathbb{P}^3$ ist dann

$$\phi = (f_0 : f_1 : f_2 : f_3) = (x_0x_1 : 3x_0^2+x_0x_2 : x_1^2 : x_1x_2).$$

Wir bestimmen Gleichungen für das Bild mit Hilfe von Gröbner-Basen: Im Polynomring $\mathbb{F}_7[x_0,x_1,x_2,y_0,y_1,y_2,y_3]$ verwendet man die lexikographische Ordnung und bestimmt eine Gröbner-Basis B des Ideals

$$I = (f, f_0-y_0, f_1-y_1, f_2-y_2, f_3-y_3).$$

Die Elemente von $B \cap \mathbb{F}_7[y_0,y_1,y_2,y_3]$, die am Schluss der Gröbner-Basis stehen, beschreiben dann $\phi(C)$.

```
R.<x0,x1,x2,y0,y1,y2,y3>=PolynomialRing(GF(7),order='lex')
f=x0^2+2*x1^2+3*x2^2
f0,f1,f2,f3=x0*x1,3*x0^2+x0*x2,x1^2,x1*x2
I=R*(f,f0-y0,f1-y1,f2-y2,f3-y3)
B=I.groebner_basis()
```

Die Gröbner-Basis besteht aus den Polynomen $g_1,\dots,g_{18}$:

$$\begin{aligned} g_1 &= x_0^2+3x_2^2+2y_2, \\ g_2 &= x_0x_1-y_0, \\ g_3 &= x_0x_2+5x_2^2-y_1+y_2, \\ g_4 &= x_0y_0+2x_1y_2+3x_2y_3, \\ g_5 &= x_0y_1-x_1y_0+2x_2y_1, \\ g_6 &= x_0y_2-x_1y_0, \\ g_7 &= x_0y_3-x_2y_0, \\ g_8 &= x_1^2-y_2, \\ g_9 &= x_1x_2-y_3, \\ g_{10} &= x_1y_1-x_1y_2-x_2y_0+2x_2y_3, \\ g_{11} &= x_1y_3-x_2y_2, \\ g_{12} &= x_2^2y_0+5x_2^2y_3-y_1y_3+y_2y_3, \\ g_{13} &= x_2^2y_1+2y_1^2+3y_1y_2+2y_2^2+3y_3^2, \\ g_{14} &= x_2^2y_2-y_3^2, \\ g_{15} &= y_0^2+2y_2^2+3y_3^2, \\ g_{16} &= y_0y_1-y_0y_2+2y_1y_3, \\ g_{17} &= y_0y_3-y_1y_2+y_2^2+5y_3^2, \\ g_{18} &= y_1^2y_2+5y_1y_2^2+4y_1y_3^2+y_2^3+5y_2y_3^2. \end{aligned}$$

Nur $g_{15}, g_{16}, g_{17}, g_{18}$ sind in $\mathbb{F}_7[y_0, y_1, y_2, y_3]$ und beschreiben daher $\phi(C)$:

$\phi(C) = \{y_0^2+2y_2^2+3y_3^2 = 0,\ y_0y_1-y_0y_2+2y_1y_3 = 0,\ y_0y_3-y_1y_2+y_2^2+5y_3^2 = 0,\ y_1^2y_2+5y_1y_2^2+4y_1y_3^2+y_2^3+5y_2y_3^2 = 0\}$.

Tatsächlich testet man, dass auch $\phi(C)$ genau 8 Punkte über $\mathbb{F}_7$ hat:

$(0:0:1:2), (0:0:1:5), (0:1:0:0), (1:0:0:4), (1:1:5:2), (1:3:5:5), (1:4:2:5), (1:6:2:2)$.

Bemerkungen:

(1) Der $\overline{K}$-Vektorraum der homogenen Polynome in x_0, x_1, x_2 vom Grad d hat Dimension

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

Eine Basis bilden die Monome

$$x_0^i x_1^j x_2^k \text{ mit } i, j, k \in \mathbb{N}_0 \text{ und } i+j+k = d.$$

(2) Sei C eine nichtsinguläre ebene Kurve vom Grad d. Ist K_C ein kanonischer Divisor und $\mathrm{div}(\ell)$ ein Geradenschnitt, so gilt

$$K_C \sim (d-3)\mathrm{div}(\ell).$$

Im Fall $d \geq 4$ gilt

$$\ell(K_C) = g = \frac{(d-1)(d-2)}{2}.$$

Wir haben gesagt, dass man $\mathcal{L}(K_C)$ mit dem Vektorraum der holomorphen Differentialformen identifizieren kann. Der Vektorraum der homogenen Polynome in x_0, x_1, x_2 vom Grad $d-3$ hat ebenfalls Dimension

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

Wir haben nicht allgemein den Schnitt zweier ebenen Kurven definiert. Daher sei nur erwähnt, dass die effektiven kanonischen Divisoren auf einer Kurve vom Grad d genau die Schnitte mit den Kurven vom Grad $d-3$ sind.

KAPITEL 11

Kurven vom Geschlecht 0

1. Allgemeines zu Kurven vom Geschlecht 0

Wenn nichts anderes erwähnt wird, bezeichnet C eine absolut irreduzible, nichtsinguläre, projektive Kurve, die über einem vollkommenen Körper K definiert ist. (Für $g = 0$ lautet Riemann-Roch $\ell(D) = \operatorname{grad}(D) + 1$ für $\operatorname{grad}(D) \geq -1$.)

SATZ. *Hat C Geschlecht 0 und gibt es einen über K definierten Divisor D vom Grad 1, so ist C (über K) isomorph zu $\mathbb{P}^1$. Insbesondere besitzt C eine über K-definierte Parametrisierung:*

$$C = \{(f_0(t_0,t_1) : f_1(t_0,t_1) : \cdots : f_r(t_0,t_1)) : (t_0 : t_1) \in \mathbb{P}^1\},$$

wo die f_i homogene Polynome gleichen Grades mit Koeffizienten in K sind.

Beweis:

- *1. Beweis:* Aus $\operatorname{grad}(D) = 1$ folgt $\ell(D) = 2$. Sei f_0, f_1 eine K-Basis von $\mathcal{L}(D)$. Wegen $\operatorname{grad}(D) = 1 = 2{\cdot}0{+}1$ ist D sehr ampel, also $\phi : C \to \mathbb{P}^1$ mit $\phi = (f_0 : f_1)$ eine Einbettung, d.h. $C \simeq \phi_D(C)$. Nun ist aber $\phi_D(C) = \mathbb{P}^1$, also ϕ_D ein Isomorphismus.
- *2. Beweis:* Aus $\operatorname{grad}(D) = 1$ folgt $\ell(D) = 2$, also gibt es ein $f \in K(C) \cap \mathcal{L}(D)$ mit $D + \operatorname{div}(f) \geq 0$, also einen Punkt $P \in C(K)$ mit $D + \operatorname{div}(f) = [P]$. Es ist $\ell([P]) = 2$, also gibt es eine Funktion $g \in K(C) \cap \mathcal{L}([P])$ mit $\mathcal{L}([P]) = \overline{K} + \overline{K}g$. Dann hat g genau eine Polstelle, und zwar in P mit $\operatorname{ord}_P(g) = -1$. Deshalb hat der zugehörige Morphismus $\phi = (1 : g) : C \to \mathbb{P}^1$ Grad 1, was $K(\mathbb{P}^1) \simeq K(C)$ impliziert. Also ist C über K isomorph zu $\mathbb{P}^1$. ■

FOLGERUNG. *Hat C Geschlecht 0 und besitzt C einen K-rationalen Punkt, so ist C über K isomorph zu $\mathbb{P}^1$. Insbesondere gilt $\#C(K) = \#\mathbb{P}^1(K)$.*

Beweis: Ist P ein K-rationaler Punkt, so ist $[P]$ natürlich auch ein K-rationaler Divisor vom Grad 1, woraus die Behauptung mit dem Satz folgt. ■

Über dem algebraischen Abschluss gibt es natürlich immer Punkte, also folgt (mit $K = \overline{K}$):

FOLGERUNG. *Jede Kurve C vom Geschlecht 0 ist über $\overline{K}$ isomorph zu $\mathbb{P}^1$. Über einem algebraisch abgeschlossenen Körper gibt es also bis auf Isomorphie genau eine Kurve vom Geschlecht 0, nämlich $\mathbb{P}^1$.*

Da die Picardgruppe über dem algebraischen Abschluss berechnet wird, folgt unmittelbar

FOLGERUNG. *Hat C Geschlecht 0, so gilt*

$$\operatorname{Pic}(C) \simeq \mathbb{Z} \quad \textit{und} \quad \operatorname{Pic}^0(C) = 0.$$

Nicht jede Kurve vom Geschlecht 0 ist (über K) isomorph zu $\mathbb{P}^1$, wie folgendes Beispiel zeigt:

Beispiel: Sei $C = \{2x_0^2 + 3x_1^2 + 5x_2^2 = 0\} \subseteq \mathbb{P}^2$. Die Kurve C ist über $\mathbb{Q}$ definiert, hat als glatte Quadrik Geschlecht 0, hat keine reellen Punkte, insbesondere $C(\mathbb{Q}) = \emptyset$. Damit kann C auch nicht über $\mathbb{Q}$ isomorph zu $\mathbb{P}^1$ sein.

Datei: algku11.tex. Version vom 18.7.2021

Die folgenden Sätze geben Situationen an, wo man sofort weiß, dass eine Kurve vom Geschlecht 0 isomorph zu $\mathbb{P}^1$ ist.

SATZ. *Ist $C \subseteq \mathbb{P}^n$ eine Kurve ungeraden Grades vom Geschlecht 0, so ist C isomorph zu $\mathbb{P}^1$ über K.*

Beweis: Sei H der Divisor eines Hyperebenenschnitts. Er ist über K definiert und hat $\operatorname{grad}(H) = 2m+1$, wenn die Kurve Grad $2m+1$ hat. Sei K_C ein über K definierter kanonischer Divisor. Es gilt $\operatorname{grad}(K_C) = -2$. Dann ist $H + mK_C$ über K definiert mit $\operatorname{grad}(H + mK_C) = 1$, also ist nach unserem Satz C über K isomorph zu $\mathbb{P}^1$. ■

Beispiel: Ist $C \subseteq \mathbb{P}^n$ eine über K definierte Gerade, so ist $C \simeq \mathbb{P}^1$, es gibt also eine Parametrisierung

$$C = \{(a_0u + b_0v : \cdots : a_nu + b_nv) : (u : v) \in \mathbb{P}^1\}$$

mit $a_0, b_0, \ldots, a_n, b_n \in K$.

SATZ. *Ist $\widetilde{C} \subseteq \mathbb{P}^n$ eine absolut irreduzible, über K definierte, projektive Kurve ungeraden Grades mit nur endlich vielen Singularitäten, so dass die Desingularisierung C Geschlecht 0 hat, so ist C über K isomorph zu $\mathbb{P}^1$, also gibt es eine Parametrisierung*

$$\widetilde{C} = \{(f_0(t_0, t_1) : f_1(t_0, t_1) : \cdots : f_r(t_0, t_1)) : (t_0 : t_1) \in \mathbb{P}^1\},$$

wo die f_i homogene Polynome gleichen Grades mit Koeffizienten in K sind.

Beweisidee: Man wähle einen über K definierten Hyperebenenschnitt, der keine Singularität enthält. (Braucht man hier eine Voraussetzung über K?) Dies liefert auf C einen Divisor H, der über K definiert ist und ungeraden Grad hat. Die Behauptung folgt mit dem letzten Satz. ■

Beispiel: Ist $f(x_0, x_1, x_2) = 0$ eine irreduzible ebene Kubik mit genau einer Singularität, so ist die Desingularisierung isomorph zu $\mathbb{P}^1$. Wählt man z.B. die Kurve

$$C = \{-27x_0^2x_1 + 152x_0^3 - 75x_0^2x_2 + 4x_1^3 + 4x_2^3 = 0\},$$

so stellt man fest, dass sie genau in $(2 : 3 : 5)$ eine Singularität hat. Substituiert man $x_0 = 1, x_1 = x, x_2 = y$ und $y = \frac{5}{2} + t(x - \frac{3}{2})$ (Geraden durch die Singularität), so spaltet der Faktor $(2x - 3)^2$ ab und aus dem Rest erhält man eine Parametrisierung:

$$x_0 = 2t^3 + 2, \quad x_1 = 3t^3 - 15t^2 - 6, \quad x_2 = -10t^3 - 9t + 5.$$

2. Wie kann man sich Kurven vom Geschlecht 0 vorstellen?

Diese Frage beantwortet folgender Satz:

SATZ. *Jede Kurve C vom Geschlecht 0 ist über K isomorph zu einem (glatten) ebenen Kegelschnitt, d.h. zu einer (glatten) Kurve*

$$\{a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0\}$$

mit $a_0, a_1, a_2, a_3, a_4, a_5$ in K.

Beweis: Wähle $f \in K(C)$ mit $df \neq 0$. Dann ist der kanonische Divisor $K_C = (df)$ über K definiert. Es gilt

$$\operatorname{grad}(-K_C) = 2 \quad \text{und} \quad \ell(-K_C) = 2 + 1 - 0 + \ell(2K_C) = 3,$$

es gibt also $f_0, f_1, f_2 \in K(C)$, die eine Basis von $\mathcal{L}(-K_C)$ bilden. Wegen $\operatorname{grad}(-K_C) \geq 2g + 1$ ist $-K_C$ sehr ampel, d.h. $\phi_{-K_C} : C \to \mathbb{P}^2$ mit $\phi_{-K_C} = (f_0 : f_1 : f_2)$ ist eine Einbettung. Also $C \simeq_K \phi_{-K_C}(C) \subseteq \mathbb{P}^2$ und $\phi_{-K_C}(C)$ hat Grad 2. Außerdem ist ϕ_{-K_C} über K definiert. Damit folgt die Behauptung. ■

Wir erinnern an eine früher hergeleitete Charakterisierung der Singularität ebener Kegelschnitte, die in jeder Charakteristik gültig ist.

SATZ. *Für einen ebenen Kegelschnitt C mit der Gleichung*

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0$$

sind äquivalent:

(1) *C ist absolut irreduzibel,*
(2) *C ist nichtsingulär,*
(3) $4a_0a_3a_5 + a_1a_2a_4 - a_2^2a_3 - a_0a_4^2 - a_1^2a_5 \neq 0$.

Die nächste Frage, die sich stellt, ist:

Frage: Wann sind zwei über K definierte ebene Kegelschnitte über K isomorph?

Eine Antwort gibt der folgende Satz:

SATZ. *Zwei über K definierte (nichtsinguläre) Kegelschnitte sind genau dann isomorph über K, wenn sie über K projektiv äquivalent sind, d.h. durch Koordinatenwechsel über K auseinander hervorgehen.*

Natürlich sind projektiv äquivalente Quadriken auch isomorph. Die Umkehrung steht in folgendem Lemma:

LEMMA. *Seien C_1 und C_2 zwei über K definierte nichtsinguläre projektive ebene Quadriken und $\psi : C_1 \to C_2$ ein über K definierter Isomorphismus. Dann gibt es eine Matrix $A = (a_{ij}) \in \mathrm{GL}_3(K)$ mit*

$$\psi((x_0 : x_1 : x_2)) = \left(\sum_j a_{0j}x_j : \sum_j a_{1j}x_j : \sum_j a_{2j}x_j \right).$$

Beweis:

- Zur Unterscheidung verwenden wir auf C_1 die projektiven Koordinaten x_0, x_1, x_2, auf C_2 die projektiven Koordinaten y_0, y_1, y_2.
- Sei H_1 der Hyperebenenschnitt (x_0) auf C_1. Er hat Grad 2 und es gilt $\ell(H_1) = 3$ und
$$\mathcal{L}(H_1) = \overline{K} + \overline{K} \cdot \frac{x_1}{x_0} + \overline{K} \cdot \frac{x_2}{x_0}.$$
- Sei H_2 der Hyperebenenschnitt (y_0) auf C_2. Er hat Grad 2 und es gilt $\ell(H_2) = 3$ und
$$\mathcal{L}(H_2) = \overline{K} + \overline{K} \cdot \frac{y_1}{y_0} + \overline{K} \cdot \frac{y_2}{y_0}.$$
- $\psi^*(H_2)$ ist dann ein effektiver Divisor vom Grad 2 auf C_1 genauso wie H_1. Also sind H_1 und $\psi^*(H_2)$ linear äquivalent, d.h. es gibt eine Funktion $f \in \overline{K}(C_1)$ mit
$$\psi^*(H_2) = H_1 + \mathrm{div}(f).$$
Da H_1 und $\psi^*(H_2)$ über K definiert sind, können wir $f \in K(C_1)$ annehmen.
- Es gilt für $i = 0, 1, 2$
$$\begin{aligned} H_1 + \mathrm{div}(f \cdot \psi^*(\frac{y_i}{y_0})) &= H_1 + \mathrm{div}(f) + \mathrm{div}(\psi^*(\frac{y_i}{y_0})) = \\ &= \psi^*(H_2) + \psi^*(\mathrm{div}(\frac{y_i}{y_0})) = \psi^*\left(H_2 + \mathrm{div}(\frac{y_i}{y_0})\right) \geq 0, \end{aligned}$$
sodass folgt
$$f \cdot \psi^*(\frac{y_i}{y_0}) \in \mathcal{L}(H_1) = \overline{K} \cdot \frac{x_0}{x_0} + \overline{K} \cdot \frac{x_1}{x_0} + \overline{K} \cdot \frac{x_2}{x_0}.$$
Also gibt es Zahlen $a_{ij} \in K$ mit
$$f \cdot \psi^*(\frac{y_i}{y_0}) = \sum_j a_{ij} \frac{x_j}{x_0}.$$
Die $\frac{y_0}{y_0}, \frac{y_1}{y_0}, \frac{y_2}{y_0}$ linear unabhängig sind, ist $A = (a_{ij})$ invertierbar.

- Seien jetzt $p_0, p_1, p_2 \in \overline{K}$ mit $P = (p_0 : p_1 : p_2) \in C_1(\overline{K})$. Wir betrachten den Fall, dass $p_0 \neq 0$ und $f(P) \neq 0$ gilt. Wir setzen P jetzt in die letzte Gleichung ein und erhalten

$$f(P) \cdot \left(\psi^*(\frac{y_i}{y_0})\right)(P) = \frac{1}{p_0} \sum_j a_{ij} p_j,$$

und damit

$$f(P) \cdot (\frac{y_i}{y_0})(\psi(P)) = \frac{1}{p_0} \sum_j a_{ij} p_j.$$

Somit gilt:

$$\begin{aligned}
\psi(P) &= \left(1 : (\frac{y_1}{y_0})(\psi(P)) : (\frac{y_2}{y_0})(\psi(P))\right) = \\
&= \left(f(P) : f(P) \cdot (\frac{y_1}{y_0})(\psi(P)) : f(P) \cdot (\frac{y_2}{y_0})(\psi(P))\right) = \\
&= \left(\frac{1}{p_0}\sum_j a_{0j}p_j : \frac{1}{p_0}\sum_j a_{1j}p_j : \frac{1}{p_0}\sum_j a_{2j}p_j\right) = \left(\sum_j a_{0j}p_j : \sum_j a_{1j}p_j : \sum_j a_{2j}p_j\right).
\end{aligned}$$

Damit gilt also

$$\psi((p_0 : p_1 : p_2)) = \left(\sum_j a_{0j}p_j : \sum_j a_{1j}p_j : \sum_j a_{2j}p_j\right)$$

auf einer offenen Teilmenge, und damit natürlich allgemein. Dies beweist die Behauptung. ■

Die Klassifikation der Kegelschnitte ist ein eigenes Thema, das stark vom Grundkörper abhängt. Wir wollen uns zunächst auf endliche Körper und $\mathbb{Q}$ beschränken.

3. Kurven vom Geschlecht 0 über endlichen Körpern

SATZ. *Jede über $\mathbb{F}_p$ definierte, absolut irreduzible, nichtsinguläre, projektive Kurve C vom Geschlecht 0 ist über $\mathbb{F}_p$ isomorph zu $\mathbb{P}^1$.*

Beweis: C ist über $\mathbb{F}_p$ isomorph zu einem nichtsingulären ebenen Kegelschnitt. Ebene Kegelschnitte haben über $\mathbb{F}_p$ aber immer $\mathbb{F}_p$-rationale Punkte. Damit erhalten wir einen über $\mathbb{F}_p$ definierten Isomorphismus zu $\mathbb{P}^1$. ■

Bis auf $\mathbb{F}_p$-Isomorphie ist also $\mathbb{P}^1$ die einzige über $\mathbb{F}_p$ definierte (absolut irreduzible, nichtsinguläre, projektive) Kurve vom Geschlecht 0.

4. Exkurs: p-adische Zahlen

Dies soll keine systematische Einführung in die p-adischen Zahlen sein, sondern es soll nur kurz ein kleiner Überblick geben werden.
Neben dem üblichen Absolutbetrag $|\cdot|$ gibt es auf $\mathbb{Q}$ für jede Primzahl p einen sogenannten p-adischen Absolutbetrag. Hat $a \in \mathbb{Q}^*$ die Primfaktorzerlegung

$$a = \pm \prod_{p \text{ Primzahl}} p^{v_p(a)},$$

so setzt man

$$|a|_p = \frac{1}{p^{v_p(a)}} \quad \text{und} \quad |0|_p = 0.$$

$|\cdot|_p$ ist eine Funktion $\mathbb{Q} \to \mathbb{R}_{\geq 0}$ mit folgenden Eigenschaften:

- $|a|_p \geq 0$ und $(|a|_p = 0 \iff a = 0)$.
- $|ab|_p = |a|_p |b|_p$.
- $|a+b|_p \leq \max(|a|_p, |b|_p)$. (Daraus folgt die Dreiecksungleichung $|a+b|_p \leq |a|_p + |b|_p$.)

Die Absolutbeträge sind so normiert, dass für alle $a \in \mathbb{Q}^*$ gilt

$$|a| \cdot \prod_p |a|_p = 1.$$

Die Absolutbeträge machen $\mathbb{Q}$ zu einem metrischen Raum. Allerdings ist $\mathbb{Q}$ bezüglich der Absolutbeträge $|\cdot|_p$ (und $|\cdot|$) nicht vollständig, d.h. es gibt Cauchy-Folgen, die nicht konvergieren. Durch Vervollständigung erhält man für den normalen Absolutbetrag die reellen Zahlen $\mathbb{R}$, für $|\cdot|_p$ die Menge der p-adischen Zahlen $\mathbb{Q}_p$. Ebenso wie $\mathbb{R}$ ist auch $\mathbb{Q}_p$ ein Körper. Auch der Absolutbetrag $|\cdot|_p$ setzt sich auf $\mathbb{Q}_p$ fort.

Die Dezimaldarstellung reeller Zahlen zeigt, dass gilt

$$\mathbb{R} = \{\sum_{k=k_0}^{\infty} a_k (\frac{1}{10})^k : a_k \in \{0, 1, \ldots, 9\}, k_0 \in \mathbb{Z}\}.$$

Überlegung: Gibt man sich $a_k \in \{0, 1, \ldots, p-1\}$ für alle $k \geq 0$ beliebig vor, so bildet die Folge der Partialsummen

$$\left(\sum_{k=0}^{n} a_k p^k\right)_{n \in \mathbb{N}}$$

eine Cauchy-Folge bzgl. $|\cdot|_p$, denn für $m > n$ gilt

$$\left|\sum_{k=0}^{m} a_k p^k - \sum_{k=0}^{n} a_k p^k\right|_p = \left|\sum_{k=n+1}^{m} a_k p^k\right|_p = |p|_p^{n+1} \left|\sum_{k=n+1}^{m} a_k p^{k-n-1}\right|_p \leq |p|_p^{n+1} = \frac{1}{p^{n+1}},$$

also existiert der Grenzwert

$$\sum_{k=0}^{\infty} a_k p^k = \lim_{n \to \infty} \left(\sum_{k=0}^{n} a_k p^k\right)$$

in $\mathbb{Q}_p$.

Man erhält dann

$$\mathbb{Q}_p = \{\sum_{k=k_0}^{\infty} a_k p^k : a_k \in \{0, 1, \ldots, p-1\}, k_0 \in \mathbb{Z}\}.$$

(Die p-adische Entwicklung $\alpha = \sum_{k=k_0}^{\infty} a_k p^k$ einer Zahl $\alpha \in \mathbb{Q}_p$ ist eindeutig bestimmt.)
SAGE stellt mit `K=Qp(p)` den Körper $\mathbb{Q}_p$ bereit, mit `K(a)` erhält man die p-adische Entwicklung einer Zahl. Beispielsweise liefern `K=Qp(7)` und `K(37/35)` die 7-adische Entwicklung von $\frac{37}{35}$:

$$\frac{37}{35} = 6 \cdot 7^{-1} + 3 + 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + 2 \cdot 7^4 + 7^5 + 4 \cdot 7^6 + 5 \cdot 7^7 + 2 \cdot 7^8 + 7^9 + 4 \cdot 7^{10} + 5 \cdot 7^{11} + 2 \cdot 7^{12} + 7^{13} + 4 \cdot 7^{14} + 5 \cdot 7^{15} + 2 \cdot 7^{16} + 7^{17} + 4 \cdot 7^{18} + O(7^{19})$$

Die Menge der **ganzen p-adischen Zahlen** ist

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

$\mathbb{Z}_p$ ist ein diskreter Bewertungsring mit der Bewertung $v_p(a)$, sodass gilt

$$|a|_p = p^{-v_p(a)}.$$

$\mathbb{Z}$ ist eine dichte Teilmenge von $\mathbb{Z}_p$ und es gilt

$$\mathbb{Z}_p = \{\sum_{k=0}^{\infty} a_k p^k : a_k \in \{0, 1, \ldots, p-1\}\}.$$

Man kann modulo p^n rechnen:

$$\sum_{k=0}^{\infty} a_k p^k \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \bmod p^n.$$

Will man in $\mathbb{R}$ eine Gleichung $f(x) = 0$ lösen, so besteht die Idee des **Newton-Verfahrens** darin, mit einer Näherungslösung x_0, d.h. $f(x_0) \approx 0$, zu beginnen, dann den Schnittpunkt der Tangente des Graphen

von f in x_0 mit der x-Achse als neuen Näherungswert x_1 zu verwenden, und dieses dann zu iterieren [**Forster1**, S.199-203].

Die gleiche Idee kann man auch in $\mathbb{Q}_p$ bzw. $\mathbb{Z}_p$ verwenden. Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom in einer Veränderlichen. Für $x_0 \in \mathbb{Z}$ gilt:

$$f(x_0) \equiv 0 \bmod p^n \iff p^n \mid f(x_0) \iff \frac{f(x_0)}{p^n} \in \mathbb{Z} \iff$$
$$\iff \left|\frac{f(x_0)}{p^n}\right|_p \leq 1 \iff |f(x_0)|_p \leq |p|_p^n = \frac{1}{p^n}.$$

Eine Lösung der Gleichung $f(x) = 0$ modulo p^n approximiert also eine p-adische Nullstelle von $f(x)$. Dies lässt sich auch präzisieren. Beispielsweise gilt folgender Satz:

SATZ. *Ist $f(x) \in \mathbb{Z}[x]$ und $x_0 \in \mathbb{Z}$ mit*

$$f(x_0) \equiv 0 \bmod p \quad \textit{und} \quad v_p(f'(x_0)) = 0,$$

so existiert eine Zahl $\widetilde{x} \in \mathbb{Z}_p$ mit $f(\widetilde{x}) = 0$ und es gilt $\widetilde{x} \equiv x_0 \bmod p$. Die angegebenen Bedingungen lassen sich auch in der Form

$$|f(x_0)|_p < 1 \quad \textit{und} \quad |f'(x_0)|_p = 1$$

schreiben.

Genaueres findet sich bei [**Serre**, S.14-15]. Aussagen dieser Art sind auch unter dem Namen **Hensels Lemma** bekannt.

5. Kurven vom Geschlecht 0 über $\mathbb{Q}$ - Hilbert-Symbol

LEMMA. *Wird die ebene projektive Quadrik C über $\mathbb{Q}$ definiert durch $f = b_0x_0^2+b_1x_1^2+b_2x_2^2$, sind b_0, b_1, b_2 paarweise teilerfremde, quadratfreie, ganze Zahlen, ist p eine ungerade Primzahl mit*

$$p \mid b_0 \quad \textit{und} \quad \left(\frac{-b_1b_2}{p}\right) = -1,$$

so gilt

$$C(\mathbb{Q}_p) = \emptyset.$$

Beweis: Angenommen, es gibt $(y_0, y_1, y_2) \in \mathbb{Q}_p^3 \setminus \{(0,0,0)\}$ mit $f(y_0, y_1, y_2) = 0$. Nach Multiplikation oder Division mit einer geeigneten Potenz von p können wir

$$(y_0, y_1, y_2) \in \mathbb{Z}_p^3 \quad \text{und} \quad \min(v_p(y_0), v_p(y_1), v_p(y_2)) = 0$$

annehmen. Aus $b_0y_0^2 + b_1y_1^2 + b_2y_2^2 = 0$ folgt mit $p \mid b_0$ modulo p

$$b_1y_1^2 + b_2y_2^2 \equiv 0 \bmod p,$$

und damit

$$(b_2y_2)^2 \equiv -b_1b_2y_1^2 \bmod p.$$

Wegen $\left(\frac{-b_1b_2}{p}\right) = -1$ muss $y_1 \equiv 0 \bmod p$ gelten. Mit $p \mid b_0$ folgt dann aus der ursprünglichen Gleichung $p \mid y_2$, und damit

$$p^2 \mid b_1y_1^2 + b_2y_2^2, \quad \text{also} \quad p^2 \mid b_0y_0^2.$$

Da p die Zahl b_0 nur einmal teilt, folgt $p \mid y_0$. Damit erhält man den Widerspruch $\min(v_p(y_0), v_p(y_1), v_p(y_2)) \geq 1$. Die Annahme ist also falsch, es folgt die Behauptung. ■

LEMMA. *Eine ebene projektive Quadrik C werde gegeben durch $f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2$ mit ganzen, quadratfreien, paarweise teilerfremden Zahlen $b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}$. Sei p eine ungerade Primzahl. Gilt*

$$p \nmid b_0b_1b_2 \quad \textit{oder} \quad \left(p \mid b_0 \textit{ und } \left(\frac{-b_1b_2}{p}\right) = 1\right),$$

so ist

$$C(\mathbb{Q}_p) \neq \emptyset.$$

Beweis: Betrachten wir das Polynom f modulo p, so erhalten wir eine Kurve $\overline{C}$ über $\mathbb{F}_p$. Im Fall $p \nmid b_0b_1b_2$ ist die Kurve nichtsingulär und es gilt $\#\overline{C}(\mathbb{F}_p) = p+1$, im Fall $p \mid b_0$ und $\left(\frac{-b_1b_2}{p}\right) = 1$ zerfällt $\overline{C}$ über $\mathbb{F}_p$ in zwei Geraden und $\#\overline{C}(\mathbb{F}_p) = 2p+1$, insbesondere gibt es auch hier über $\mathbb{F}_p$ definierte nichtsinguläre Punkte. In jedem Fall finden wir also $(y_0, y_1, y_2) \in \mathbb{Z}^3 \subseteq \mathbb{Z}_p^3$ mit

$$f(y_0, y_1, y_2) \equiv 0 \bmod p \quad \text{und} \quad (\frac{\partial f}{\partial x_0}(y_0, y_1, y_2), \frac{\partial f}{\partial x_1}(y_0, y_1, y_2), \frac{\partial f}{\partial x_2}(y_0, y_1, y_2)) \not\equiv (0,0,0) \bmod p.$$

Nach [**Serre**, S.14, Theorem 1] gibt es dann Zahlen $\widetilde{y}_0, \widetilde{y}_1, \widetilde{y}_2 \in \mathbb{Z}_p$ mit

$$f(\widetilde{y}_0, \widetilde{y}_1, \widetilde{y}_2) = 0 \quad \text{und} \quad \widetilde{y}_i \equiv y_i \bmod p \text{ für } i = 0,1,2.$$

Dann ist $(\widetilde{y}_0 : \widetilde{y}_1 : \widetilde{y}_2) \in C(\mathbb{Q}_p)$ und die Behauptung folgt. ■

Bemerkung: [**Serre**, S.14, Theorem 1] enthält leider den Schreibfehler $0 < 2k < n$. In der französischen Aussage [**Serre 1970**, S.28-29, Théorème 1] steht richtig $0 \leq 2k < n$.

Damit können wir den Satz von Legendre nun umformulieren:

Satz (Satz von Legendre, 2. Version). *Sei C eine absolut irreduzible, nichtsinguläre, projektive, ebene Quadrik, die über $\mathbb{Q}$ definiert ist. Dann gilt:*

$$C(\mathbb{Q}) \neq \emptyset \quad \Longleftrightarrow \quad C(\mathbb{R}) \neq \emptyset \text{ und } C(\mathbb{Q}_p) \neq \emptyset \text{ für alle ungeraden Primzahlen } p.$$

Erstaunlicherweise wird im vorangegangenen Satz die Primzahl 2 nicht erwähnt.

Das Hilbert-Symbol [**Serre**, S.19-26, Chapter III]. Im Folgenden schreiben wir $\mathbb{Q}_\infty$ für $\mathbb{R}$. Für $v = \infty$ oder $v = p$ und $a, b \in \mathbb{Q}_v^*$ wird das **Hilbert-Symbol** $(a,b)_v$ von a, b bezüglich $\mathbb{Q}_v$ definiert durch

$$(a,b)_v = \begin{cases} 1, & \text{falls } ax^2 + by^2 = z^2 \text{ hat eine Lösung } (x,y,z) \in \mathbb{Q}_v^3 \setminus \{(0,0,0)\}, \\ -1 & \text{sonst.} \end{cases}$$

Man kann das Hilbert-Symbol ausrechnen [**Serre**, S.20, Theorem 1]:

Satz. (1) *Für $a, b \in \mathbb{R}^*$ gilt*

$$(a,b)_\infty = \begin{cases} 1, & \text{falls } a > 0 \text{ oder } b > 0, \\ -1, & \text{falls } a < 0 \text{ und } b < 0. \end{cases}$$

(2) *Seien $a, b \in \mathbb{Q}_p^*$. Zerlegt man*

$$a = p^\alpha u, \quad b = p^\beta v \quad \text{mit} \quad v_p(u) = v_p(v) = 0,$$

so gilt im Fall $p > 2$ (mit den Legendre-Symbolen $\left(\frac{u}{p}\right)$ und $\left(\frac{v}{p}\right)$)

$$(a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$$

und im Fall $p = 2$

$$(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}.$$

Dabei sind ε und ω die Funktionen

$$\varepsilon(u) = \frac{u-1}{2} \bmod 2 \quad \text{und} \quad \omega(u) = \frac{u^2-1}{8} \bmod 2.$$

Bemerkung: Für $a, b \in \mathbb{Q}^*$ gilt für eine ungerade Primzahl p

$$(a,b)_p = 1, \text{ falls } v_p(a) = v_p(b) = 0 \text{ ist.}$$

Da in der Primfaktorzerlegung von a und b nur endlich viele Primzahlen vorkommen, ist

$$\{p \text{ Primzahl} : (a,b)_p = -1\}$$

eine endliche Menge.

Bemerkung: SAGE berechnet das Hilbert-Symbol $(a,b)_p$ mit dem Befehl `hilbert_symbol(a,b,p)`, das Hilbert-Symbol $(a,b)_\infty$ mit dem Befehl `hilbert_symbol(a,b,-1)`.

Bemerkung: Jede über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadrik C kann nach Koordinatenwechsel über $\mathbb{Q}$ durch eine Gleichung der Form

$$f = ax_0^2 + bx_1^2 - x_2^2$$

beschrieben werden. Dann gilt also

$$C(\mathbb{Q}_p) = \emptyset \quad \Longleftrightarrow \quad (a,b)_p = -1.$$

Beispiele: Wir betrachten eine nichtsinguläre Quadrik C über $\mathbb{Q}$, die durch ein Polynom $f = b_0x_0^2 + b_1x_1^2 + b_2x^2$ gegeben ist mit $b_0, b_1, b_2 \in \mathbb{Z} \setminus \{0\}$, quadratfrei, paarweise teilerfremd. Es gilt:

$$b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = 0 \quad \Longleftrightarrow \quad -b_0b_2x_0^2 - b_1b_2x_1^2 = (b_2x_2)^2,$$

die Quadrik lässt sich also auch durch

$$(-b_0b_2)x^2 + (-b_1b_2)y^2 = z^2$$

beschreiben. Wir betrachten daher für eine ungerade Primzahl p das Hilbert-Symbol

$$(-b_0b_2, -b_1b_2)_p.$$

(1) **Fall $p \nmid b_0b_1b_2$:** Aus $v_p(-b_0b_2) = v_p(-b_1b_2) = 0$ folgt sofort

$$(-b_0b_2, -b_1b_2)_p = 1.$$

(2) **Fall $p \mid b_0b_1b_2$:** O.E. betrachten wir den Fall $p \mid b_0$. Wir zerlegen

$$-b_0b_2 = p^1u, \quad -b_1b_2 = p^0v, \quad \text{also} \quad \alpha = 1, \quad \beta = 0.$$

Wegen $\beta = 0$ und $\alpha = 1$ erhalten wir

$$(-b_0b_2, -b_1b_2)_p = \left(\frac{-b_1b_2}{p}\right).$$

Dieses Legendre-Symbol mussten wir im Satz von Legendre betrachten.

Für das globale Verhalten ist folgender Satz wichtig [**Serre**, S.23, Theorem 3 (Hilbert)]:

Satz (Produktformel für das Hilbert-Symbol). *Sind $a, b \in \mathbb{Q}^*$, so gilt $(a,b)_p = 1$ für fast alle Primzahlen und*

$$(a,b)_\infty \cdot \prod_p (a,b)_p = 1.$$

Bemerkungen:

(1) Aus der Produktformel für das Hilbert-Symbol folgt

$$(a,b)_2 = (a,b)_\infty \cdot \prod_{p \neq 2} (a,b)_p.$$

Dies erklärt, warum wir beim Satz von Legendre die Primzahl 2 nicht gebraucht haben.

(2) Wir können die Produktformel auch nach $(a,b)_\infty$ auflösen:

$$(a,b)_\infty = \prod_p (a,b)_p.$$

Für eine über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadrik C definieren wir

$$\Psi(C) = \{p \text{ Primzahl} : C(\mathbb{Q}_p) = \emptyset\}.$$

Wird C durch eine Gleichung $ax_0^2 + bx_1^2 = x_2^2$ beschrieben, so ist also

$$\Psi(C) = \{p \text{ Primzahl} : (a,b)_p = -1\}.$$

Wegen der Produktformel für das Hilbert-Symbol folgt dann

$$C(\mathbb{R}) \begin{cases} \neq \emptyset, & \text{falls } \#\Psi(C) \text{ gerade,} \\ = \emptyset, & \text{falls } \#\Psi(C) \text{ ungerade.} \end{cases}$$

Wir können nun den Satz von Legendre auch so formulieren:

$$C(\mathbb{Q}) \neq \emptyset \quad \Longleftrightarrow \quad \Psi(C) = \emptyset.$$

Bemerkung: SAGE berechnet für eine nichtsinguläre Quadrik C der Form $ax_0^2 + bx_1^2 - x_2^2$ das Produkt

$$\prod_{p \in \Psi(C)} p$$

mit dem Befehl `hilbert_conductor(a,b)`.

Satz. *Zwei über $\mathbb{Q}$ definierte nichtsinguläre projektive ebene Quadriken C_1 und C_2 sind genau dann isomorph über $\mathbb{Q}$, wenn gilt $\Psi(C_1) = \Psi(C_2)$.*

Leider kenne ich keinen direkten Beweis dieses Satzes. Ein Beweis benutzt Quaternionenalgebren. (Der Zusammenhang zwischen Kegelschnitten und Quaternionenalgebren wird in [**Gille-Szamuely**, Abschnitte 1.3 (The associated conic) und 1.4 (A Theorem of Witt)] behandelt.)

Beispiele: Wir haben zufällig $a_0, \ldots, a_5 \in \mathbb{Z}$ (mit $|a_i| \leq 10$) gewählt, dazu die durch $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ definierte Quadrik C betrachtet - nur im nichtsingulären Fall -, die Quadrik zu $ax_0^2 + bx_1^2 = x_2^2$ diagonalisiert und dann $\Psi(C)$ berechnet:

$(a_0, a_1, a_2, a_3, a_4, a_5)$	(a, b)	$\Psi(C)$
$(-7, -6, 7, -9, 1, -3)$	$(-21, -14)$	$\{2\}$
$(5, -9, 7, -2, 8, 5)$	$(-55, 55)$	$\emptyset$
$(0, 0, -4, 1, 0, -9)$	$(-1, 1)$	$\emptyset$
$(-2, -9, -10, 6, 2, -7)$	$(-126678, 982)$	$\emptyset$
$(3, -2, 3, 6, 7, -4)$	$(26265, 1545)$	$\{5, 103\}$
$(-1, 10, 0, 0, 0, -8)$	$(-2, 2)$	$\emptyset$
$(-6, -5, 8, 4, 5, -8)$	$(-993, 993)$	$\emptyset$
$(8, 4, 10, 9, -9, 9)$	$(-510, -30)$	$\{5\}$
$(-2, 10, 2, -6, 4, 9)$	$(2158, -166)$	$\{2, 83\}$
$(-8, -5, -5, 6, -9, -1)$	$(-1085, 5)$	$\{5, 7\}$
$(2, -10, -8, -6, 0, -7)$	$(26270, -710)$	$\{2, 5\}$
$(7, 1, -2, 10, -5, 6)$	$(-318773, -10283)$	$\{13\}$
$(-1, -7, 9, 2, 5, -5)$	$(9519, -167)$	$\emptyset$
$(2, -5, 9, 7, -8, -4)$	$(3162, 102)$	$\{17, 3\}$
$(-7, 8, -5, 10, 5, -1)$	$(-41538, 483)$	$\{3, 23\}$
$(7, 9, -1, -2, -2, 7)$	$(-927353, 6769)$	$\emptyset$
$(7, 1, -5, 2, -10, -6)$	$(15862, 7210)$	$\{5, 103\}$
$(8, 1, 10, -2, -9, -4)$	$(-9035, 139)$	$\emptyset$
$(10, 1, -8, 5, 7, 4)$	$(1393, 7)$	$\emptyset$

$(a_0, a_1, a_2, a_3, a_4, a_5)$	(a, b)	$\Psi(C)$
$(8, 3, 10, -3, -5, 2)$	$(-546, 130)$	$\emptyset$
$(-3, 6, 8, -10, -4, 0)$	$(217, 93)$	$\emptyset$
$(9, -2, 6, 6, 8, -2)$	$(4346, 82)$	$\{41, 2\}$
$(-10, -3, 9, 5, 8, -7)$	$(-2145, 3705)$	$\{19, 3\}$
$(-8, -1, -4, 3, -2, 3)$	$(6790, -70)$	$\{5, 7\}$
$(-6, 0, 2, 8, -4, -5)$	$(-2, 6)$	$\emptyset$
$(4, 9, -10, 10, -1, 6)$	$(8690, 110)$	$\emptyset$
$(-3, -7, -9, 9, 9, 10)$	$(701319, -4467)$	$\emptyset$
$(-10, -6, 1, 3, 2, 5)$	$(11778, -302)$	$\emptyset$
$(-4, 1, -4, 6, -9, 4)$	$(3007, -31)$	$\emptyset$
$(5, 4, -2, 2, 7, -9)$	$(70, 105)$	$\emptyset$
$(-8, 5, 2, 7, 7, 10)$	$(63993, -257)$	$\emptyset$
$(-8, -8, 5, 10, -3, 10)$	$(11694, -1949)$	$\emptyset$
$(1, -4, 9, 4, 4, -7)$	$(-109, 1)$	$\emptyset$
$(-9, 9, 2, -8, -2, -1)$	$(-161, -7)$	$\{7\}$
$(5, -6, -1, -6, 7, 8)$	$(-39, 1)$	$\emptyset$
$(10, -7, 3, -4, -6, 6)$	$(-6270, 30)$	$\{11, 3\}$
$(-1, 0, 1, 4, 6, -3)$	$(-5, 5)$	$\emptyset$
$(0, -5, 3, 1, -10, 2)$	$(91, -91)$	$\emptyset$
$(-2, -4, 3, 1, -1, -9)$	$(-663, 442)$	$\{17, 13\}$
$(4, -5, 9, 2, -9, 8)$	$(7, 1)$	$\emptyset$
$(-7, -5, 8, 9, 2, 4)$	$(17174, -62)$	$\{2, 31\}$
$(-4, -2, 5, -9, 2, 5)$	$(32235, 921)$	$\emptyset$
$(10, 8, -6, 9, 6, -1)$	$(58645, 3170)$	$\{2, 317\}$
$(7, 1, 2, 3, -5, -1)$	$(830, 10)$	$\{2, 5\}$
$(7, 1, 4, -1, 2, 9)$	$(-53795, 1855)$	$\emptyset$
$(1, 8, 3, -1, -6, 5)$	$(-8687, 511)$	$\{73, 7\}$
$(2, -4, -3, 3, -7, -8)$	$(273, 546)$	$\{13, 7\}$
$(5, -3, -1, 0, -10, 0)$	$(-106, 106)$	$\emptyset$
$(7, 4, 8, 8, 1, -1)$	$(63245, 4865)$	$\{139, 5\}$
$(8, 3, -8, -4, -9, 4)$	$(-49594, 362)$	$\emptyset$

Bei den Beispielen fällt auf, dass die Fälle mit $\psi(C) = \emptyset$ recht häufig sind. (Dies sind genau die Fälle mit $C(\mathbb{Q}) \neq \emptyset$.)

Bemerkungen:

(1) $\Psi(C)$ ist eine endliche Menge von Primzahlen. Man kann umgekehrt zeigen, dass es zu jeder endlichen Menge $\widetilde{P}$ von Primzahlen eine Kurve C mit $\Psi(C) = \widetilde{P}$ gibt.

(2) Ist $\widetilde{P} = \{p_1, \ldots, p_r\}$ eine endliche Menge von Primzahlen, setzt man $d = p_1 \ldots p_r$ so liefert der SAGE-Befehl `hilbert_conductor_inverse(d)` ein Zahlenpaar $(a, b) \in \mathbb{Z}^2$, sodass für die durch $ax_0^2 + bx_1^2 = x_2^2$ definierte Kurve C gilt $\Psi(C) = \widetilde{P}$. Beispielsweise erhält man für $\widetilde{P} = \{2, 3, 5, 7, 11\}$ die Kurve $-22x_0^2 + 210x_1^2 = x_2^2$.

(3) Die $\mathbb{Q}$-Isomorphieklassen der über $\mathbb{Q}$ definierten, absolut irreduziblen, nichtsingulären, projektiven Kurven vom Geschlecht 0 stehen also in Bijektion zu den endlichen Teilmengen der Menge der Primzahlen.

Bemerkung: Sind C_1, C_2 zwei nichtsinguläre ebene Quadriken mit $\Psi(C_1) = \Psi(C_2)$, so gibt es also einen über $\mathbb{Q}$ definierten Koordinatenwechsel, der C_1 in C_2 überführt. Wie findet man einen solchen?
Hier ist eine (nicht ganz ausgereifte) Idee:

(1) Wir transformieren C_1 auf eine Gleichung $ax_0^2 + bx_1^2 - abx_2^2 = 0$ und C_2 auf eine Gleichung $\widetilde{a}y_0^2 - \widetilde{y}_1^2 - \widetilde{a}\widetilde{b}y_2^2 = 0$.

(2) Die Zahlen $a, b \in \mathbb{Q}^*$ definieren die Quaternionen-Algebra $Q(a, b)$ mit $\mathbb{Q}$-Basis $1, i, j, k$, d.h.

$$Q(a, b) = \mathbb{Q} \cdot 1 + \mathbb{Q} \cdot i + \mathbb{Q} \cdot j + \mathbb{Q} \cdot k,$$

wobei gilt

$$i^2 = a, \quad j^2 = b, \quad ji = -ij, \quad k = ij, \quad k^2 = -ab.$$

(3) Da C_1 über $\mathbb{Q}$ isomorph zu C_2 sein sollte, sind nach dem Satz von Witt [**Gille-Szamuely**, Theorem 1.4.2 (Witt)] die Quaternionenalgebren $Q(a,b)$ und $Q(\widetilde{a},\widetilde{b})$ isomorph. Es sollte also Elemente $\widetilde{i},\widetilde{j} \in Q(a,b)$ geben mit

$$\widetilde{i}^2 = \widetilde{a}, \quad \widetilde{j}^2 = \widetilde{b}, \quad \widetilde{j}\widetilde{i} = -\widetilde{i}\widetilde{j}.$$

Wir setzen dann

$$\widetilde{k} = \widetilde{i}\widetilde{j}.$$

(Es folgt $\widetilde{k}^2 = -\widetilde{a}\widetilde{b}$.) Dann gibt es $a_{ij} \in \mathbb{Q}$ mit

$$\begin{pmatrix} \widetilde{i} \\ \widetilde{j} \\ \widetilde{k} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} i \\ j \\ k \end{pmatrix}.$$

(4) Definieren wir einen Koordinatenwechsel durch

$$\begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} = \begin{pmatrix} y_0 & y_1 & y_2 \end{pmatrix} \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix},$$

so gilt

$$ax_0^2 + bx_1^2 - abx_2^2 = \widetilde{a}y_0^2 + \widetilde{b}y_1^2 - \widetilde{a}\widetilde{b}y_2^2,$$

wie man durch Einsetzen nachrechnen kann. Damit haben einen gesuchten Isomorphismus gefunden. (Natürlich bleibt die Frage, wie man $\widetilde{i},\widetilde{j}$ praktisch finden kann.)

KAPITEL 12

Kurven vom Geschlecht 1 — elliptische Kurven

1. Einführung

Sofern nichts anderes gesagt, verstehen wir unter einer Kurve immer eine über dem Grundkörper K definierte, absolut irreduzible, nichtsinguläre, projektive Kurve.

Beispiel: Ist $C \subseteq \mathbb{P}^2$ eine nichtsinguläre Kubik,

$$C = \{a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + \cdots + a_9x_2^3 = 0\},$$

so hat C Geschlecht $g = \frac{(3-1)(3-2)}{2} = 1$.

Was können wir allgemein über eine Kurve C vom Geschlecht $g = 1$ sagen?

(1) Für kanonische Divisoren gilt: $\operatorname{grad}(K_C) = 2g-2 = 0$ und $\ell(K_C) = g = 1$. Sei $f \in \mathcal{L}(K_C) \setminus \{0\}$. Dann gilt $K_C + \operatorname{div}(f) \geq 0$. Wegen $\operatorname{grad}(K_C + \operatorname{div}(f)) = \operatorname{grad}(K_C) = 0$ gilt bereits $K_C + \operatorname{div}(f) = 0$, also ist auch der triviale Divisor 0 kanonisch. Der einzige effektive kanonische Divisor ist also der Divsor 0. Wir können also stets $K_C = 0$ annehmen.

(2) Der Satz von Riemann-Roch wird dann zu

$$\ell(D) = \operatorname{grad}(D) + \ell(-D).$$

Insbesondere folgt

$$\ell(D) = \operatorname{grad}(D) \quad \text{für } \operatorname{grad}(D) \geq 1.$$

(3) Wie kann man C als projektive Kurve realisieren? Im Fall $g(C) = 0$ war $C \simeq \phi_{-K_C}(C) \subseteq \mathbb{P}^2$ eine ebene Quadrik. Im Fall $g(C) = 1$ haben wir leider keinen natürlichen über K definierten Divisor zur Verfügung. (Ich weiß keine Antwort auf diese Frage. Wichtige Ausnahme: Kurven vom Geschlecht 1 über einem endlichen Körper)

Es gibt Kurven vom Geschlecht 1 über $\mathbb{Q}$, die keine $\mathbb{Q}$-rationalen Punkt besitzen, wie folgendes Beispiel zeigt.

Beispiel: Sei $\alpha \in \mathbb{F}_8$ mit $\alpha^3 + \alpha + 1 = 0$. Es ist $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$. Wir betrachten über $\mathbb{F}_2$ ($x \mapsto x^2$ ist der Frobeniusautomorphismus, $x \mapsto x^2$ und $x \mapsto x^4$ also die nichttrivialen Elemente der Galoisgruppe):

$$f = (x_0 + \alpha x_1 + \alpha^2 x_2)(x_0 + \alpha^2 x_1 + \alpha^4 x_2)(x_0 + \alpha^4 x_1 + \alpha^8 x_2).$$

Ausmultiplizieren liefert

$$f = x_0^3 + x_0x_1^2 + x_0x_1x_2 + x_0x_2^2 + x_1^3 + x_1x_2^2 + x_2^3.$$

$\{f = 0\} \subseteq \mathbb{P}^2$ besteht aus 3 Geraden, die nicht durch einen Punkt gehen, hat also keinen $\mathbb{F}_2$-rationalen Punkt.
Wir definieren jetzt über $\mathbb{Q}$:

$$F = x_0^3 + x_0x_1^2 + x_0x_1x_2 + x_0x_2^2 + x_1^3 + x_1x_2^2 + x_2^3 \in \mathbb{Q}[x_0, x_1, x_2]$$

und $C = \{F = 0\} \subseteq \mathbb{P}^2$. Man rechnet nach, dass C nichtsingulär ist. Da F modulo 2 keine nichttrivialen Nullstellen hat, hat C keine $\mathbb{Q}$-rationalen Punkte, wie man durch Reduktion modulo 2 sieht.

Datei: algku12.tex. Version vom 18.7.2021

Bemerkung: Ist C eine über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 1, so gilt folgende Abschätzung von Hasse [**HKT**, S.343, Theorem 9.18 (Hasse-Weil Bound)] oder [**Luetkebohmert**, S.162, Satz 7.4.1 (Weil-Schranke)]:

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

Daraus folgt sofort

$$\#C(\mathbb{F}_p) \neq \emptyset.$$

Wir betrachten jetzt Kurven vom Geschlecht 1 mit einem K-rationalen Punkt.

2. Elliptische Kurven

DEFINITION. *Eine* **elliptische Kurve** *E über K ist eine (absolut irreduzible, nichtsinguläre, projektive) Kurve vom Geschlecht 1 zusammen mit einem Punkt $O \in E(K)$.*

Da wir jetzt bei elliptischen Kurven nichttriviale, über K definierte Divisoren kennen, können wir sie als projektive Kurven realisieren:

SATZ. *Sei (E, O) eine elliptische Kurve über K. Dann ist E über K isomorph zu einer ebenen Kubik der Gestalt*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

mit $a_i \in K$, wobei O dem Punkt $(0:0:1)$ entspricht. Eine solche Gleichung nennt man auch eine **Weierstraßgleichung** *für E.*

Beweis:

- Wir wissen, dass ein ein Divisor D mit $\operatorname{grad}(D) \geq 2g+1 = 3$ sehr ampel ist, d.h. ϕ_D liefert eine Einbettung von C als Kurve vom Grad $\operatorname{grad}(D)$ in $\mathbb{P}^{\ell(D)-1}$. Wir wählen den über K definierten Divisor $D = 3 \cdot [O]$. Riemann-Roch liefert $\ell(3 \cdot [O]) = 3$, also erhalten wir
$$E \simeq \phi_{3[O]}(E) \subseteq \mathbb{P}^2$$
als Kurve vom Grad 3 im $\mathbb{P}^2$.
- Wie sieht $\phi_{3[O]}$ aus? Riemann-Roch liefert $\ell(n[O]) = n$ für $n \geq 1$. Sei t uniformisierend in O, d.h. $\operatorname{ord}_O(t) = 1$. Wir beschreiben jetzt die Vektorräume $\mathcal{L}(n[O])$:
- Natürlich ist $\mathcal{L}([O]) = \overline{K} \cdot 1$.
- Wegen $\ell(2[O]) = 2$ gibt es ein $x \in K(E)$ mit $\mathcal{L}(2[O]) = \overline{K} + \overline{K} \cdot x$. Wegen $x \notin \mathcal{L}([O])$ ist $\operatorname{ord}_O(x) = -2$ und wir können nach Multiplikation mit einer Konstanten $(t^2x)([O]) = 1$ erreichen.
- Analog erhält man ein $y \in K(E)$ mit $\mathcal{L}(3[O]) = \overline{K} + \overline{K}x + \overline{K}y$. Die Funktion y erfüllt $\operatorname{ord}_O(y) = -3$, also können wir wieder o.E. $(t^3y)(O) = 1$ annehmen. x und y haben außer in O keine Polstelle.
- Wir definieren jetzt $\phi = \phi_{3[O]} = (1 : x : y)$. Was ist $\phi(O)$? Es ist $\phi = (t^3 : t(t^2x) : t^3y)$, also wegen $t(O) = 0$:
$$\phi(O) = (0:0:1).$$
$\phi(E)$ ist eine zu E isomorphe ebene Kurve vom Grad 3. Wir brauchen jetzt nur noch eine nichttriviale Relation zwischen $1, x, y$ um die Kurvengleichung zu erhalten.
- Es gilt weiter
$$\mathcal{L}(4[O]) = \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2, \quad \mathcal{L}(5[O]) = \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy,$$
$$\mathcal{L}(6[O]) = \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy + \overline{K}x^3.$$
Nun ist $y^2 \in \mathcal{L}(6[O]) \setminus \mathcal{L}(5[O])$, also gibt es $a_1, a_2, a_3, a_4, a_6, c \in K$, $c \neq 0$ mit
$$y^2 = cx^3 + a_2x^2 + a_4x + a_6 - a_1xy - a_3y.$$
Multipliziert man mit t^6 und setzt dann O ein, so erhält man
$$(t^3y)^2(O) = c(t^2x)^3(O) + 0,$$

also $c = 1$. Damit haben wir

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Dieser Gleichung genügt dann auch $\phi(E)$ in $\mathbb{P}^2$, was wir noch zeigen wollten. ■

Beispiel: Wir betrachten über $\mathbb{F}_{13}$ die durch

$$f = x_0^3 + 2x_1^3 + 4x_2^3$$

definierte ebene Kubik. Sie ist nichtsingulär und hat deswegen Geschlecht 1. Wir betrachten den Punkt $P = (1 : 2 : 4)$. Mit SAGE erhalten wir

$$\begin{aligned}
\mathcal{L}(2[P]) &= \left[\frac{4x_0 + 8x_1}{5x_0 + x_1 + 8x_2}, \frac{3x_0 + x_2}{-x_0 + 5x_1 + x_2}\right], \\
\mathcal{L}(3[P]) &= \left[\frac{6x_0^3 + x_0^2x_1 + 10x_0x_1^2 + x_1^3 + 8x_0^2x_2 + x_0x_1x_2 - x_0x_2^2}{9x_0^3 - x_0^2x_1 + x_1x_2^2}, \frac{x_0^3 + x_0^2x_1 + 5x_0x_1^2 + 3x_0^2x_2 + 9x_0x_1x_2 + x_1^2x_2 + 10x_0x_2^2}{9x_0^3 - x_0^2x_1 + x_1x_2^2}, 1\right]
\end{aligned}$$

Wir schreiben dies mit $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$:

$$\begin{aligned}
\mathcal{L}(2[P]) &= \left[\frac{8x + 4}{x + 8y + 5}, \frac{y + 3}{5x + y + 12}\right], \\
\mathcal{L}(3[P]) &= \left[\frac{x^3 + 10x^2 + xy - y^2 + x + 8y + 6}{xy^2 - x + 9}, \frac{x^2y + 5x^2 + 9xy + 10y^2 + x + 3y + 1}{xy^2 - x + 9}, 1\right]
\end{aligned}$$

Wir lösen die Gleichung $f(1, x, y) = 0$ in $F_{13}[[t]]$ im Punkt $P = (2, 4)$ wie zuvor erläutert:

$$\begin{aligned}
x &= 2 + t, \\
y &= 4 + 8t + t^2 + 12t^3 + 3t^4 + 5t^5 + 4t^7 + 8t^8 + 7t^9 + 2t^{10} + 10t^{11} + 9t^{12} + 8t^{14} + 8t^{15} + t^{16} + t^{17} + \\
&\quad +9t^{18} + 6t^{19} + 5t^{20} + 3t^{21} + 10t^{22} + t^{23} + 3t^{25} + 7t^{26} + 3t^{27} + 9t^{28} + 7t^{29} + 2t^{30} + O(t^{31}).
\end{aligned}$$

Damit sehen die Funktionen in obigen Vektorräumen so aus:

$$\begin{aligned}
\mathcal{L}(2[P]) &= [\frac{9}{t^2} + \frac{10}{t} + 9 + 12t + 10t^4 + 9t^6 + 2t^7 + 4t^8 + 8t^9 + 10t^{10} + 3t^{11} + 10t^{12} + 11t^{13} + 7t^{15} + 2t^{16} + O(t^{18}), \\
&\quad \frac{7}{t^2} + \frac{2}{t} + 8 + 5t + 2t^4 + 7t^6 + 3t^7 + 6t^8 + 12t^9 + 2t^{10} + 11t^{11} + 2t^{12} + 10t^{13} + 4t^{15} + 3t^{16} + O(t^{18})], \\
\mathcal{L}(3[P]) &= [\frac{8}{t^3} + \frac{6}{t^2} + \frac{10}{t} + 12 + 11t + 2t^2 + 3t^4 + 8t^5 + t^6 + 2t^7 + 9t^8 + 2t^9 + t^{11} + 4t^{12} + 10t^{13} + 9t^{14} + 7t^{15} + 11t^{16} + O(t^{17}), \\
&\quad \frac{1}{t^3} + \frac{12}{t^2} + \frac{4}{t} + 1 + 5t + 10t^2 + 8t^4 + t^5 + 6t^7 + 11t^8 + 7t^9 + 6t^{10} + 12t^{11} + 2t^{13} + 6t^{14} + 8t^{15} + 12t^{16} + O(t^{17}), 1]
\end{aligned}$$

Sei X das erste Element aus $\mathcal{L}(2[P])$ dividiert durch 9, Y das erste Element aus $\mathcal{L}(3[P])$ dividiert durch 8:

$$\begin{aligned}
X &= \frac{1}{t^2} + \frac{4}{t} + 1 + 10t + 4t^4 + t^6 + 6t^7 + 12t^8 + 11t^9 + 4t^{10} + 9t^{11} + 4t^{12} + 7t^{13} + 8t^{15} + 6t^{16} + O(t^{18}), \\
Y &= \frac{1}{t^3} + \frac{4}{t^2} + \frac{11}{t} + 8 + 3t + 10t^2 + 2t^4 + t^5 + 5t^6 + 10t^7 + 6t^8 + 10t^9 + 5t^{11} + 7t^{12} + 11t^{13} + 6t^{14} + 9t^{15} + 3t^{16} + O(t^{17}).
\end{aligned}$$

Nun sind wir in der Situation wie im vorangegangenen Beweis zu den elliptischen Kurven. Es ist nicht schwer, eine Gleichung herzuleiten:

```
R.<t>=LaurentSeriesRing(GF(13))
X=t^-2 + 4*t^-1 + 1 + 10*t + 4*t^4 + t^6 + 6*t^7 + 12*t^8 + 11*t^9 + 4*t^10 + 9*t^11 + 4*t^12 + 7*t^13 +
Y=t^-3 + 4*t^-2 + 11*t^-1 + 8 + 3*t + 10*t^2 + 2*t^4 + t^5 + 5*t^6 + 10*t^7 + 6*t^8 + 10*t^9 + 5*t^11 +
```

Man findet:

$$Y^2 - X^3 - 9XY - 6X^2 - 11Y - 12X - 8 = O(t^{14}),$$

also

$$Y^2 - 9XY - 11Y = X^3 + 6X^2 + 12X + 8.$$

FOLGERUNG. *Ist* $\mathrm{char}(K) \neq 2,3$ *und* (E,O) *eine elliptische Kurve über* K*, so ist* E *isomorph zu einer ebenen Kurve*

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

mit $a, b \in K$*, wo* O *dem Punkt* $(0:0:1)$ *entspricht.*

Beweis: Wir können mit einer Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

starten. Das Ziel erreichen wir durch quadratische und kubische Ergänzung. Wir können auch einen Koordinatenwechsel ansetzen:

$$y = y' + Ax' + B, \quad x = x' + C.$$

Wählt man

$$A = -\frac{1}{2}a_1, \quad B = -\frac{1}{2}a_3 + \frac{1}{6}a_1a_2 + \frac{1}{24}a_1^3, \quad C = -\frac{1}{3}a_2 - \frac{1}{12}a_1^2,$$

so erhält man eine Gleichung $y'^2 = x'^3 + ax' + b$ der gewünschten Form. ■

Während für Kurven vom Geschlecht 0 die Picardgruppe Pic^0 trivial ist, gilt für Kurven vom Geschlecht 1 folgender Satz:

SATZ. *Sei* (E,O) *eine elliptische Kurve. Dann ist die Abbildung*

$$\psi : E \to \mathrm{Pic}^0(E), \quad P \mapsto \textit{Klasse von } [P] - [O]$$

eine Bijektion.

Beweis:

- ψ *ist surjektiv:* Sei D ein Divisor vom Grad 0. Dann hat $D + [O]$ Grad 1, nach Riemann-Roch ist $\ell(D + [O]) = 1$, also gibt es eine Funktion $f \in \overline{K}(E)^*$ mit $D + [O] + \mathrm{div}(f) \geq 0$. Der Divisor $D + [O] + \mathrm{div}(f)$ ist effektiv vom Grad 1, also ein Punkt: $D + [O] + \mathrm{div}(f) = [P]$. Damit gilt $D \sim [P] - [O]$, also Klasse von $D = \psi(P)$.
- ψ *ist injektiv:* Sei $\psi(P) = \psi(Q)$. D.h. $[P]-[O] \sim [Q]-[O]$, und damit auch $[P] \sim [Q]$. Es gibt also eine Funktion f mit $[P] = [Q] + \mathrm{div}(f)$ und damit $\mathrm{div}(f) = [P] - [Q]$. Also ist $f \in \mathcal{L}([Q]) = \overline{K}$ und damit $P = Q$. ■

Diese Bijektion erlaubt uns jetzt eine Gruppenstruktur auf (E,O) einzuführen:

DEFINITION. *Sei* (E,O) *eine elliptische Kurve und* $\psi : E \to \mathrm{Pic}^0(E), P \mapsto$ *Klasse von* $([P] - [O])$*. Für* P_1, P_2 *definieren wir*

$$P_1 \oplus P_2 = \psi^{-1}(\psi(P_1) + \psi(P_2)).$$

Dadurch wird E *zu einer abelschen Gruppe mit* O *als neutralem Element.*

Bemerkungen:

- Für $P, Q, R \in E$ gilt:

$$\begin{aligned} P \oplus Q = R \quad &\iff \quad \psi(P) + \psi(Q) = \psi(R) \\ &\iff \quad [P] - [O] + [Q] - [O] \sim [R] - [O] \\ &\iff \quad [P] + [Q] \sim [O] + [R] \iff [R] \sim [P] + [Q] - [O]. \end{aligned}$$

  Wie findet man also R? Der Divisor $[P] + [Q] - [O]$ hat Grad 1, also ist $\mathcal{L}([P] + [Q] - [O])$ 1-dimensional. Sei $\mathcal{L}([P] + [Q] - [O]) = \overline{K}f$. Dann ist $[P] + [Q] - [O] + \mathrm{div}(f)$ effektiv vom Grad 1, also ein Punkt, nämlich $[R]$.
- Aus der Überlegung eben folgt sofort, dass $E(K)$ abgeschlossen bzgl. $\oplus$ ist, also eine Untergruppe.
- Das inverse Element zu P ist durch die Gleichung $[P] + [P'] \sim 2[O]$ bestimmt.

Wir wollen für ebene Kubiken die Gruppenstruktur geometrisch deuten, wozu wir ein paar Aussagen über Geradenschnitte brauchen:

LEMMA. *Sei $E \subseteq \mathbb{P}^2$ eine nichtsinguläre Kurve vom Grad 3 und $H = \operatorname{div}(h)$ ein Geradenschnitt, insbesondere $\operatorname{grad}(H) = 3$. Dann gilt: Ist D ein effektiver Divisor, der linear äquivalent zu H ist, so ist D selbst schon ein Geradenschnitt, d.h. es gibt eine Gerade $g = b_0x_0 + b_1x_1 + b_2x_2 = 0$ mit $D = \operatorname{div}(g)$.*

Beweis: Nach Riemann-Roch gilt $\ell(H) = \operatorname{grad}(H) = 3$, also ist

$$\mathcal{L}(H) = \overline{K}\frac{x_0}{h} + \overline{K}\frac{x_1}{h} + \overline{K}\frac{x_2}{h}.$$

Wegen $D \sim H$ gibt es eine Funktion f mit $D = H + \operatorname{div}(f)$. Wegen $D \geq 0$ ist $f \in \mathcal{L}(H)$, also gibt es $b_0, b_1, b_2 \in \overline{K}$ mit

$$f = \frac{b_0x_0 + b_1x_1 + b_2x_2}{h},$$

woraus sofort $D = \operatorname{div}(b_0x_0 + b_1x_1 + b_2x_2)$ folgt. ■

Aufgabe: Zeige die analoge Aussage für alle nichtsingulären ebenen Kurven. Die entsprechende Eigenschaft wird auch lineare Normalität genannt.

Geometrische Deutung der Addition für nichtsinguläre ebene Kubiken: Sei $E = \{f = 0\} \subseteq \mathbb{P}^2$ eine nichtsinguläre Kurve vom Grad 3 und $O \in E(K)$. Wie kann man die oben definierte Addition beschreiben?

(1) Seien P und Q Punkte auf E. Dann gibt es eine eindeutig bestimmte Gerade $g = 0$ und einen weiteren Punkt $R' \in E$ mit

$$[P] + [Q] + [R'] = \operatorname{div}(g).$$

$g = 0$ ist die Gerade durch P und Q bzw. die Tangente in P an E im Fall $P = Q$.

(2) Analog gibt es eine eindeutig bestimmte Gerade $h = 0$ durch O und R' und einen weiteren Punkt $R \in E$ mit

$$[O] + [R'] + [R] = \operatorname{div}(h).$$

Im Fall $O = R'$ ist $h = 0$ die Tangente in O an E.

(3) Nun wollen wir $P \oplus Q$ bestimmen. Es gilt für $S \in E$:

$$\begin{aligned}
P \oplus Q = S \quad &\iff \quad [P] - [O] + [Q] - [O] \sim [S] - [O] \quad \iff \quad [S] + [O] \sim [P] + [Q] \\
&\iff \quad [S] + [O] + [R'] \sim [P] + [Q] + [R'] \sim \operatorname{div}(g) \\
&\iff \quad [S] + [O] + [R'] \text{ ist Geradenschnitt nach dem Lemma} \\
&\iff \quad [S] + [O] + [R'] = \operatorname{div}(h) = [R] + [O] + [R'] \\
&\iff \quad S = R.
\end{aligned}$$

Damit gilt also $R = P \oplus Q$.

(4) Wir wollen noch das Inverse zu $P \in E$ bestimmen. Sei dazu $g = 0$ die Tangente in O an E und $\operatorname{div}(g) = 2[O] + [O']$.

$$\begin{aligned}
P \oplus P' = O \quad &\iff \quad [P] - [O] + [P'] - [O] \sim [O] - [O] \\
&\iff \quad [P] + [P'] \sim 2[O] \\
&\iff \quad [P] + [P]' + [O'] \sim 2[O] + [O'] = \operatorname{div}(g) \\
&\iff \quad [P] + [O'] + [P'] \text{ ist Geradenschnitt}
\end{aligned}$$

Ist $h = 0$ die Gerade durch P und O', so ist also P' eindeutig bestimmt durch $[P] + [O'] + [P'] = \operatorname{div}(h)$.

Wir fassen zusammen:

SATZ. *Sei E eine nichtsinguläre ebene Kubik und $O \in E(K)$.*

(1) *Die Addition zweier Punkte $P, Q \in E$ ergibt sich geometrisch wie folgt:*
- *Bestimme die Gerade $g = 0$ durch P und Q und damit den 3. Schnittpunkt R' mit* $\operatorname{div}(g) = [P] + [Q] + [R']$.
- *Bestimme die Gerade $h = 0$ durch R' und O und damit den 3. Schnittpunkt R mit* $\operatorname{div}(h) = [R'] + [O] + [R]$.

Dann gilt $P \oplus Q = R$.

(2) *Bestimme die Tangente $t = 0$ in O an E und damit den 3. Schnittpunkt O' mit* $\operatorname{div}(t) = 2[O] + [O']$.
Bestimme für $P \in E$ die Gerade $s = 0$ durch P und O' und damit den 3. Schnittpunkt P' mit $\operatorname{div}(s) = [P] + [O'] + [P']$. *Dann ist $\ominus P = P'$, d.h. $P \oplus P' = O$.*

Beispiel: Wir betrachten wieder $E = \{f = 0\}$ über $\mathbb{Q}$ mit

$$f = 3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3$$

und $O = (1 : 0 : 0)$.

- Die Tangente in O ist $x_1 = 0$, woraus man schnell $O' = (1 : 0 : 1)$ errechnet.
- Wir wollen $2 \cdot O' = O' \oplus O'$ berechnen. Die Tangente in O' ist $x_0 + 6x_1 - x_2 = 0$, einsetzen in f liefert
$$f(x_0, x_1, x_0 + 6x_1) = -x_1^2(205x_1 + 51x_0),$$
woraus sich als 3. Schnittpunkt mit der Tangente $R' = (205 : -51 : -101)$ ergibt. Die Gerade zwischen O und R' hat die Gleichung $x_2 = \frac{101}{51}x_1$, mit
$$f(x_0, x_1, \frac{101}{51}x_1) = \frac{1}{132651}x_1(5x_0 + 205x_1)(7803x_0 - 3110x_1)$$
erhält man als 3. Schnittpunkt $R = (3110 : 7803 : 15453)$, also
$$2 \cdot (1 : 0 : 1) = (3110 : 7803 : 15453).$$
(Über $\mathbb{R}$ ist $(205 : -51 : -101) \approx (1 : -0.25 : -0.49)$ und $(3110 : 7803 : 15453) \approx (1 : 2.51 : 4.97)$.)
- Wir berechnen jetzt $(1 : 0 : 1) \oplus (3110 : 7803 : 15453)$: Die Gerade durch die beiden Punkte ist
$$x_2 = x_0 + \frac{12343}{7803}x_1,$$
einsetzen in f liefert
$$\frac{1}{475099770627}x_1(269008425x_0 + 274115666x1)(7803x_0 - 3110x_1),$$
so dass man für den 3. Schnittpunkt
$$(274115666 : -269887425 : -151409259)$$
erhält. Die Gerade durch diesen Punkt und O ist
$$x_2 = \frac{989603}{1758225}x_1,$$
sie schneidet E in dem 3. Punkt
$$3 \cdot (1 : 0 : 1) = (1043360347 : 60614806875 : 34116563425).$$
- Die Addition kann man natürlich auch einfach programmieren, was wir auch für die folgenden Rechnungen gemacht haben.
- Welche $\mathbb{Q}$-rationalen Punkte hat E?
- Vorbemerkung: Ist $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2(\mathbb{Q})$, so können wir o.E. $p_0, p_1, p_2 \in \mathbb{Z}$ und $\operatorname{ggT}(p_0, p_1, p_2) = 1$ annehmen. Die Höhe des Punktes P definieren wir dann als
$$H(P) = \max(|p_0|, |p_1|, |p_2|).$$
- Wir haben alle Punkte der Höhe ≤ 340 in $E(\mathbb{Q})$ bestimmt. Sie stehen in nachfolgender Tabelle. Dabei steht Pn für einen Punkt der Höhe n. Gibt es mehrere, haben wir sie mit $a, b, c, \ldots$ durchnumeriert.

- Da $E(\mathbb{Q})$ eine Gruppe bildet, kann man natürlich fragen, welche Struktur diese Gruppe hat. Nach ein paar Versuchen haben wir

$$A_1 = (1:0:1) = P1b, \quad A_2 = (1:1:-1) = P1d, \quad A_3 = (3:-4:2) = P4$$

gewählt, womit sich alle gefundenen Punkte der Tabelle linear kombinieren ließen. (In der Tabelle stehen bei jedem Punkt die Koeffizienten n_1, n_2, n_3 von $P = n_1A_1 + n_2A_2 + n_3A_3$.) Die Frage stellt sich jetzt: Gilt

$$E(\mathbb{Q}) = \mathbb{Z}A_1 + \mathbb{Z}A_2 + \mathbb{Z}A_3,$$

bzw. $E(\mathbb{Q}) \simeq \mathbb{Z}^3$?

Geometrische Addition für $y^2 = x^3 + ax + b$:

- E sei also affin gegeben durch $f = 0$ mit $f = x^3 + ax + b - y^2$ bzw. projektiv durch $F = 0$ mit $F = x_1^3 + ax_0^2x_1 + bx_0^3 - x_0x_2^2$ und $O = (0:0:1)$. Wir setzen weiter voraus, dass die Charakteristik $\neq 2, 3$ ist.
- Wann ist E singulär? Es gilt

$$\frac{\partial F}{\partial x_0} = 2ax_0x_1 + 3bx_0^2 - x_2^2, \quad \frac{\partial F}{\partial x_1} = 3x_1^2 + ax_0^2, \quad \frac{\partial F}{\partial x_2} = -2x_0x_2.$$

Wäre $x_0 = 0$, so würde $x_1 = x_2 = 0$ folgen, was nicht geht. Also o.E. $x_0 = 1$ und $x_1 = x$, $x_2 = y$. Es folgt $y = 0$ und $2ax + 3b = 0$, $3x^2 + a = 0$. Für $a = 0$ erhält man $b = 0$ und $x = 0$, für $a \neq 0$ durch Elimination $x = -\frac{3b}{2a}$ und die Bedingung $4a^3 + 27b^2 = 0$. Definiert man

$$\Delta = 4a^3 + 27b^2,$$

so kann man dies zusammenfassen:

$$E \text{ ist singulär} \iff \Delta = 0.$$

- Der einzige unendlich ferne Punkt, d.h. Punkt auf der Geraden $x_0 = 0$ ist O. Damit folgt auch sofort $O' = O$. Die Geraden durch O haben die Form $c_0x_0 + c_1x_1 = 0$, außer x_0 sind dies also die Geraden $x = c$ mit $c \in \overline{K}$.
- Was ist $\ominus P$ für $P = (x_0, y_0)$? Die Gerade durch P und O' hat die affine Gleichung $x = x_0$, einsetzen in f liefert

$$f(x_0, y) = x_0^3 + ax_0 + b - y^2 = y_0^2 - y^2 = -(y - y_0)(y + y_0).$$

Also ist der 3. Punkt auf der Geraden $(x_0, -y_0)$ und es folgt

$$\ominus(x_0, y_0) = (x_0, -y_0).$$

- Seien $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ Punkte auf E. Wir wollen $P_1 \oplus P_2$ berechnen. Gilt $x_1 = x_2$ und $y_2 = -y_1$, so ist $P_1 \oplus P_2 = O$, also können wir voraussetzen, dass dieser Fall nicht vorliegt. Im Fall $x_1 = x_2$ ist also $y_1 = y_2 \neq 0$.
- Sei $y = \lambda x + \mu$ die Gerade und P_1 und P_2. Zunächst ist immer $\mu = y_1 - \lambda x_1$. Ist $P_1 \neq P_2$, so ist

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

Ist $P_1 = P_2$, so müssen wir die Tangente berechnen, also

$$\frac{\partial f}{\partial x}(P_1)(x - x_1) + \frac{\partial f}{\partial y}(P_1)(y - y_1) = 0,$$

bzw.

$$y - y_1 = \frac{3x_1^2 + a}{2y_1}(x - x_1),$$

woraus sofort

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

folgt.

P	Punkt	$P = n_1A_1 + n_2A_2 + n_3A_3$
$P1a$	$(1:0:0)$	$0,0,0$
$P1b$	$(1:0:1)$	$1,0,0$
$P1c$	$(0:1:1)$	$0,2,-1$
$P1d$	$(1:1:-1)$	$0,1,0$
$P3a$	$(1:1:3)$	$1,-2,0$
$P3b$	$(2:-3:3)$	$1,-1,0$
$P4$	$(3:-4:2)$	$0,0,1$
$P5a$	$(4:-5:-1)$	$0,-2,1$
$P5b$	$(5:-3:-3)$	$1,-2,1$
$P5c$	$(5:-4:-3)$	$-1,2,0$
$P6$	$(5:6:-3)$	$1,0,-1$
$P9$	$(1:6:9)$	$0,-1,1$
$P11$	$(11:-4:-6)$	$1,1,-1$
$P12$	$(7:12:-2)$	$1,-3,1$
$P13$	$(3:8:-13)$	$0,-1,0$
$P21$	$(19:-21:-9)$	$0,1,-1$
$P22$	$(22:-3:-9)$	$0,2,0$
$P46$	$(19:-36:46)$	$-1,3,-1$
$P48$	$(1:-48:-36)$	$2,-2,0$
$P49$	$(4:49:21)$	$1,-1,1$
$P51$	$(7:-33:51)$	$-1,0,1$
$P54$	$(41:-54:9)$	$0,3,-1$
$P57$	$(22:57:3)$	$-1,1,0$
$P75$	$(19:75:15)$	$1,2,-1$
$P92$	$(11:92:34)$	$0,0,-1$
$P101$	$(101:-3:69)$	$-1,4,-1$
$P120$	$(120:-1:23)$	$2,-4,1$
$P135$	$(47:-100:135)$	$1,-4,2$
$P147$	$(109:-147:91)$	$1,2,-2$
$P152$	$(152:-3:53)$	$-1,1,1$
$P159$	$(79:30:159)$	$-1,2,-1$
$P187$	$(76:121:-187)$	$2,0,-1$
$P189$	$(170:189:-117)$	$0,-2,2$
$P205$	$(205:-51:-101)$	$-1,0,0$
$P209$	$(209:-196:-119)$	$2,-3,0$
$P236$	$(236:-9:-61)$	$1,-1,-1$
$P311$	$(311:-4:79)$	$0,3,-2$
$P312$	$(-7:-192:312)$	$1,1,0$
$P319$	$(319:-42:-129)$	$1,-4,1$
$P324$	$(-211:-240:324)$	$0,4,-2$
$P336$	$(1:336:204)$	$-1,3,0$

$\mathbb{Q}$-rationale Punkte der Höhe ≤ 340 auf

$$E = \{3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3 = 0\}.$$

- Wir berechen den 3. Schnittpunkt $(\widetilde{x}, \widetilde{y})$ mit der Geraden und setzen dazu $y = \lambda x + \mu$ in f ein:

  $$f(x, \lambda x + \mu) = x^3 + ax + b - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2).$$

  Dies muss gleich dem Polynom

  $$(x - x_1)(x - x_2)(x - \widetilde{x}) = x^3 - (x_1 + x_2 + \widetilde{x})x^2 + \ldots$$

sein, woraus durch Koeffizientenvergleich bei x^2 sofort

$$\widetilde{x} = \lambda^2 - x_1 - x_2 \text{ und damit } \widetilde{y} = \lambda\widetilde{x} + \mu$$

folgt. Der 3. Schnittpunkt auf der Verbindungsgeraden von $(\widetilde{x}, \widetilde{y})$ und O ist $(\widetilde{x}, -\widetilde{y})$, also folgt schließlich für $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$:

$$x_3 = \lambda^2 - x_1 - x_2 \text{ und } y_3 = -\lambda x_3 - \mu.$$

- Damit sieht man jetzt auch: $P_1 \oplus P_2 \oplus P_3 = O$ genau dann, wenn P_1, P_2, P_3 auf einer Geraden liegen.

Wir fassen das Ergebnis zusammen:

SATZ. *In Charakteristik $\neq 2, 3$ ist die Kurve $y^2 = x^3 + ax + b$ genau dann nichtsingulär, wenn $\Delta = 4a^3 + 27b^2 \neq 0$ gilt. In diesem Fall ist E mit dem Punkt $O = (0 : 0 : 1)$ eine elliptische Kurve, für die das Additionsgesetz wie folgt aussieht, wenn (x_i, y_i) Punkte auf E sind.*

$$\begin{aligned}
\ominus(x_1, y_1) &= (x_1, -y_1) \\
(x_1, y_1) \oplus (x_1, -y_1) &= O \\
(x_1, y_1) \oplus (x_2, y_2) &= (x_3, y_3) \text{ mit} \\
&\quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -\lambda x_3 - y_1 + \lambda x_1 \text{ und} \\
&\quad \lambda = \left\{ \begin{array}{cc} \frac{y_1 - y_2}{x_1 - x_2} & \text{für } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{für } x_1 = x_2 \text{ und } y_1 = y_2 \neq 0. \end{array} \right\}
\end{aligned}$$

Außerdem gilt: $P_1 \oplus P_2 \oplus P_3 = O$ genau dann, wenn $[P_1] + [P_2] + [P_3]$ ein Geradenschnitt ist.

Beispiel: Sei E gegeben durch $y^2 = x^3 + 17$. Man findet $P = (-2, 3) \in E$ und rechnet mit den Formeln dann nach

$$P \oplus P = (8, -23), \quad P \oplus P \oplus P = (\frac{19}{25}, \frac{522}{125}).$$

Man suche mit dem Computer weitere Punkte und versuche die Gruppenstruktur von $E(\mathbb{Q})$ zu erraten.

Allgemeine Additionstheoreme: Ist E eine elliptische Kurve in Charakteristik $\neq 2, 3$, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$ (mit $\Delta = 4a^3 + 27b^2 \neq 0$), so geben folgende Formeln die Addition an:

$$(z_{i0} : z_{i1} : z_{i2}) = (x_0 : x_1 : x_2) \oplus (y_0 : y_1 : y_2).$$

(Für jeden Punkt $P \in E$ gibt es mindestens ein i mit $(z_{i0}(P), z_{i1}(P), z_{i2}(P)) \neq 0$.)

```
z10 := a*x0^2*y0*y1-a*x0*x1*y0^2-x0^2*y2^2+x2^2*y0^2+3*x0*x1*y1^2
       -3*x1^2*y0*y1;
z11 := -3*b*x0^2*y0*y1+3*b*x0*x1*y0^2-a*x0^2*y1^2+a*x1^2*y0^2
       -x0*x1*y2^2+x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
z12 := 3*b*x0^2*y0*y2-3*b*x0*x2*y0^2+a*x0^2*y1*y2-a*x1*x2*y0^2
       +2*a*x0*x1*y0*y2-2*a*x0*x2*y0*y1-x0*x2*y2^2+x2^2*y0*y2
       +3*x1^2*y1*y2-3*x1*x2*y1^2;

z20 := 3*b*x0^2*y0*y1-3*b*x0*x1*y0^2+a*x0^2*y1^2-a*x1^2*y0^2
       +x0*x1*y2^2-x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
z21 := a^2*x0^2*y0*y1-a^2*x0*x1*y0^2-3*b*x0^2*y1^2+3*b*x1^2*y0^2
       -a*x0*x1*y1^2+a*x1^2*y0*y1+x1^2*y2^2-x2^2*y1^2;
z22 := -a^2*x0^2*y0*y2+a^2*x0*x2*y0^2+3*b*x0^2*y1*y2-3*b*x1*x2*y0^2
       +6*b*x0*x1*y0*y2-6*b*x0*x2*y0*y1+2*a*x0*x1*y1*y2
       -2*a*x1*x2*y0*y1-a*x0*x2*y1^2+a*x1^2*y0*y2+x1*x2*y2^2-x2^2*y1*y2;

z30 := 6*b*x0*x2*y0^2+6*b*x0^2*y0*y2+2*a*x1*x2*y0^2+2*a*x0^2*y1*y2
       +4*a*x0*x2*y0*y1+4*a*x0*x1*y0*y2+2*x2^2*y0*y2+2*x0*x2*y2^2
       +6*x1*x2*y1^2+6*x1^2*y1*y2;
z31 := 2*a^2*x0*x2*y0^2+2*a^2*x0^2*y0*y2-6*b*x1*x2*y0^2-6*b*x0^2*y1*y2
```

```
       -12*b*x0*x2*y0*y1-12*b*x0*x1*y0*y2-4*a*x1*x2*y0*y1
       -4*a*x0*x1*y1*y2-2*a*x1^2*y0*y2-2*a*x0*x2*y1^2+2*x2^2*y1*y2
       +2*x1*x2*y2^2;
z32 := -2*x0^2*y0^2*a^3-18*x0^2*y0^2*b^2-6*a*b*x0*x1*y0^2
       -6*a*b*x0^2*y0*y1-2*a^2*x1^2*y0^2-2*a^2*x0^2*y1^2
       -8*a^2*x0*x1*y0*y1+18*b*x1^2*y0*y1+18*b*x0*x1*y1^2+6*a*x1^2*y1^2
       +2*x2^2*y2^2;
```

Außerdem gilt:

$$\ominus(x_0 : x_1 : x_2) = (x_0 : x_1 : -x_2).$$

Damit erhält man:

FOLGERUNG. *Auf einer elliptischen Kurve E sind die Addition $E \times E \to E$ und die Inversenbildung $E \to E$ Morphismen.*

Indem man einen Punkt fest einsetzt, folgt:

FOLGERUNG. *Ist (E, O) eine elliptische Kurve und $P_0 \in E$, so ist die Translation*

$$\tau_{P_0} : E \to E, \quad P \mapsto P \oplus P_0$$

ein Isomorphismus. Es ist $\tau_{P_0}^{-1} = \tau_{\ominus P_0}$.

3. Isomorphie elliptischer Kurven

Wir wollen uns jetzt der Frage zuwenden, wieweit die Weierstraßgleichung einer elliptischen Kurve eindeutig bestimmt ist.

(1) Seien (E, O) und (E', O') zwei elliptische Kurven in Weierstraßgleichung: $y^2 = x^3 + ax + b$ und $y'^2 = x'^3 + a'x' + b'$ und $\phi : E \to E'$ ein Isomorphismus. Indem wir ϕ eventuell um eine Translation abändern, können wir $\phi(O) = O'$ annehmen.

(2) Es ist

$$\mathcal{L}(2[O]) = \overline{K} + \overline{K}x \text{ und } \mathcal{L}(2[O']) = \overline{K} + \overline{K}x'$$

und

$$\mathcal{L}(3[O]) = \overline{K} + \overline{K}x + \overline{K}y \text{ und } \mathcal{L}(3[O']) = \overline{K} + \overline{K}x' + \overline{K}y'.$$

Da ϕ ein Isomorphismus ist, hat $\phi^*([O'])$ Grad 1, also $\phi^*([O']) = [O]$. Daher gilt für $n \in \mathbb{N}$ und $f \in \overline{K}(E')$:

$$f \in \mathcal{L}(n[O']) \Rightarrow \operatorname{div}(f) + n[O'] \geq 0 \Rightarrow 0 \leq \operatorname{div}(\phi^* f) + n[O] \Rightarrow \phi^* f \in \mathcal{L}(n[O]).$$

Wendet man dies für $n = 2, 3$ an, so sieht man, dass es $v, v_1, w, w_1, w_2 \in K$ gibt mit $v, w \neq 0$ und

$$\phi^* x' = x'' = vx + v_1 \text{ und } \phi^* y' = y'' = wy + w_1 x + w_2.$$

Natürlich gilt $y''^2 = x''^3 + a'x'' + b''$. Andererseits ist $y^2 = x^3 + ax + b$ die kleinste Relation zwischen x und y. Durch Einsetzen sieht man sofort, dass keine Terme xy und y auftreten, was $w_1 = w_2 = 0$ ergibt. Da auch kein Term x^2 auftritt, folgt auch $v_1 = 0$. Also bleibt $x'' = vx$ und $y'' = wy$. Wir setzten jetzt ein:

$$\begin{aligned} 0 &= x''^3 + a'x'' + b' - y''^2 = v^3x^3 + a'vx + b' - w^2y^2 = \\ &= v^3x^3 + a'vx + b' - w^2(x^3 + ax + b) = \\ &= (v^3 - w^2)x^3 + (a'v - w^2a)x + (b' - w^2b), \end{aligned}$$

was durch Koeffizientenvergleich sofort

$$v^3 = w^2, \quad a'v = w^2a, \quad b' = w^2b$$

ergibt. Setzt man $u = \frac{w}{v}$, so ergibt sich

$$u^2 = v, \quad u^3 = w \text{ und } a' = u^4a, \quad b' = u^6b.$$

(3) Gilt umgekehrt für ein $u \in K$, $u \neq 0$:

$$a' = u^4 a, \quad b' = u^6 b,$$

so führt der Koordinatenwechsel $(x, y) \mapsto (u^2 x, u^3 y)$ die Kurve E in E' über.

Damit haben wir bewiesen:

SATZ. *Zwei elliptische Kurven $E : y^2 = x^3 + ax + b$ und $E' : y^2 = x^3 + a'x + b'$ sind genau dann über K isomorph, wenn es ein $u \in K^*$ gibt mit*

$$a' = u^4 a \text{ und } b' = u^6 b.$$

In diesem Fall liefert $(x, y) \mapsto (u^2 x, u^3 y)$ einen Isomorphismus $E \to E'$.

Wir werden nun eine wichtige Invariante einführen: Ist E eine elliptische Kurve und sind $y^2 = x^3 + ax + b$ und $y^2 = x^3 + a'x + b'$ zwei Weierstraßgleichungen für E, so gibt es also ein $u \in K$ mit $a' = u^4 a$ und $b' = u^6 b$. Für die Diskriminanten gilt:

$$\Delta' = 4a'^3 + 27b'^2 = u^{12}\Delta \neq 0$$

und damit

$$\frac{4a'^3}{4a'^3 + 27b'^2} = \frac{4a^3}{4a^3 + 27b^2}.$$

Daher ist dieser Ausdruck unabhängig von der Auswahl der Weierstraßgleichung und man definiert:

DEFINITION. *Ist E eine elliptische Kurve in Charakteristik $\neq 2, 3$ und $y^2 = x^3 + ax + b$ eine beschreibende Weierstraßgleichung, so definiert man die j-Invariante von E durch*

$$j = j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Aus obiger Überlegung folgt auch sofort:

FOLGERUNG. *Sind E und E' zwei über K isomorphe elliptische Kurven, so gilt: $j(E) = j(E')$.*

Elliptische Kurven zu vorgebener j-Invariante: Sei also $j \in K$ gegeben. Wir wollen sehen, ob es dazu elliptische Kurven gibt, und wie diese aussehen.

(1) Wir gehen aus von $j = 1728 \frac{4a^3}{4a^3 + 27b^2}$. Zunächst ist klar:

$$j = 0 \iff a = 0 \quad \text{und} \quad j = 1728 \iff b = 0.$$

(2) Wir setzen also jetzt $j \neq 0, 1728$ voraus. Dann haben wir die Umformungen:

$$\begin{aligned} j = 1728 \frac{4a^3}{4a^3 + 27b^2} &\iff 4ja^3 + 27jb^2 = 1728 \cdot 4a^3 \\ &\iff 27jb^2 = 4(1728 - j)a^3 \\ &\iff (\frac{b}{2})^2 = \frac{1728 - j}{j} (\frac{a}{3})^3 \text{ und nach Multiplikation mit } (\frac{1728 - j}{j})^2 \\ &\iff (\frac{1728 - j}{2j} b)^2 = (\frac{1728 - j}{3j} a)^3. \end{aligned}$$

Also gibt es wie üblich ein $t \in K$ mit

$$\frac{1728 - j}{2j} b = t^3, \quad \frac{1728 - j}{3j} a = t^2$$

oder anders geschrieben

$$a = \frac{3j}{1728 - j} t^2, \quad b = \frac{2j}{1728 - j} t^3.$$

(3) Wann liefern t_1 und t_2 eine isomorphe Kurve? Genau dann, wenn es ein $u \in K^\times$ gibt mit

$$u^4 = \frac{a_{t_1}}{a_{t_2}} = (\frac{t_1}{t_2})^2 \quad \text{und} \quad u^6 = \frac{b_{t_1}}{b_{t_2}} = (\frac{t_1}{t_2})^3,$$

was nach Divison mit

$$u^2 = \frac{t_1}{t_2}$$

äquivalent ist.

Damit erhalten wir folgenden Satz:

SATZ. (1) *Ist $j \in K$ und $j \neq 0, 1728$, so haben genau die Kurven E_t mit $y^2 = x^3 + a_t x + b_t$ und*

$$a_t = \frac{3j}{1728 - j} t^2, \quad b_t = \frac{2j}{1728 - j} t^3, \quad t \in K^*$$

j-Invariante j. Weiterhin sind E_{t_1} und E_{t_2} genau dann isomorph über K, wenn es ein $u \in K$ gibt mit $t_2 = u^2 t_1$. Ist $t_\alpha, \alpha \in A$ ein Repräsentantensystem der Gruppe K^*/K^{*2}, so repräsentieren die Kurven E_{t_α} alle Isomorphieklassen elliptischer Kurven über K mit j-Invariante j.

(2) *Ist $j = 0$, so haben genau die Kurven E_b mit $y^2 = x^3 + b$ j-Invariante 0. Zwei Kurven E_{b_1} und E_{b_2} sind genau dann isomorph über K, wenn es ein $u \in K, u \neq 0$ gibt mit $b_2 = u^6 b_1$. Repräsentieren $b_\beta, \beta \in B$ die Klassen K^*/K^{*6}, so die Kurven E_β die Isomorphieklassen elliptischer Kurven über K mit j-Invariante 0.*

(3) *Ist $j = 1728$, so haben genau die Kurven E_a mit $y^2 = x^3 + ax$ j-Invariante 1728. Zwei Kurven E_{a_1} und E_{a_2} sind genau dann isomorph über K, wenn es ein $u \in K, u \neq 0$ gibt mit $a_2 = u^6 a_1$. Repräsentieren $a_\alpha, \alpha \in A$ die Klassen K^*/K^{*4}, so die Kurven E_α die Isomorphieklassen elliptischer Kurven über K mit j-Invariante 1728.*

FOLGERUNG. *Für elliptische Kurven E und E' gilt:*

$$E \sim_{\overline{K}} E' \quad \Longleftrightarrow \quad j(E) = j(E').$$

Beispiel: Für $K = \mathbb{R}$ gilt

$$\mathbb{R}^{*2} = \mathbb{R}^{*4} = \mathbb{R}^{*6} = \{r \in \mathbb{R} : r > 0\},$$

modulo zweiten, vierten und sechsten Potenzen bilden ± 1 ein Repräsentantensystem. Also erhält man folgendes Repräsentantensystem für die elliptischen Kurven über $\mathbb{R}$, wo j alle reellen Zahlen durchläuft:

$$\begin{aligned} j \neq 0, 1728: &\quad y^2 = x^3 + \frac{3j}{1728 - j} x + \frac{2j}{1728 - j} \text{ und } y^2 = x^3 + \frac{3j}{1728 - j} x - \frac{2j}{1728 - j} \\ j = 0: &\quad y^2 = x^3 + 1 \text{ und } y^2 = x^3 - 1 \\ j = 1728: &\quad y^2 = x^3 + x \text{ und } y^2 = x^3 - x \end{aligned}$$

Beispiel: Für $K = \mathbb{F}_5$ gilt

$$\mathbb{F}_5^{*2} = \{1, 4\}, \quad \mathbb{F}_5^{*4} = \{1\}, \quad \mathbb{F}_5^{*6} = \{1, 4\},$$

also

$$\mathbb{F}_5^*/\mathbb{F}_5^{*2} = \{\overline{1}, \overline{2}\}, \quad \mathbb{F}_5^*/\mathbb{F}_5^{*4} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}, \quad \mathbb{F}_5^*/\mathbb{F}_5^{*6} = \{\overline{1}, \overline{2}\}.$$

Damit erhält man folgende Tabelle:

j	Kurven E mit Anzahl von Punkten $\#E(\mathbb{F}_5)$
0	$y^2 = x^3 + 1 (N = 6), \quad y^2 = x^3 + 2 (N = 6)$
1	$y^2 = x^3 + 4x + 1 (N = 8), \quad y^2 = x^3 + x + 3 (N = 4)$
2	$y^2 = x^3 + x + 4 (N = 9), \quad y^2 = x^3 + 4x + 2 (N = 3)$
$1728 = 3$	$y^2 = x^3 \pm x (N = 4, 8), \quad y^2 = x^3 \pm 2x (N = 2, 10)$
4	$y^2 = x^3 + 3x + 2 (N = 5), \quad y^2 = x^3 + 2x + 1 (N = 7)$

(Beachte die symmetrische Verteilung der Anzahlen um 6.)

Aufgabe: Gib für $\mathbb{F}_{53}$ ein Repräsentantensystem der Isomorphieklassen elliptischer Kurven an und bestimme jeweils $\#E(\mathbb{F}_{53})$.

Beispiel: $K = \mathbb{F}_p$ ein endlicher Körper mit $p \geq 5$. Bezeichnet A die Anzahl der Isomorphieklassen elliptischer Kurven über $\mathbb{F}_p$, so gilt offensichtlich

$$A = (p-2)\#\mathbb{F}_p^*/\mathbb{F}_p^{*2} + \#\mathbb{F}_p^*/\mathbb{F}_p^{*4} + \#\mathbb{F}_p^*/\mathbb{F}_p^{*6}.$$

Der Kern der Abbildung $\mathbb{F}_p^* \overset{x\mapsto x^n}{\to} \mathbb{F}_p^*$ hat $ggT(p-1,n)$ Elemente, da $\mathbb{F}_p^*$ zyklisch ist. Daher gilt auch $\#\mathbb{F}_p^*/\mathbb{F}_p^{*n} = \mathrm{ggT}(p-1,n)$. Damit erhält man

$$A = 2(p-2) + \left\{ \begin{array}{lll} 10 & \text{für} & p \equiv 1 \bmod 12 \\ 6 & \text{für} & p \equiv 5 \bmod 12 \\ 8 & \text{für} & p \equiv 7 \bmod 12 \\ 4 & \text{für} & p \equiv 11 \bmod 12 \end{array} \right\}$$

4. Morphismen zwischen elliptischen Kurven

Wir wollen jetzt Morphismen zwischen elliptischen Kurven betrachten. Es gilt der wichtige Satz:

SATZ. *Seien (E_1, O_1) und (E_2, O_2) elliptische Kurven und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus. Gilt $\phi(O_1) = O_2$, dann ist ϕ ein Gruppenhomomorphismus. Man nennt ϕ eine* **Isogenie** *und die Kurven E_1 und E_2* **isogen**.

FOLGERUNG. *Sind (E_1, O_1) und (E_2, O_2) elliptische Kurven und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus, dann gibt es eine Isogenie ψ und eine Translation τ mit $\phi = \tau \circ \psi$.*

Zum Beweis des Satzes brauchen wir ein Lemma:

LEMMA. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen Kurven. Dann gilt*

$$\phi_*(\textit{Hauptdivisor}) = \textit{Hauptdivisor}.$$

Beweisskizze: Wir beschränken uns auf den Fall, dass $\overline{K}(C_1)$ über $\overline{K}(C_2)$ galoissch ist mit Galoisgruppe G. Dann operiert G auch auf C_1. Insbesondere gilt für jeden Punkt $P \in C_1$:

$$\phi^*\phi_*[P] = \sum_{\sigma\in G} [\sigma P].$$

Sei $f \in \overline{K}(C_1)^*$ und $\mathrm{div}(f) = \sum_i n_i[P_i]$. Dann gilt

$$\begin{aligned} \phi^*\phi_*(\mathrm{div}(f)) &= \phi^*\phi_*(\sum_i n_i[P_i]) = \sum_i n_i\phi^*\phi_*[P_i] = \sum_i n_i \sum_{\sigma\in G}[\sigma P_i] = \sum_{\sigma\in G}\sigma(\sum_i n_i[P_i]) = \\ &= \sum_{\sigma\in G}\sigma(\mathrm{div}(f)) = \sum_{\sigma\in G}\mathrm{div}(\sigma f) = \mathrm{div}(\prod_{\sigma\in G}\sigma f). \end{aligned}$$

Nun ist aber $g = \prod_{\sigma\in G}\sigma f \in \overline{K}(C_2)$, also folgt $\phi^*\phi_*(\mathrm{div}(f)) = \phi^*(\mathrm{div}(g))$ und damit $\phi_*(\mathrm{div}(f)) = \mathrm{div}(g)$, also die Behauptung. ■

Beweis des Satzes: Zu zeigen ist für $P_1, P_2, P_3 \in E_1$:

$$P_1 \oplus P_2 = P_3 \quad \Rightarrow \quad \phi(P_1) \oplus \phi(P_2) = \phi(P_3).$$

Sei also $P_1 \oplus P_2 = P_3$. Dies bedeutet $[P_1] + [P_2] \sim [P_3] + [O_1]$ und damit $[P_1] + [P_2] - [P_3] - [O_1] \sim 0$, d.h. $[P_1] + [P_2] - [P_3] - [O_1]$ ist Hauptdivisor. Nach dem Lemma gilt dann

$$0 \sim \phi_*([P_1] + [P_2] - [P_3] - [O_1]) = [\phi(P_1)] + [\phi(P_2)] - [\phi(P_3)] - [O_2],$$

was auf die gleiche Weise wieder $\phi(P_1) \oplus \phi(P_2) = \phi(P_3)$ liefert, also die Behauptung. ■

Ist A eine abelsche Gruppe, so bilden die Endomorphismen $\phi : A \to A$ einen Ring durch die Definitionen

$$\begin{aligned} 0(a) &= 0, \\ 1(a) &= \mathrm{id}_A(a) = a, \\ (\phi_1 + \phi_2)(a) &= \phi_1(a) + \phi_2(a), \\ (\phi_1\phi_2)(a) &= \phi_1(\phi_2(a)). \end{aligned}$$

Dies überträgt sich sofort auf elliptische Kurven:

DEFINITION. *Ist (E, O) eine elliptische Kurve, so ist*

$$\mathrm{End}(E) = \{\phi : E \to E \text{ über } \overline{K} \text{ definierter Morphismus mit } \phi(O) = O\}$$

ein Ring, der sogenannte **Endomorphismenring von** E. *Betrachtet man nur über K definierte Morphismen, so schreibt man* $\mathrm{End}_K(E)$. *Die Einheitengruppe von* $\mathrm{End}(E)$

$$\mathrm{Aut}(E) = \{\phi : E \to E \text{ Isomorphismus mit } \phi(O) = O\}$$

heißt die **Automorphismengruppe von** E.

Wir haben oben für Charakteristik $\neq 2, 3$ gesehen, dass jeder Isomorphismus $\phi : E \to E'$ zwischen elliptischen Kurven mit $\phi(O) = O'$ durch einen Koordinatenwechsel $x \mapsto u^2x, y \mapsto u^3y$, $u \in \overline{K}^*$ gegeben ist. Wann liefert nun eine solche Transformation einen Automorphismus von E? Genau dann, wenn $(x, y) \mapsto (u^2x, u^3y)$ die Kurve E in sich überführt, d.h. die transformierte Gleichung muss identisch erfüllt sein, also:

$$u^6y^2 = u^6x^3 + au^2x + b \text{ bzw. } y^2 = x^3 + \frac{a}{u^4}x + \frac{b}{u^6},$$

was sofort die Bedingung $a = u^4a, b = u^6b$ liefert. Damit ergibt sich sofort folgender Satz:

SATZ. *In Charakteristik $\neq 2, 3$ gilt für eine elliptische Kurve E:*

(1) *Ist $j(E) \neq 0, 1728$, so ist*
$$\mathrm{Aut}(E) = \{P \mapsto P, P \mapsto -P\} \simeq \mathbb{Z}/(2).$$
(2) *Ist $j(E) = 1728$ (Typ $y^2 = x^3 + ax$), so ist*
$$\begin{aligned} \mathrm{Aut}(E) &= \{(x, y) \mapsto (x, y), (x, y) \mapsto (-x, iy), (x, y) \mapsto (-x, -iy), (x, y) \mapsto (x, -y)\} \\ &\simeq \mathbb{Z}/(4) \text{ mit } i^2 = -1. \end{aligned}$$
(3) *$j(E) = 0$ (Typ $y^2 = x^3 + b$), so ist*
$$\mathrm{Aut}(E) = \{(x, y) \mapsto (x, \pm y), (x, y) \mapsto (\zeta_3 x, \pm y), (x, y) \mapsto (\zeta_3^2 x, \pm y)\} \simeq \mathbb{Z}/(6).$$
mit einer primitiven 3-ten Einheitswurzel ζ_3.

Aufgabe:

(1) Zeige, dass die Kurve $y^2 = x^3 - x$ in Charakteristik 3 eine Automorphismengruppe der Ordnung 12 besitzt.
(2) Zeige, dass $y^2 + y = x^3$ in Charakteristik 2 eine Automorphismengruppe der Ordnung 24 besitzt.

Die Bestimmung von $\mathrm{End}(E)$ ist nicht so einfach. Ist E eine elliptische Kurve und $n \in \mathbb{Z}, n \geq 0$, so ist die Multiplikation mit n

$$E \to E, \quad P \mapsto nP = P \oplus \cdots \oplus P$$

eine Endomorpmismus, der manchmal mit $[n]$ bezeichnet wird. Entsprechend definiert man $[-n]$:

$$E \to E, \quad P \mapsto n(\ominus P) = \ominus P \ominus \cdots \ominus P.$$

Diese Endomorphismen hat man bei jeder elliptischen Kurve.

SATZ. *Sei (E, O) eine elliptische Kurve. Dann gilt:*

(1) *Der Endomorphismenring* $\mathrm{End}(E)$ *ist nullteilerfrei, d.h. $\phi\psi = 0$ impliziert $\phi = 0$ oder $\psi = 0$.*

(2) *Die Abbildung*

$$\mathbb{Z} \to \mathrm{End}(E), \quad n \mapsto [n]$$

ist ein injektiver Ringhomomorphismus. Also kann man immer $\mathbb{Z} \subseteq \mathrm{End}(E)$ *schreiben.*

Beweis:

(1) Sei $\phi\psi = 0$. Ein Morphismus $E \to E$ ist surjektiv oder konstant. Ist ψ surjektiv, so folgt $0 = \phi(\psi(E)) = \phi(E)$, also $\phi = 0$. Ist ψ konstant, so $\psi = 0$ wegen $\psi(O) = O$.

(2) Wir beschränken uns auf elliptische Kurven der Form $y^2 = x^3 + ax + b$ in Charakteristik $\neq 2, 3$. Dass $\mathbb{Z} \to \mathrm{End}(E)$, $n \mapsto [n]$ ein Ringhomomorphismus ist, ist klar. Wir zeigen für jede Primzahl p, dass $[p] \neq 0$ gilt. Dann folgt nach 1. auch $[n] \neq 0$ für jede ganze Zahl $n \geq 0$.
1. Fall $p = 2$*:* Sei $P = (x, y) \in E$ mit $y \neq 0$. Dann gilt $P \neq -P$, also $2P \neq 0$.
2. Fall $p > 2$*:* Sei $e \in \overline{K}$ eine Nullstelle von $x^3 + ax + b$. Dann ist $P = (e, 0) \in E$ mit $P = -P$, also $2P = 0$. Es folgt mit $p = 2m + 1$:

$$pP = m(2P) + P = P \neq 0,$$

also die Behauptung. ■

Man unterscheidet drei Typen von Endomorphismenringen elliptischer Kurven:

(1) $\mathrm{End}(E) = \mathbb{Z}$.

(2) $\mathrm{End}(E)$ ist Unterring eines quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-d})$ (mit $d \in \mathbb{N}$) und nicht von Typ 1. Man sagt, E hat **komplexe Multiplikation**.

(3) End ist Unterring einer Quaternionenalgebra $Q(a, b)$ und nicht von Typ 1 oder 2. Man sagt, E ist **supersingulär**. Dieser Fall kommt nur in Charakteristik p vor.

Ausführlich wird das Thema in [**Silverman**] behandelt.

Frage: Was kann man über die Struktur von $E(K)$ und $E(\overline{K})$ sagen?

Wir werden auf diese Frage nicht näher eingehen, sondern nur kurz den Fall $K = \mathbb{R}$ betrachten.

5. Elliptische Kurven über $\mathbb{R}$

Wir betrachten E mit $y^2 = x^3 + ax + b$, $a, b \in \mathbb{R}$ und $\Delta = 4a^3 + 27b^2 \neq 0$. Es gibt zwei Fälle:

(1) $x^3 + ax + b$ hat genau eine reelle Nullstelle, die andern beiden sind komplex konjugiert, also

$$x^3 + ax + b = (x - \alpha)(x + \frac{1}{2}\alpha + \beta i)(x + \frac{1}{2}\alpha - \beta i)$$

mit $\alpha, \beta \in \mathbb{R}, \beta \neq 0$, was durch Koeffizientenvergleich

$$a = -\frac{3}{4}\alpha^2 + \beta^2, \quad b = -\frac{1}{4}\alpha^3 - \alpha\beta^2$$

und damit

$$\Delta = \frac{1}{4}\beta^2(9\alpha^2 + 4\beta^2)^2 > 0$$

liefert. Man kann zeigen, dass $E(\mathbb{R})$ zusammenhängend ist, und dass $E(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}$ gilt.

(2) $x^3 + ax + b$ hat 3 reelle Nullstellen, also

$$x^3 + ax + b = (x - \alpha)(x - \beta)(x + \alpha + \beta),$$

was sofort

$$a = -\alpha^2 - \alpha\beta - \beta^2, \quad b = \alpha^2\beta + \alpha\beta^2$$

und damit

$$\Delta = -(\alpha + 2\beta)^2(2\alpha + \beta)^2(\alpha - \beta)^2 < 0$$

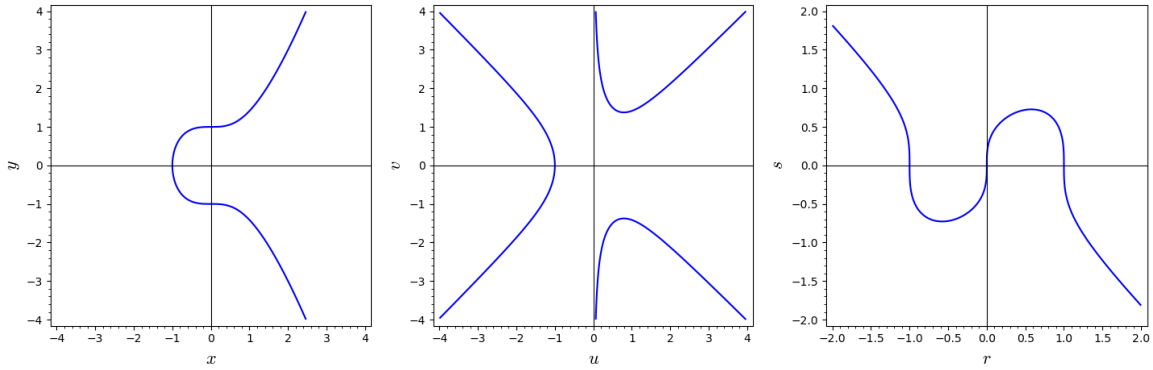
liefert. Man kann zeigen, dass $E(\mathbb{R})$ zwei Zusammenhangskomponenten hat, und dass gilt $E(\mathbb{R}) \simeq \mathbb{Z}/(2) \oplus \mathbb{R}/\mathbb{Z}$.

SATZ. *Ist E mit $y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbb{R}$, so gilt*

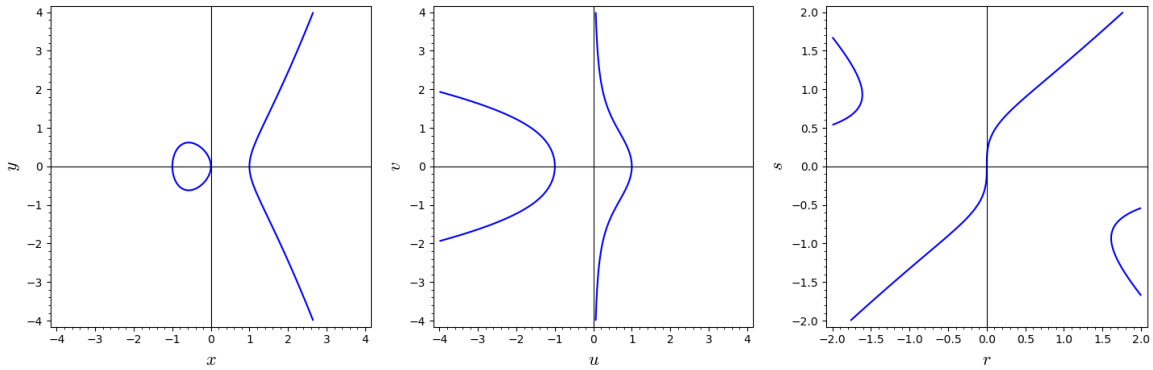
$$E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/\mathbb{Z} & \text{für } \Delta > 0 \\ \mathbb{Z}/(2) \oplus \mathbb{R}/\mathbb{Z} & \text{für } \Delta < 0. \end{cases}$$

Beispiele:

(1) $y^2 = x^3 + 1$ mit $\Delta = 27$:



(2) $y^2 = x^3 - x$ mit $\Delta = -4$:



KAPITEL 13

Hyperelliptische Kurven

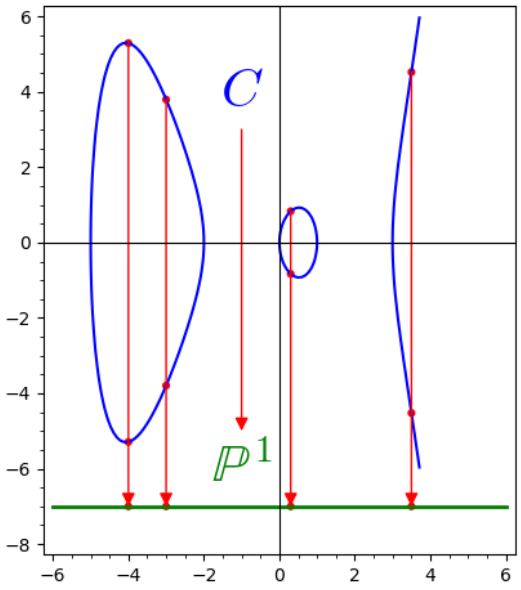
1. Einführung

Wir setzen in diesem Kapitel der Einfachkeit halber voraus, dass die Charakteristik des (vollkommenen) Grundkörpers K von 2 verschieden ist. Wenn nichts anderes gesagt wird, meint Kurve stets eine über K definierte, absolut irreduzible, nichtsinguläre, projektive Kurve.

DEFINITION. *Eine* **hyperelliptische Kurve** C *über* K *ist eine über* K *definierte, absolut irreduzible, nichtsinguläre, projektive Kurve vom Geschlecht* $g \geq 2$*, sodass ein über* K *definierter Morphismus*

$$\phi : C \to \mathbb{P}^1$$

vom Grad 2 *existiert.*



Wie kann man sich hyperelliptische Kurven konkret vorstellen?

LEMMA. *Ist* C *eine über* K *definierte, absolut irreduzible, nichtsinguläre, projektive Kurve und* $\phi : C \to \mathbb{P}^1$ *ein über* K *definierter Morphismus vom Grad* 2*, so gibt es Funktionen* $x, y \in K(C)$ *und ein separables Polynom* $f(X) \in K[X]$ *vom Grad* $n \geq 1$*, sodass gilt*

$$K(C) = K(x, y), \quad y^2 = f(x) \quad \text{und} \quad \phi = (1 : x).$$

Beweis:

---

(1) Bezeichnet $\widetilde{x}$ die Koordinatenfunktion von $\mathbb{P}^1$, so ist $K(\mathbb{P}^1) = K(\widetilde{x})$. Der Funktionenkörper $K(C)$ ist dann eine quadratische Erweiterung von $\phi^*K(\mathbb{P}^1) = \phi^*K(\widetilde{x}) = K(\phi^*(\widetilde{x}))$. Wir schreiben $x = \phi^*(\widetilde{x})$ und haben dann $\phi^*K(\mathbb{P}^1) = K(x)$. Da $K(C)$ eine quadratische Erweiterung von $K(x)$ ist, gibt es eine Funktion $y \in K(C)$, sodass y einer Gleichung
$$a(x)y^2 + b(x)y + c(x) = 0$$
genügt mit rationalen Funktionen $a(X), b(X), c(X) \in K(X)$. Es ist dann
$$K(C) = K(x, y) = K(x)[y].$$
(2) Wir ändern nun y ab, damit die y beschreibende Gleichung etwas einfacher aussieht.
(3) Wegen $y \notin K(x)$ ist $a(x) \neq 0$. Multiplizieren wir obige Gleichung mit $a(x)$, so können wir schreiben
$$(a(x)y)^2 + b(x)(a(x)y) + a(x)c(x) = 0.$$
Betrachten die statt y die Funktion $a(x) \cdot y$, so können wir $a(x) = 1$ annehmen. Die y beschreibende Gleichung wird dann zu
$$y^2 + b(x)y + c(x) = 0.$$
(4) Nun machen wir quadratische Ergänzung, wofür $\mathrm{char}(K) \neq 2$ wichtig ist:
$$\left(y + \frac{1}{2}b(x)\right)^2 = \frac{1}{4}b(x)^2 - c(x).$$
Betrachten wir also statt y die Funktion $y + \frac{1}{2}b(x)$, setzen wir $d(X) = \frac{1}{4}b(X)^2 - c(X)$, so genügt y der Gleichung
$$y^2 = d(x).$$
(5) Nun zerlegen wir in $K(X)$ die rationale Funktion $d(X)$ in das Produkt aus einem Quadrat $e(X)^2$ und einem quadratfreien Polynom $f(X)$:
$$d(X) = e(X)^2 \cdot f(X) \quad \text{mit} \quad e(X) \in K(X) \quad \text{und} \quad f(X) \in K[X] \text{ quadratfrei.}$$
Es ist
$$y^2 = e(x)^2 \cdot f(x).$$
Indem wir statt y die Funktion $\frac{y}{e(x)}$ betrachten, können wir $e(X) = 1$ annehmen, d.h. y genügt der Gleichung
$$y^2 = f(x),$$
wobei nun $f(X) \in K[X]$ ein quadratfreies Polynom ist. (Ist K algebraisch abgeschlossen, so kann man noch erreichen, dass $f(X)$ normiert ist.) Statt quadratfrei kann man natürlich auch separabel sagen, da der Grundkörper als vollkommen vorausgesetzt wurde. Damit ist das Lemma bewiesen. ■

Wir betrachten zunächst die einfachsten Fälle:

LEMMA. *Sei $f(x) \in K[x]$ ein separables Polynom vom Grad n mit $n \in \{1, 2, 3\}$ und C die durch $y^2 = f(x)$ definierte ebene projektive Kurve.*

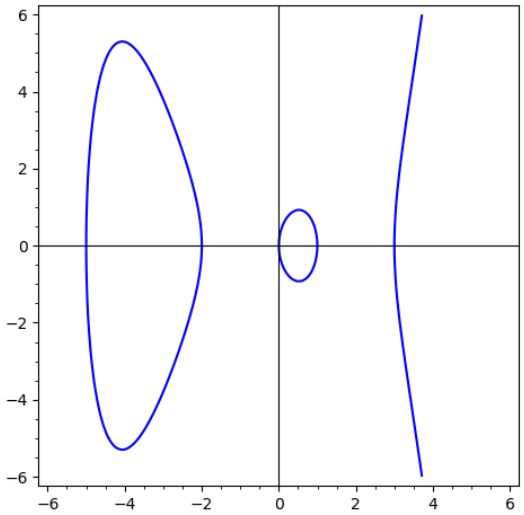
(1) *Im Fall $n = 1$ oder $n = 2$ ist C eine nichtsinguläre projektive ebene Quadrik und hat Geschlecht 0.*
(2) *Im Fall $n = 3$ ist C eine nichtsinguläre projektive ebene Kubik und hat Geschlecht 1.*

Beweis: Übungsaufgabe. ■

LEMMA. *Sei $f(x) \in K[x]$ ein separables Polynom vom Grad $n \geq 4$, d.h. es gibt eine Zahl $c \in K^*$ und paarweise verschiedene Zahlen $\gamma_1, \ldots, \gamma_n \in \overline{K}$ mit*
$$f(x) = c(x - \gamma_1) \ldots (x - \gamma_n).$$
und C_0 die durch
$$y^2 = f(x)$$
definierte projektive ebene Kurve.

(1) *C_0 ist nichtsingulär in Endlichen.*
(2) *C_0 besitzt genau einen Punkt im Unendlichen, nämlich $(0:0:1)$. Der Punkt $(0:0:1)$ ist eine Singularität von C_0.*
(3) *Für einen Punkt $(\alpha,\beta)\in C_0$ mit $\beta\neq 0$ ist $x-\alpha$ uniformisierend, für die Punkte $(\gamma_i,0)\in C$ $(i=1,\dots,n)$ ist y uniformisierend.*

Beispiel: $y^2=\frac{1}{10}x(x-1)(x-3)(x+2)(x+5)$



Beweis:

(1) C_0 wird im Endlichen beschrieben durch
$$g(x,y)=y^2-f(x).$$
Nun ist
$$\frac{\partial g}{\partial x}=-f'(x)\quad\text{und}\quad\frac{\partial g}{\partial y}=2y.$$
Ein Kurvenpunkt ist genau dann singulär, wenn gilt
$$y^2=f(x),\quad f'(x)=0,\quad y=0,\quad\text{also}\quad f(x)=f'(x)=0,\quad y=0.$$
Nun war aber $f(x)$ als separabel vorausgesetzt, weswegen $f(x)$ und $f'(x)$ keine gemeinsame Nullstelle haben. Daher besitzt C_0 keine Singularität im Endlichen. Für $(a,b)\in C_0$ lautet die Tangentengleichung
$$-f'(a)\cdot(x-a)+2b\cdot(y-b)=0.$$
(2) Der projektive Abschluss der affinen Kurve wird durch
$$x_0^{n-2}x_2^2=c(x_1-\gamma_1x_0)\dots(x_1-\gamma_nx_0)$$
beschrieben. Wegen $c\neq 0$ ist $(0:0:1)$ der einzige Punkt im Unendlichen. Verwenden wir die affinen Koordinaten r,s (von U_2) mit $(1:x:y)=(r:s:1)$, so wird die Kurve in U_2 zu
$$r^{n-2}=c(s-\gamma_1r)\dots(s-\gamma_nr).$$
Die Taylorentwicklung in $(r,s)=(0,0)$ ist
$$r^{n-2}-c(s-\gamma_1r)\dots(s-\gamma_nr).$$
Wegen $n\geq 4$ gibt es keinen linearen Term, sodass die Kurve hier singulär ist.
(3) Wir haben bereits unter (1) die Tangentengleichung für einen Punkt $(a,b)\in C_0$ hergeleitet:
$$-f'(a)\cdot(x-a)+2b\cdot(y-b)=0.$$
Ist $b\neq 0$, so ist also $x-a$ uniformisierend, ist $b=0$, so ist y uniformisierend. ■

SATZ. *Sei $f(x) \in K[X]$ ein separables Polynom vom Grad $n \geq 4$, C_0 die durch*

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

definierte projektive ebene Kurve, C ein nichtsinguläres Modell von C_0 (mit birationalem Morphismus $\pi : C \to C_0$) und $\phi : C \to \mathbb{P}^1$ der durch $\phi = (1 : x)$ gegebene Morphismus vom Grad 2. (Wir schreiben $f(x) = c(x - \gamma_1) \dots (x - \gamma_n)$ mit paarweise verschiedenen Zahlen $\gamma_1, \dots, \gamma_n \in \overline{K}$ und $c \in K^*$.)

(1) *Der birationale Morphismus liefert eine Isomorphie*

$$C \setminus \phi^{-1}(\infty) \simeq C_0 \setminus \{(0 : 0 : 1)\}.$$

(2) *Die im Endlichen gelegenen Verzweigungspunkte von ϕ sind genau die Punkte*

$$(\gamma_1, 0), (\gamma_2, 0), \dots, (\gamma_n, 0),$$

jeweils mit Verzweigungsindex 2.

(3) *Es gilt*

$$\#\phi^{-1}(\infty) = \begin{cases} 2, & \text{falls } n \text{ gerade ist,} \\ 1, & \text{falls } n \text{ ungerade ist.} \end{cases}$$

Wir schreiben

$$\phi^{-1}(\infty) = \begin{cases} \{\infty_1, \infty_2\}, & \text{falls } n \text{ gerade ist,} \\ \{\infty\}, & \text{falls } n \text{ ungerade ist.} \end{cases}$$

(4) *Für das Geschlecht von C gilt:*

$$g(C) = \begin{cases} \frac{n-2}{2}, & \text{falls } n \text{ gerade ist,} \\ \frac{n-1}{2}, & \text{falls } n \text{ ungerade ist} \end{cases} \qquad \text{bzw.} \qquad n = \begin{cases} 2g+2, & \text{falls } n \equiv 0 \bmod 2, \\ 2g+1, & \text{falls } n \equiv 1 \bmod 2. \end{cases}$$

(5) *Für ungerades n gilt*

$$\operatorname{ord}_\infty(x) = -2 \quad \text{und} \quad \operatorname{ord}_\infty(y) = -n.$$

Außerdem gilt

$$\operatorname{div}(y) = [(\gamma_1, 0)] + \dots + [(\gamma_n, 0)] - n[\infty]$$

und für $\alpha \in \overline{K}$

$$\operatorname{div}(x - \alpha) = [(\alpha, \sqrt{f(\alpha)})] + [(\alpha, -\sqrt{f(\alpha)})] - 2[\infty].$$

Für $\alpha = \gamma_i$ kann man natürlich auch schreiben

$$\operatorname{div}(x - \gamma_i) = 2[(\gamma_i, 0)] - 2[\infty].$$

(6) *Für gerades n gilt*

$$\operatorname{ord}_{\infty_1}(x) = \operatorname{ord}_{\infty_2}(x) = -1 \quad \text{und} \quad \operatorname{ord}_{\infty_1}(y) = \operatorname{ord}_{\infty_2}(y) = -\frac{n}{2}.$$

Beweis:

(1) Da $C_0 \setminus \{(0 : 0 : 1)\}$ nichtsingulär ist, ist

$$C \setminus \pi^{-1}((0 : 0 : 1)) \xrightarrow{\pi} C_0 \setminus \{(0 : 0 : 1)\}$$

ein Isomorphismus. Wir können also $C \setminus \pi^{-1}((0 : 0 : 1))$ mit $C_0 \setminus \{(0 : 0 : 1)\}$ identifzieren. Der Morphismus

$$C_0 \setminus \{(0 : 0 : 1)\} \to \mathbb{P}^1, \quad (x, y) \mapsto (1 : x)$$

liefert einen Morphismus $\phi : C \to \mathbb{P}^1$ vom Grad 2. Im Unendlichen gilt

$$\phi^{-1}(\infty) = \pi^{-1}((0 : 0 : 1)).$$

(2) Sei $(\alpha, \beta) \in C$.

- **Fall $\beta \neq 0$:** Dann ist $x - \alpha$ uniformisierend in (α, β). Nun ist $\phi((\alpha, \beta)) = \alpha$. Im Bildpunkt ist $\widetilde{x} - \alpha$ uniformisierend, woraus wegen $\phi^*(\widetilde{x} - \alpha) = x - \alpha$ sofort

$$e_\phi((\alpha, \beta)) = 1$$

folgt.

- **Fall** $\beta = 0$**:** Dann ist $(\alpha, \beta) = (\gamma_i, 0)$ für ein i. Im Bild ist $\widetilde{x} - \gamma_i$ uniformisierend, in $(\gamma_i, 0)$ die Funktion y. Es ist $e_\phi((\gamma_i, 0)) = \operatorname{ord}_{(\gamma_i,0)}(\phi^*(\widetilde{x} - \gamma_i)) = \operatorname{ord}_{(\gamma_i,0)}(x - \gamma_i)$. Aus

$$y^2 = (x - \gamma_1) \dots (x - \gamma_i) \dots (x - \gamma_n)$$

sieht man dann

$$e_\phi((\gamma_i, 0)) = \operatorname{ord}_{(\gamma_i,0)}(x - \gamma_i) = 2.$$

(3) Da ϕ Grad 2 hat, gilt

$$\sum_{P \in \phi^{-1}(\infty)} e_\phi(P) = 2.$$

Wegen $e_\phi(P) \in \mathbb{N}$ gibt es also nur zwei Möglichkeiten.

- **Fall** $\#\phi^{-1}(\infty) = 2$**:** Wir schreiben $\phi^{-1}(\infty) = \{\infty_1, \infty_2\}$. Mit obiger Formel folgt

$$e_\phi(\infty_1) = 1 \quad \text{und} \quad e_\phi(\infty_2) = 1.$$

ϕ ist also unverzweigt in den Punkten ∞_1, ∞_2. Die Riemann-Hurwitz-Formel liefert

$$2g - 2 = 2 \cdot (-2) + \sum_{i=1}^{n} e_\phi((\gamma_i, 0)) - 1),$$

also $2g - 2 = -4 + n$, und damit

$$2g = n - 2.$$

Daher ist in diesem Fall n eine gerade Zahl und es gilt

$$g = \frac{n-2}{2} \quad \text{bzw.} \quad n = 2g + 2.$$

- **Fall** $\#\phi^{-1}(\infty) = 1$**:** Wir schreiben $\phi^{-1}(\infty) = \{\infty\}$. (Natürlich hat hier ∞ auf der linken Seite der Gleichung eine andere Bedeutung als auf der rechten Seite.) Dann gilt $e_\phi(\infty) = 2$. Die Riemann-Hurwitz-Formel liefert

$$2g - 2 = 2 \cdot (-2) + (e_\phi(\infty) - 1) + \sum_{i=1}^{n} (e_\phi((\gamma_i, 0)) - 1),$$

also $2g - 2 = -4 + 1 + n$, und damit

$$2g = n - 1.$$

In diesem Fall muss n eine ungerade Zahl sein, und es gilt

$$g = \frac{n-1}{2} \quad \text{bzw.} \quad n = 2g + 1.$$

(4) Wir betrachten den Fall, dass n ungerade ist, d.h. dass $\phi^{-1}(\infty) = \{\infty\}$ gilt. Die Nullstellen von y sind offensichtlich $(\gamma_i, 0)$. Da y in diesen Punkten uniformisierend ist, ist der Nullstellendivisor von y

$$[(\gamma_1, 0)] + \dots + [(\gamma_n, 0)].$$

Da $\operatorname{div}(y)$ Grad 0 hat und es nur einen Punkt im Unendlichen gibt, folgt

$$\operatorname{div}(y) = [(\gamma_1, 0)] + \dots + [(\gamma_n, 0)] - n[\infty].$$

Sei $\alpha \in \overline{K}$. Setzt man $x = \alpha$ in $y^2 = f(x)$ ein, so folgt $y^2 = f(\alpha)$. Nach eventueller Fallunterscheidung und Betrachtung der Uniformisierenden erhält man

$$\operatorname{div}(x - \alpha) = [(\alpha, \sqrt{f(\alpha)})] + [(a, -\sqrt{f(\alpha)}] - 2[\infty].$$

Auf die weiteren Details verzichten wir hier.

(5) Auf den Fall, dass n gerade ist, gehen wir an dieser Stelle nicht näher ein. ■

Im Folgenden werden wir uns auf den Fall beschränken, dass n ungerade ist. Dann gibt es im Unendlichen nur einen Punkt. Es gilt dann $n = 2g + 1$. Außerdem ist dann ∞ ein Verzweigungspunkt.

FOLGERUNG. *Sei C eine hyperelliptische Kurve vom Geschlecht 2, gegeben durch eine Gleichung $y^2 = f(x)$ mit einem Polynom $f(x)$ vom Grad 5. Dann gilt:*

$$\begin{aligned}
\mathcal{L}(0\cdot[\infty]) &= \overline{K},\\
\mathcal{L}(1\cdot[\infty]) &= \overline{K},\\
\mathcal{L}(2\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x,\\
\mathcal{L}(3\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x,\\
\mathcal{L}(4\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x+\overline{K}\cdot x^2,\\
\mathcal{L}(5\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x+\overline{K}\cdot x^2+\overline{K}\cdot y,\\
\mathcal{L}(6\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x+\overline{K}\cdot x^2+\overline{K}\cdot y+\overline{K}\cdot x^3.
\end{aligned}$$

Beweis: Die Inklusionen $\supseteq$ folgen sofort aus

$$\operatorname{ord}_\infty(x) = -2, \quad \operatorname{ord}_\infty(x^2) = -4, \quad \operatorname{ord}_\infty(y) = -5, \quad \operatorname{ord}_\infty(x^3) = -6.$$

Nun gilt nach Riemann-Roch mit $K_C = 2[\infty]$ für $n \geq 3$

$$\ell(n\cdot[\infty] = n+1-2+\ell(2[\infty]-n[\infty]) = n-1+\ell((2-n)[\infty]) = n-1,$$

woraus dann für $n \geq 3$ die Gleichheiten folgen. ■

Ist C eine hyperelliptische Kurve, gegeben durch eine Gleichung $y^2 = f(x)$, so ist

$$\iota : C \to C, \quad (x,y) \mapsto (x,-y)$$

ein Automorphismus mit $\iota^2 = \mathrm{id}_C$. Der Automorphismus ι wird auch **hyperelliptische Involution** genannt. Für $P \in C$ gilt dann

$$\phi^{-1}(\phi(P)) = \{P, \iota(P)\} \quad \text{und} \quad \phi^*([\phi(P)]) = [P] + [\iota(P)].$$

Wir geben noch eine andere Charakterisierung hyperelliptischer Kurven.

SATZ. *Eine Kurve C vom Geschlecht $g \geq 2$ ist genau dann hyperelliptisch, wenn es einen Divisor D vom Grad 2 mit $\ell(D) = 2$ gibt.*

Beweis:

- Ist C hyperelliptisch und $\phi : C \to \mathbb{P}^1$ ein Morphismus vom Grad 2, so ist $D = \phi^*([\infty])$ ein Divisor vom Grad 2 und $1, x \in \mathcal{L}(D)$, also $\ell(D) \geq 2$. Schreibt man $D = [P_1] + [P_2]$, so gilt

  $$\overline{K} \subseteq \mathcal{L}([P_1] \subseteq \mathcal{L}([P_1]+[P_2]) = \mathcal{L}(D).$$

  Da C Geschlecht > 0 hat, gilt $\mathcal{L}([P_1]) = \overline{K}$. Da $\ell([P_1]+[P_2]) \leq \ell([P_1])+1$ gilt, folgt $\ell(D) = 2$.
- Ist D ein Divisor vom Grad 2 mit $\ell(D) = 2$, ist $\mathcal{L}(D) = \overline{K}\cdot f_0 + \overline{K}\cdot f_1$, so definiert

  $$\phi = (f_0 : f_1)$$

  einen Morphismus vom Grad 2. ■

FOLGERUNG. *Jede Kurve vom Geschlecht 2 ist hyperelliptisch.*

Beweis: Für jeden kanonischen Divisor K_C gilt $\operatorname{grad}(K_C) = 2\cdot 2 - 2 = 2$ und $\ell(K_C) = 2$. Der vorangegangene Satz liefert dann die Behauptung. ■

Beispiele: Hier sind Beispiele von hyperelliptischen Kurven, die über $\mathbb{F}_3$ durch eine Gleichung $y^2 = f(x)$ mit $\operatorname{grad}(f) = 5$ definiert sind.

$\#C(\mathbb{F}_3)$	$f(x)$	$C(\mathbb{F}_p)$
1	$x^5 + 2x + 2$	$\{\infty\}$
2	$x^5 + 2x^2 + 2$	$\{\infty, (2,0)\}$
3	$x^5 + x^2 + 2$	$\{\infty, (1,1), (1,2)\}$
4	$x^5 + 1$	$\{\infty, (0,1), (0,2), (2,0)\}$
5	$x^5 + 2x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2)\}$
6	$x^5 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$
7	$x^5 + 2x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$

2. Effektive kanonische Divisoren

SATZ. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$, gegeben durch eine Gleichung $y^2 = f(x)$ mit einem separablen Polynom $f(x) \in K[x]$ vom Grad $2g+1$.*

(1) *Die effektiven kanonischen Divisoren sind genau die Divisoren der Gestalt*

$$D = \sum_{i=1}^{r} ([(\alpha_i, \beta_i)] + [(\alpha_i, -\beta_i)]) + 2(g-1-r)[\infty]$$

mit Kurvenpunkten (α_i, β_i) und $r \leq g-1$.

(2) *Die effektiven kanonischen Divisoren sind genau die Divisoren der Gestalt*

$$\phi^*([P_1]) + \phi^*([P_2]) + \cdots + \phi^*([P_{g-1}]),$$

wo $P_1, \ldots, P_{g-1}$ beliebige Punkte in $\mathbb{P}^1$ sind.

(3) *Die effektiven kanonischen Divisoren sind genau die Divisoren der Gestalt*

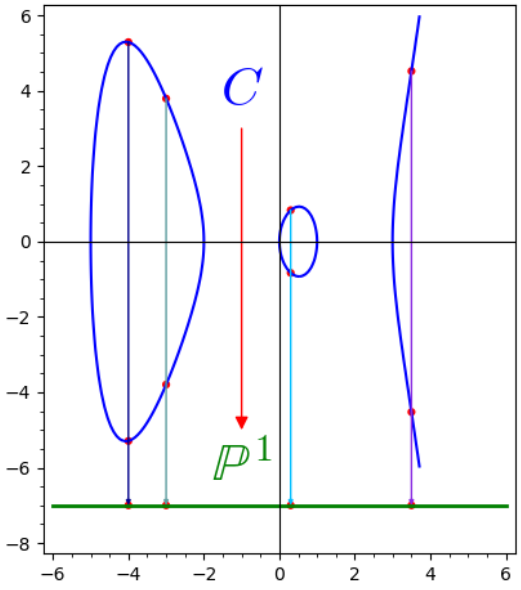
$$[P_1] + [\iota(P_1)] + [P_2] + [\iota(P_2)] + \cdots + [P_{g-1}] + [\iota(P_{g-1})],$$

wo $P_1, \ldots, P_{g-1}$ beliebige Punkte von C sind.

Beispiel: Bei einer hyperelliptischen Kurve vom Geschlecht 2 haben die effektiven kanonischen Divisoren also die Gestalt

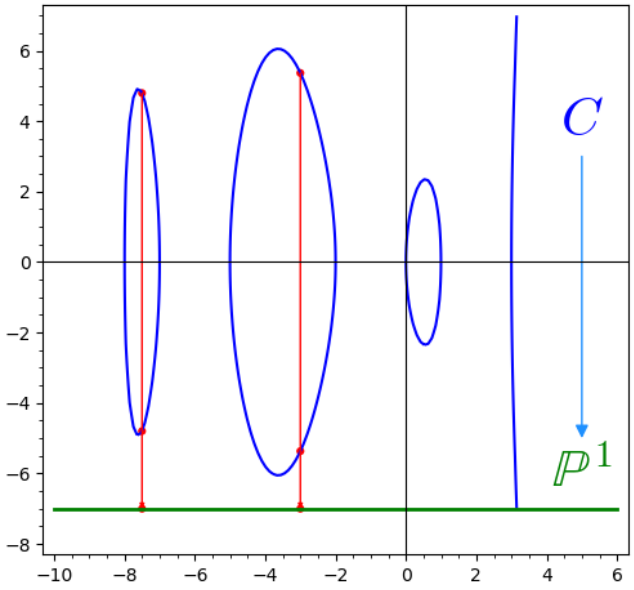
$$\phi^*([\widetilde{P}]) \text{ mit } \widetilde{P} \in \mathbb{P}^1 \quad \text{bzw.} \quad [P] + [\iota(P)] \text{ mit } P \in C.$$

Das Bild zeigt die Kurve $y^2 = \frac{1}{10}x(x-1)(x-3)(x+2)(x+5)$. Im Bild bilden je zwei „übereinanderliegende Punkte“ einen effektiven kanonischen Divisor.



Beispiel: $y^2 = \frac{1}{100}x(x-1)(x-3)(x+2)(x+5)(x+7)(x+8)$ definiert eine hyperelliptische Kurve vom Geschlecht 3. Die effektiven kanonischen Divisoren bestehen jeweils aus 4 Punkten der Form

$$[P_1] + [\iota(P_1)] + [P_2] + [\iota(P_3)] \text{ mit } P_1, P_2 \in C.$$



Beweis des Satzes:

(1) Ist $f(x) = c(x-\gamma_1)\dots(x-\gamma_{2g+1})$, so ist der Verzweigungsdivisor von ϕ

$$R = \sum_{i=1}^{2g+1} [(\gamma_i, 0)] + [\infty].$$

Wir wollen die Riemann-Hurwitz-Formel anwenden. Sei $\widetilde{x}$ die Koordinatenfunktion auf $\mathbb{P}^1$. Dann ist $x = \phi^*(\widetilde{x})$. Es ist

$$\operatorname{div}(d\widetilde{x}) = -2[\infty] \quad \text{und} \quad \phi^*(\operatorname{div}(d\widetilde{x})) = -4[\infty].$$

Es folgt

$$\begin{aligned} \operatorname{div}(dx) &= \operatorname{div}(\phi^*(d\widetilde{x})) = \phi^*(\operatorname{div}(d\widetilde{x})) + R = -4[\infty] + \sum_{i=1}^{2g+1} [(\gamma_i, 0)] + [\infty] = \\ &= \sum_{i=1}^{2g+1} [(\gamma_i, 0)] - 3[\infty]. \end{aligned}$$

(2) Der Divisor von y ist

$$\operatorname{div}(y) = \sum_{i=1}^{2g+1} [(\gamma_i, 0)] - (2g+1)[\infty].$$

Mit dem Divisor von dx ergibt sich

$$\operatorname{div}(\frac{dx}{y}) = 2(g-1)[\infty].$$

(3) Die Funktionen x^i mit $0 \le i \le g-1$ haben nur in ∞ eine Polstelle, und zwar gilt

$$\operatorname{ord}_\infty(x^i) = -2i \in \{0, -2, -4, \dots, -2(g-1)\}.$$

Es folgt

$$\operatorname{div}(x^i \cdot \frac{dx}{y}) \ge 0 \text{ für } i = 0, 1, \dots, g-1,$$

also

$$1, x, x^2, \ldots, x^{g-1} \in \mathcal{L}(\mathrm{div}(\frac{dx}{y})).$$

Wegen $\ell(K_C) = g$ folgt

$$\mathcal{L}(\mathrm{div}(\frac{dx}{y})) = \overline{K} \cdot 1 + \overline{K} \cdot x + \cdots + \overline{K} \cdot x^{g-1} = \{g(x) \in \overline{K}[x] : \mathrm{grad}(g(x)) \leq g-1\}.$$

Die Divisoren

$$\mathrm{div}(g(x)\frac{dx}{y}) \text{ mit } g(x) \in \{g(x) \in \overline{K}[x] : \mathrm{grad}(g(x)) \leq g-1\} \setminus \{0\}$$

sind dann genau die effektiven kanonischen Divisoren. Zerlegt man

$$g(x) = c(x-\alpha_1)\ldots(x-\alpha_r) \text{ mit } r \leq g-1,$$

so gilt wegen $\mathrm{div}(x-\alpha_i) = \phi^*([\alpha_i]) - 2[\infty]$

$$\begin{aligned} \mathrm{div}(g(x)\frac{dx}{y}) &= \sum_{i=1}^{r} \mathrm{div}(x-\alpha_i) + 2(g-1)[\infty] = \\ &= \sum_{i=1}^{r} (\phi^*([\alpha_i] - 2[\infty]) + 2(g-1)[\infty] = \\ &= \sum_{i=1}^{r} \phi^*([\alpha_i]) + 2(g-1-r)[\infty]. \end{aligned}$$

Mit $\phi^*([\alpha_i]) = [(\alpha_i, \beta_i)] + [(\alpha_i, -\beta_i)]$ ergibt sich die erste Darstellung. Die zweite folgt so:

$$\mathrm{div}(g(x)\frac{dx}{y}) = \sum_{i=1}^{r} \phi^*([\alpha_i]) + (g-1-r)\phi^*([\infty]).$$

Analog folgt die dritte Darstellung. Dies beweist die Behauptungen. ■

Mit diesem Hilfsmittel können wir folgenden Satz zeigen:

SATZ. *Eine nichtsinguläre projektive ebene Kurve C vom Geschlecht $g \geq 2$ ist nicht hyperelliptisch.*

Beweis: Sei $C \subseteq \mathbb{P}^2$ eine ebene Kurve vom Grad d. Wegen $g = \frac{1}{2}(d-1)(d-2)$ folgt $d \geq 4$. Sei K_C ein kanonischer Divisor von C und H der Divisor eines Geradenschnitts. Dann ist

$$K_C \sim (d-3)H$$

nach der Adjunktionsformel. Angenommen, C wäre hyperelliptisch mit hyperelliptischer Involution ι. Sei $P \in C$ mit $P \neq \iota(P)$. Sei $\ell = 0$ eine Gerade, die durch P, aber nicht durch $\iota(P)$ geht. Dann ist $\widetilde{K} = (d-3)\mathrm{div}(\ell)$ ein effektiver kanonischer Divisor, also

$$\widetilde{K} = (d-3)([P] + [P_2] + \cdots + [P_d]) = (d-3)[P] + (d-3)[P_2] + \cdots + (d-3)[P_d].$$

Da C nach Annahme hyperelliptisch ist, gibt es Punkte $P_2', \ldots, P_{g-1}'$ mit

$$\widetilde{K} = [P] + [\iota(P)] + [P_2'] + [\iota(P_2')] + \cdots + [P_{g-1}'] + [\iota(P_{g-1}')].$$

Da aber $\iota(P)$ kein Punkt der Geraden $\ell = 0$ ist, ist dies ein Widerspruch. ■

3. Reduzierte Divisoren - Beschreibung von $\mathrm{Pic}^0(C)$

Wir wollen die Divisorenklassengruppe $\mathrm{Pic}^0(C)$ für eine hyperelliptische Kurve C vom Geschlecht $g \geq 2$ mit genau einem Punkt ∞ im Unendlichen beschreiben. Früher haben wir für allgemeine Kurven C gezeigt, dass jeder Divisor vom Grad 0 zu einem Divisor der Gestalt

$$[P_1] + \cdots + [P_g] - g[\infty]$$

linear äquivalent ist. Eine wichtige Frage ist dann, wann zwei solcher Divisoren untereinander äquivalent sind.
Wird C gegeben durch

$$y^2 = c(x - \gamma_1) \dots (x - \gamma_{2g+1}),$$

so gilt für einen Punkt $P = (\alpha, \beta)$ mit der hyperelliptischen Involution ι

$$\mathrm{div}(x - \alpha) = [(\alpha, \beta)] + [(\alpha, -\beta)] - 2[\infty] = [P] + [\iota(P)] - 2[\infty].$$

Insbesondere gilt

$$[P] + [\iota(P)] \sim 2[\infty].$$

Es gilt auch $\mathcal{L}(2[\infty]) = \overline{K} \cdot 1 + \overline{K} \cdot x$, also $\ell(2[\infty]) = 2$.

LEMMA. *Ist C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$ mit ∞ als einzigem Punkt im Unendlichen, sind $P_1, \dots, P_n \in C$ (nicht notwendig verschiedene) Punkte mit $n \leq g$, dann gilt:*

$$\ell([P_1] + \cdots + [P_n]) \geq 2 \quad \Longleftrightarrow \quad \text{es gibt Indizes } i \neq j \text{ mit } P_j = \iota(P_i).$$

Beweis:

$\Longleftarrow$ Gibt es Indizes $i \neq j$ mit $P_j = \iota(P_i)$, so ist

$$[P_i] + [\iota(P_i)] = [P_i] + [P_j] \leq [P_1] + \cdots + [P_n],$$

und mit $[P_i] + [\iota(P_i)] \sim 2[\infty]$ und $\ell(2[\infty]) = 2$ folgt

$$2 = \ell(2[\infty]) = \ell([P_i] + [\iota(P_i)]) = \ell([P_i] + [P_j]) \leq \ell([P_1] + \cdots + [P_n]),$$

was die eine Richtung der Behauptung beweist.

$\Longrightarrow$ **Fall $n = g$:** Wir betrachten zunächst den Fall $n = g$ und setzen voraus, dass $\ell([P_1]+\cdots+[P_g]) \geq 2$ gilt. Riemann-Roch liefert, wenn K_C einen kanonischen Divisor bezeichnet,

$$2 \leq \ell([P_1] + \cdots + [P_g]) = g + 1 - g + \ell(K_C - ([P_1] + \cdots + [P_g])),$$

also

$$\ell(K - ([P_1] + \cdots + [P_g])) \geq 1.$$

Für $f \in \mathcal{L}(K_C - ([P_1]+\cdots+[P_g])) \setminus \{0\}$ folgt $K_C - ([P_1]+\cdots+[P_g]) + \mathrm{div}(f) \geq 0$. Da K_C Grad $2g-2$ hat gibt es Punkte $Q_1, \dots, Q_{g-2}$ mit $K_C - ([P_1]+\cdots+[P_g]) + \mathrm{div}(f) = [Q_1]+\cdots+[Q_{g-2}]$, also

$$K_C + \mathrm{div}(f) = [P_1] + \cdots + [P_g] + [Q_1] + \cdots + [Q_{g-2}].$$

Da $K_C + \mathrm{div}(f)$ ein effektiver kanonischer Divisor ist, gibt es Punkte $R_1, \dots, R_{g-1}$ mit

$$[P_1] + \cdots + [P_g] + [Q_1] + \cdots + [Q_{g-2}] = [R_1] + [\iota(R_1)] + \cdots + [R_{g-1}] + [\iota(R_{g-1})].$$

Also muss es Indizes $i \neq j$ geben mit $P_j = \iota(P_i)$, was wir zeigen wollten.
Fall $n < g$: Sei nun $n < g$ und $\ell(P_1 + \cdots + P_n) \geq 2$. Wir wählen einen Punkt Q mit $Q \neq \iota(Q)$ und

$$Q \notin \{P_1, \dots, P_n, \iota(P_1), \dots, \iota(P_n)\}.$$

Dann gilt

$$\ell([P_1] + \cdots + [P_n] + (g-n)[Q]) \geq \ell([P_1] + \cdots + [P_n]) \geq 2.$$

Nach dem eben Gezeigten gibt es Indizes $i \neq j$ mit $P_j = \iota(P_i)$, was wir zeigen wollten. ∎

DEFINITION. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$ mit genau einem Punkt ∞ im Unendlichen. Ein Divisor D vom Grad 0 heißt* **reduziert**, *wenn er die Gestalt*

$$D = [P_1] + \cdots + [P_n] - n[\infty]$$

hat, wobei folgende Eigenschaften erfüllt sind:

- $0 \leq n \leq g$, $P_i \neq \infty$. *(Die Punkte P_i müssen nicht verschieden sein.)*
- *Für Indizes $i \neq j$ ist $P_j \neq \iota(P_i)$.*

Die entscheidene Bedeutung reduzierter Divisoren kommt in folgendem Satz zum Ausdruck:

SATZ. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$ mit genau einem Punkt ∞ im Unendlichen. Jeder Divisor D vom Grad 0 ist dann zu genau einem reduzierten Divisor linear äquivalent. (Die Menge der reduzierten Divisoren ist also ein Repräsentantensystem der Divisorenklassengruppe $\mathrm{Pic}^0(C)$.)*

Beweis:

(1) Sei D ein Divisor vom Grad 0. Nach Riemann-Roch gilt:

$$\ell(D + g[\infty]) = g + 1 - g + \ell(K_C - (D + g[\infty]) \geq 1.$$

Wählt man $f \in \mathcal{L}(D + g[\infty]) \setminus \{0\}$, so ist $D + g[\infty] + \mathrm{div}(f) \geq 0$, d.h. es gibt Punkte $P_1, \ldots, P_g$ mit $D + g[\infty] + \mathrm{div}(f) = [P_1] + \cdots + [P_g]$. Es folgt

$$D \sim ([P_1] + \cdots + [P_g]) - g[\infty].$$

Sind einige der P_i identisch mit ∞, so können wir die Darstellung zu

$$D \sim ([P_1] + \cdots + [P_n]) - n[\infty] \quad \text{mit} \quad 0 \leq n \leq g$$

verkürzen. Gibt es jetzt Indizes $i \neq j$ mit $\iota(P_i) = P_j$, so ist

$$[P_i] + [P_j] - 2[\infty] = [P_i] + [\iota(P_i)] - 2[\infty] \sim 0,$$

also können wir die Darstellung weiter verkürzen. Dies geht, bis wir eine Darstellung

$$D \sim [P_1] + \cdots + [P_n] - n[\infty] \quad \text{mit} \quad 0 \leq n \leq g \text{ und } P_j \neq \iota(P_i) \text{ für } i \neq j$$

erreicht haben. Hier ist $[P_1] + \cdots + [P_n] - n[\infty]$ ein reduzierter Divisor.

(2) Seien $[P_1] + \cdots + [P_n] - n[\infty]$ und $[Q_1] + \cdots + [Q_m] - m[\infty]$ zwei reduzierte Divisoren, die linear äquivalent sind, d.h.

$$[P_1] + \cdots + [P_n] - n[\infty] \sim [Q_1] + \cdots + [Q_m] - m[\infty].$$

Wir können o.E. $n \geq m$ voraussetzen und erhalten dann

$$[P_1] + \cdots + [P_n] \sim [Q_1] + \cdots + [Q_m] + (n - m)[\infty].$$

Also gibt es $f \in \overline{K}(C)^*$ mit

$$[P_1] + \cdots + [P_n] + \mathrm{div}(f) = [Q_1] + \cdots + [Q_m] + (n - m)[\infty].$$

Daher sind $1, f \in \mathcal{L}([P_1] + \cdots + [P_n])$. Mit dem vorangegangenen Lemma folgt aber aus der Reduziertheit die Eigenschaft $\ell(P_1 + \cdots + P_n) = 1$, d.h. f ist konstant, was sofort $m = n$ und $[P_1] + \cdots + [P_n] = [Q_1] + \cdots + [Q_m]$ impliziert. ■

Wir wollen reduzierte Divisoren noch konkreter beschreiben. Dazu denken wir uns C gegeben durch $y^2 = f(x)$, wo $f(x)$ ein separables Polynom vom Grad $2g + 1$ ist.

- Ist D ein reduzierter Divisor, so können wir schreiben

$$D = \sum_{i=1}^{n} [(\alpha_i, \beta_i)] - n[\infty]$$

mit $n \leq g$ und $(\alpha_j, \beta_j) \neq \iota((\alpha_i, \beta_i))$ für $i \neq j$.

- Fassen wir gleiche Punkte zusammen, so können wir schreiben

$$D = \sum_{i=1}^{r} n_i \cdot [(\alpha_i, \beta_i)] - (\sum_{i=1}^{r} n_i)[\infty]$$

mit $(\alpha_i, \beta_i) \neq (\alpha_j, \beta_j)$ für $i \neq j$. Ist $\beta_i \neq 0$, so darf $(\alpha_i, -\beta_i)$ nicht vorkommen, was einfach durch $\alpha_i \neq \alpha_j$ für $i \neq j$ ausgedrückt werden kann. Ist $\beta_i = 0$, so muss $n_i = 1$ gelten. Natürlich muss auch $n_i \geq 1$ und $\sum_{i=1}^{r} n_i \leq g$ gelten.

Wir fassen dies zusammen:

LEMMA. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$, gegeben durch $y^2 = f(x)$ mit einem Polynom $f(x)$ vom Grad $2g+1$. Ein Divisor D ist genau dann reduziert, wenn er sich in der Form*

$$D = \sum_{i=1}^{r} n_i \cdot [(\alpha_i, \beta_i)] - (\sum_{i=1}^{r} n_i)[\infty]$$

schreiben lässt mit

- $r \geq 0$,
- $(\alpha_i, \beta_i) \in C$,
- $\alpha_i \neq \alpha_j$ *für* $i \neq j$,
- $n_i \geq 1$ *und* $\sum_{i=1}^{r} n_i \leq g$,
- $n_i = 1$, *falls* $\beta_i = 0$.

Beispiel: Wie sehen die reduzierten Divisoren für eine hyperelliptische Kurve vom Geschlecht 2 (mit genau einem Punkt ∞ im Unendlichen) aus?

- 0 ist ein reduzierter Divisor.
- Jeder Kurvenpunkt (α, β) liefert einen reduzierten Divisor $D = [(\alpha, \beta)] - [\infty]$.
- Ist (α, β) ein Kurvenpunkt mit $\beta \neq 0$, so ist auch $D = 2[(\alpha, \beta)] - 2[\infty]$ ein reduzierter Divisor.
- Sind $(\alpha_1, \beta_1), (\alpha_2, \beta_2)$ zwei Kurvenpunkte mit $\alpha_1 \neq \alpha_2$, so ist $D = [(\alpha_1, \beta_1)] + [(\alpha_2, \beta_2)] - 2[\infty]$ ein reduzierter Divisor.

DEFINITION. *Ist $f(x) \in K[x]$ ein separables Polynom vom Grad $2g+1$ mit $g \geq 2$, ist C die durch $y^2 = f(x)$ definierte hyperelliptische Kurve, so sei*

$$\mathcal{R}(f, K)$$

die Menge der über K definierten reduzierten Divisoren und

$$\mathcal{R}(f, \overline{K})$$

die Menge aller reduzierten Divisoren von C.

Da jede Divisorenklasse genau einen reduzierten Divisor enthält, ist klar, dass sowohl

$$\mathcal{R}(f, \overline{K}) \to \mathrm{Pic}^0(C)$$

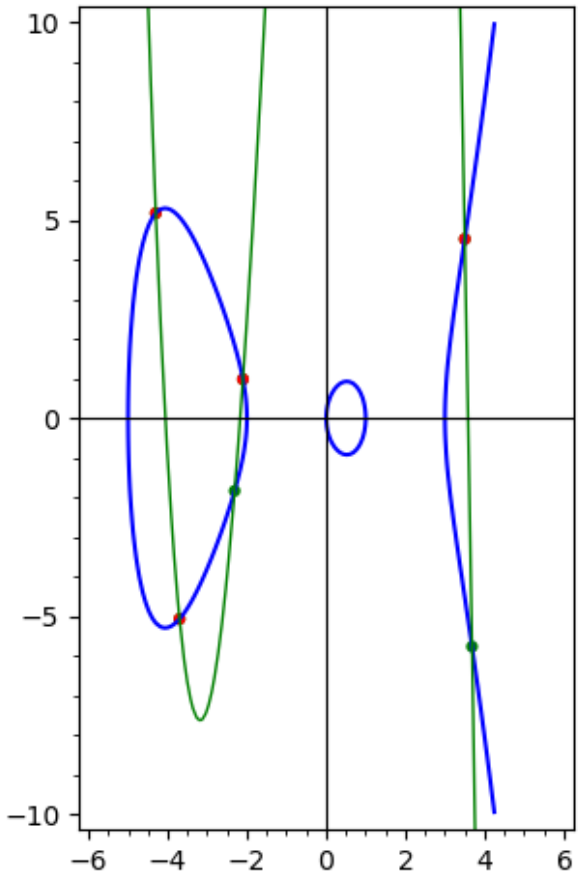
also auch

$$\mathcal{R}(f, K) \to \mathrm{Pic}^0_K(C)$$

ein Bijektionen sind.

Frage: Kann man die Addition in der Divisorenklassengruppe $\mathrm{Pic}^0(C)$ einer hyperelliptischen Kurve geometrisch deuten, ähnlich wie es bei ebenen Kubiken der Fall ist?

Überlegung: Sei C eine hyperelliptische Kurve vom Geschlecht 2, gegeben durch eine Gleichung $y^2 = f(x)$, wo $f(x)$ ein Polynom vom Grad 5 ist. Man sieht in diesem Zusammenhang manchmal Bilder folgender Art:



Seien $[P_1]+[P_2]-2[\infty]$ und $[Q_1]+[Q_2]-2[\infty]$ zwei Repräsentanten von Divisorenklassen. Wir schreiben

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad Q_1 = (x_3, y_3), \quad Q_2 = (x_4, y_4).$$

Wir nehmen an, dass alle x_i verschieden sind. Dann gibt es ein kubisches Polynom $g(x)$ mit

$$g(x_1) = y_1, \quad g(x_2) = y_2, \quad g(x_3) = y_3, \quad g(x_4) = y_4.$$

Die Punkte P_1, P_2, Q_1, Q_2 sind also Nullstellen der Funktion

$$y - g(x) \in \mathcal{L}(6 \cdot [\infty]).$$

Hat $g(x)$ Grad 3, so gilt $\mathrm{ord}_\infty(y - g(x)) = -6$, also gibt es zwei Punkte R_1, R_2 mit

$$\mathrm{div}(y - g(x)) = [P_1] + [P_2] + [Q_1] + [Q_2] + [R_1] + [R_2] - 6[\infty].$$

In der obigen Skizze sind die Punkte P_1, P_2, Q_1, Q_2 rot gezeichnet, die neuen Punkte R_1, R_2 grün. Grün ist auch die kubische Funktion $x \mapsto g(x)$ gezeichnet.
In $\mathrm{Pic}^0(C)$ gilt dann

$$\overline{[P_1]+[P_2]-2[\infty]} + \overline{[Q_1]+[Q_2]-2[\infty]} + \overline{[R_1]+[R_2]-2[\infty]} = 0.$$

Aus $[R_i] + [\iota(R_i)] \sim 2[\infty]$ folgt $-\overline{[R_i]-[\infty]} = \overline{[\iota(R_i)]-[\infty]}$, sodass wir erhalten

$$\overline{[P_1]+[P_2]-2[\infty]} + \overline{[Q_1]+[Q_2]-2[\infty]} = \overline{[\iota(R_1)]+[\iota(R_2)]-2[\infty]}.$$

Ähnlich wie bei ebenen Kubiken im Fall von Geschlecht 1 haben wir also die Addition in $\mathrm{Pic}^0(C)$ geometrisch gedeutet.

Wir werden diese eben vorgestellten Überlegungen nicht weiterverfolgen, sondern einen Weg einschlagen, der von der Zahlentheorie inspiriert ist.

Ist der Grundkörper K nicht algebraisch abgeschlossen, so ist obige Beschreibung reduzierter Divisoren für das Rechnen nicht besonders geeignet. Es gibt aber einen Weg, der zunächst nicht sehr motiviert erscheint.

Die folgenden Abschnitte müssen noch überarbeitet werden.

4. Beschreibung von reduzierten Divisoren durch Polynome

Vorbemerkung: Die hyperelliptische Kurve C vom Geschlecht $g \geq 2$ sei gegeben durch eine Gleichung $y^2 = f(x)$ mit einem separablen Polynom $f(x)$ vom Grad $2g+1$. Dann hat die Kurve genau einen Punkt im Unendlichen. Die affine Kurve $y^2 = f(x)$ hat den Koordinatenring

$$R = K[x,y]/(y^2 - f(x)) \simeq K[x][\sqrt{f(x)}] = \{a + b\sqrt{f} : a, b \in K[x]\}.$$

Ein (endlicher) Kurvenpunkt $P = (\alpha, \beta)$ liefert ein maximales Ideal in R:

$$\mathfrak{m}_P = (x - \alpha, y - \beta) = (x - \alpha, \beta - \sqrt{f}).$$

(Die folgenden Aussagen werden hier nicht bewiesen.) Die von 0 verschiedenen Ideale von R lassen sich darstellen in der Form

$$\mathfrak{a} = A\left(K[x] \cdot a + K[x] \cdot (b - \sqrt{f})\right)$$

mit Polynomen $A, a, b \in K[x]$, wobei A und a normiert sind, $\operatorname{grad}(b) < \operatorname{grad}(a)$ und

$$a \mid f - b^2, \quad \text{d.h.} \quad f \equiv b^2 \bmod a$$

gilt. Unter diesen Bedingungen sind die Polynome A, a, b eindeutig bestimmt. Die Bedingung $a \mid f - b^2$ kommt daher, dass $\mathfrak{a}$ unter Multiplikation mit $\sqrt{f}$ abgeschlossen sein muss; es ist nämlich

$$\sqrt{f} \cdot \begin{pmatrix} a \\ b - \sqrt{f} \end{pmatrix} = \begin{pmatrix} b & a \\ \frac{b^2 - f}{a} & -b \end{pmatrix} \begin{pmatrix} a \\ b - \sqrt{f} \end{pmatrix}.$$

Man kann zeigen, dass die Divisorenklassengruppe von C isomorph zur Klassengruppe des Ringes R ist. Der Ring R ist ähnlich aufgebaut wie die Ringe $\mathbb{Z}[\sqrt{-d}]$ für quadratfreie $d \in \mathbb{N}$ mit $d \not\equiv 3 \bmod 4$. Wie man dort Klassengruppen berechnet, überträgt sich auf die Kurvensituation.

Wir definieren

$$\mathcal{P}(f, K) = \{(a, b) : a, b \in K[x], \operatorname{grad}(b) < \operatorname{grad}(a) \leq g, a \text{ normiert }, f \equiv b^2 \bmod a\}.$$

Überlegungen:

(1) Sei $(a, b) \in \mathcal{P}(f, \overline{K})$. Wir faktorisieren zunächst a:

$$a(x) = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}$$

mit paarweise verschiedenen Zahlen $\alpha_1, \ldots, \alpha_r \in \overline{K}$ und $n_i \in \mathbb{N}$ mit $\sum_{i=1}^{r} n_i \leq g$.

(2) Aus $a \mid f - b^2$ folgt dann $(x - \alpha_i)^{n_i} \mid f - b^2$, also existiert ein Polynom c_i mit

$$(x - \alpha_i)^{n_i} c_i(x) = f(x) - b(x)^2.$$

Setzen wir $x = \alpha_i$ ein, so ergibt sich

$$f(\alpha_i) = b(\alpha_i)^2, \quad \text{d.h.} \quad (\alpha_i, b(\alpha_i)) \in C.$$

Ist $b(\alpha_i) = 0$, so gilt $x - \alpha_i \mid b(x)$, also $(x - \alpha_i)^2 \mid b(x)^2$. Da $f(x)$ separabel ist, muss $n_i = 1$ gelten.

(3) Daher ist

$$D = \sum_{i=1}^{r} n_i \cdot [(\alpha_i, b(\alpha_i))] - (\sum_{i=1}^{r} n_i)[\infty]$$

ein reduzierter Divisor.

(4) Damit haben wir eine Abbildung

$$\mathcal{P}(f,\overline{K}) \to \mathcal{R}(f,\overline{K})$$

definiert.

Wir werden jetzt herleiten, wie man umgekehrt einem reduzierten Divisor ein Element $(a,b) \in \mathcal{P}(f,\overline{K})$ zuordnen kann.

LEMMA. *Gegeben seien ein Körper K der Charakteristik $\neq 2$, ein Polynom $g(t) \in K[t]$ und eine Zahl $h_0 \in K \setminus \{0\}$ mit $g(0) = h_0^2$.*
Beginnend mit h_0 werden rekursiv werden Zahlen $h_1, h_2, h_3, \ldots$ wie folgt definiert: Kennt man für $n \geq 1$ bereits $h_0, h_1, \ldots, h_{n-1}$, ist c_n der Koeffizient des Polynoms $(\sum_{i=0}^{n-1} h_i t^i)^2 - g(t)$ bei t^n, d.h.

$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 - g(t) = \cdots + c_n t^n + \ldots,$$

so definiert man

$$h_n = -\frac{c_n}{2h_0}.$$

Dann gilt:

$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 \equiv g(t) \bmod t^n \text{ für alle } n \in \mathbb{N}.$$

Beweis: Wir beweisen die Aussage durch Induktion nach n. Für $n = 1$ folgt die Aussage einfach aus $h_0^2 = g(0)$. Sei nun $n \in \mathbb{N}$ und die Aussage bereits für n gezeigt, d.h.

$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 \equiv g(t) \bmod t^n.$$

Dann gilt mit der im Lemma definieren Zahl c_n

$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 - g(t) = c_n t^n + \text{ höhere Terme in } t.$$

Modulo t^{n+1} ergibt sich

$$\begin{aligned}
\left(\sum_{i=0}^{n} h_i t^i\right)^2 - g(t) &= \left(\sum_{i=0}^{n-1} h_i t^i + h_n t^n\right)^2 - g(t) = \\
&= \left(\sum_{i=0}^{n-1} h_i t^i\right)^2 + 2\left(\sum_{i=0}^{n-1} h_i t^i\right) \cdot h_n t^n + h_n^2 t^{2n} - g(t) = \\
&= \left(\sum_{i=0}^{n-1} h_i t^i\right)^2 - g(t) + \sum_{i=0}^{n-i} 2h_i h_n t^{i+n} + h_n^2 t^{2n} = \\
&= (c_n t^n + \ldots) + (2h_0 h_n t^n + \ldots) + \cdots = \\
&= (c_n + 2h_0 h_n) t^n + \cdots = 0 \cdot t^n + \cdots \equiv 0 \bmod t^{n+1}.
\end{aligned}$$

Dies beweist die Behauptung. ■

Eine zugehörige SAGE-Funktion könnte so aussehen:

```
def L(g,h0,n,K):
  R.<t>=K[]
  h=R(h0)
  for k in range(1,n):
    c=(h^2-g).coefficients(sparse=False)[k]
    h=h-c/(2*h0)*t^k
```

```
  return h
```

LEMMA. *Sei K ein Körper der Charakteristik $\neq 2$, $f(x) \in K[x]$, $x_0, y_0 \in K$ mit $y_0^2 = f(x_0)$, $y_0 \neq 0$ und $n \in \mathbb{N}$. Dann existiert ein Polynom $b(x) \in K[x]$ vom Grad $\leq n-1$ mit*

$$f(x) \equiv b(x)^2 \bmod (x-x_0)^n \quad \text{und} \quad b(x_0) = y_0.$$

Konkret: Wählt man im letzten Lemma $g(t) = f(x_0+t)$, $h_0 = y_0$, so erhält man ein Polynom $h(t) \in K[t]$ vom Grad $\leq n-1$ mit $h(t)^2 \equiv g(t) \bmod t^n$ und $h(0) = y_0$. Dann löst $b(x) = h(x-x_0)$ das Problem.

Beweis: Es gibt ein Polynom $\ell(t)$ mit

$$h(t)^2 = g(t) + t^n \cdot \ell(t).$$

Setzen wir nun $t = x - x_0$ ein, so ergibt sich

$$h(x-x_0)^2 = g(x-x_0) + (x-x_0)^n \ell(x-x_0).$$

Nun ist aber $g(x-x_0) = f(x)$, sodass sich

$$h(x-x_0)^2 = f(x) + (x-x_0)^n \cdot \ell(x-x_0)$$

ergibt. Mit $h(x_0-x_0) = h(0) = y_0$ folgt, dass $b(x) = h(x-x_0)$ das Problem löst. ■

```
def L0(g,h0,n,K):
  R.<t>=K[]
  h=R(h0)
  for k in range(1,n):
    c=(h^2-g).coefficients(sparse=False)[k]
    h=h-c/(2*h0)*t^k
  return h

def L(f,x0,y0,n,K):
  R.<x>=K[]
  S.<t>=K[]
  f=R(f)
  if y0^2!=f(x=x0):
    return 'Fehler: y0^2!=f(x0)!'
  g=f(x=x0+t)
  h=L0(g,y0,n,K)
  b=h(t=x-x0)
  return b
```

SATZ. *Sei K ein Körper der Charakteristik $\neq 2$, $f(x) \in K[x]$, Punkte (x_i, y_i) für $i = 1, \ldots, r$ mit paarweise verschiedenen Zahlen x_i und $y_i^2 = f(x_i)$, Zahlen $n_1, \ldots, n_r \in \mathbb{N}$, sodass $n_i = 1$ im Fall $y_i = 0$ gilt. Man definiere*

$$a(x) = (x-x_1)^{n_1} \ldots (x-x_r)^{n_r}.$$

Dann gibt es genau ein Polynom $b(x) \in K[x]$ mit $\operatorname{grad}(b) < \operatorname{grad}(a)$, sodass gilt

$$f(x) \equiv b(x)^2 \bmod a(x) \quad \text{und} \quad b(x_i) = y_i \text{ für } i = 1, \ldots, r.$$

Beweis: Mit dem vorangegangenen Lemma finden wir im Fall $y_i \neq 0$ Polynome $b_i(x)$ mit

$$f(x) \equiv b_i(x)^2 \bmod (x-x_i)^{n_i}, \quad \operatorname{grad}(b_i(x)) < n_i \quad \text{und} \quad b_i(x_i) = y_i.$$

Im Fall $y_i = 0$ wählen wir einfach $b_i(x) = 0$, sodass auch in diesem Fall die letzte Aussage gilt. Mit dem chinesischen Restsatz finden wir ein Polynom $b(x)$ mit

$$b(x) \equiv \begin{cases} b_1(x) \bmod (x - x_1)^{n_1}, \\ b_2(x) \bmod (x - x_2)^{n_2}, \\ \vdots \\ b_r(x) \bmod (x - x_r)^{n_r}. \end{cases}$$

Dabei können wir $\operatorname{grad}(b(x)) < n_1 + \cdots + n_r = \operatorname{grad}(a(x))$ annehmen. Auch $b(x_i) = y_i$ ist klar.
Warum ist $b(x)$ durch diese Bedingungen eindeutig bestimmt?

- Sei $\widetilde{b}(x)$ ein weiteres Polynom mit diesen Eigenschaften. Dann folgt

  $$\widetilde{b}(x)^2 \equiv f(x) \equiv b(x)^2 \bmod (x - x_i)^{n_i},$$

  also

  $$(x - x_i)^{n_i} \mid (\widetilde{b}(x) - b(x)) \cdot (\widetilde{b}(x) + b(x)).$$

  Im Fall $y_i \neq 0$ ist $\widetilde{b}(x_i) + b(x_i) = 2y_i \neq 0$, also gilt $x - x_i \nmid \widetilde{b}(x) + b(x)$. Daher folgt

  $$(x - x_i)^{n_i} \mid \widetilde{b}(x) - b(x),$$

  also

  $$\widetilde{b}(x) \equiv b(x) \bmod (x - x_i)^{n_i}.$$

  Im Fall $y_i = 0$ ist $\widetilde{b}(x_i) = b(x_i) = 0$, sodass natürlich auch hier

  $$\widetilde{b}(x) \equiv b(x) \bmod (x - x_i),$$

  und wegen $n_i = 1$ dann auch

  $$\widetilde{b}(x) \equiv b(x) \bmod (x - x_i)^{n_i}$$

  gilt.
- Es folgt $a(x) \mid \widetilde{b}(x) - b(x)$. Aus der Gradbedingung folgt dann $\widetilde{b}(x) = b(x)$. ■

FOLGERUNG. *Sei $f(x) \in K[x]$ ein separables Polynom vom Grad $2g + 1$ und C die durch $y^2 = f(x)$ definierte hyperelliptische Kurve vom Geschlecht g. Dann ist*

$$\mathcal{P}(f, \overline{K}) \to \mathcal{R}(f, \overline{K})$$

mit

$$(a(x), b(x)) \mapsto \sum_{i=1}^{r} n_i \cdot [(\alpha_i, b(\alpha_i)] - (\sum_{i=1}^{r} n_i)[\infty] \text{ mit } a(x) = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}$$

bijektiv. Schränkt man sich auf Divisoren, die über K definiert sind, ein, so erhält man eine Bijektion

$$\mathcal{P}(f, K) \simeq \mathcal{R}(f, K).$$

Wir erhalten damit eine Bijektion

$$\operatorname{Pic}_K^0(C) \simeq \mathcal{P}(f, K).$$

Im Folgenden werden wir die Elemente aus $\operatorname{Pic}_K^0(C)$ durch Polynompaare $(a(x), b(x)) \in \mathcal{P}(f, K)$ angeben. Diese Darstellung wird auch als **Mumford representation** bezeichnet.

Beispiele:

- Die Klasse $0 \in \operatorname{Pic}^0(C)$ wird durch $(1, 0)$ repräsentiert.
- Ist $(\alpha, \beta) \in C$, so wird die zugehörige Klasse $\overline{[(\alpha, \beta)] - [\infty]}$ durch das Paar $(x - \alpha, \beta)$ repräsentiert:

  $$(\alpha, \beta) \longrightarrow \overline{[(\alpha, \beta)] - [\infty]} \simeq (x - \alpha, \beta).$$

Beispiele: Wir betrachten hyperelliptische Kurven über $\mathbb{F}_3$ vom Geschlecht 2 mit genau einem Punkt im Unendlichen:

$\#C(\mathbb{F}_3)$	$\#\mathrm{Pic}^0_{\mathbb{F}_3}(C)$	f, $C(\mathbb{F}_3)$, $\mathrm{Pic}^0_{\mathbb{F}_3}(C)$
1	5	$f = x^5 + 2\,x + 2$ $C(\mathbb{F}_3) = \{\infty\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,\,(x^2+1,x)\,,\,(x^2+1,2x)\,,\,(x^2+x+2,x+1)\,,\,(x^2+x+2,2x+2)\}$
2	8	$f = x^5 + 2\,x^2 + 2$ $C(\mathbb{F}_3) = \{\infty,(2,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,\,(x+1,0)\,,\,(x^2+2x+2,x)\,,\,(x^2+2x+2,2x)\,,\,(x^2+x+2,1),$ $(x^2+1,2x+1)\,,\,(x^2+x+2,2)\,,\,(x^2+1,x+2)\}$
3	6	$f = x^5 + x^2 + 2$ $C(\mathbb{F}_3) = \{\infty,(1,1)\,,(1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x+2,1)\,,(x+2,2)\,,(x^2+2x+2,0)\,,(x^2+x+1,x+1)\,,$ $(x^2+x+1,2x+2)\}$
4	10	$f = x^5 + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(2,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+1,0)\,,(x^2+x+2,x)\,,(x^2+x+2,2x)\,,(x^2,1)\,,$ $(x^2+x,x+1)\,,(x^2,2)\,,(x^2+x,2x+2)\}$
5	14	$f = x^5 + 2\,x^2 + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(1,1)\,,(1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+2,1)\,,(x+2,2)\,,(x^2+x+2,0)\,,(x^2,1)\,,(x^2+2x,1),$ $(x^2+x+1,1)\,,(x^2+2x,x+1)\,,(x^2,2)\,,(x^2+2x,2)\,,(x^2+x+1,2),$ $(x^2+2x,2x+2)\}$
6	24	$f = x^5 + x^2 + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(1,0)\,,(2,1)\,,(2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+2,0)\,,(x+1,1)\,,(x+1,2)\,,(x^2,1)\,,(x^2+x,1),$ $(x^2+2x+1,1)\,,(x^2+x+2,x+1)\,,(x^2+2x+2,x+1)\,,(x^2+x,2x+1),$ $(x^2+2x,2x+1)\,,(x^2+1,2x+1)\,,(x^2+2,2x+1)\,,(x^2,2)\,,(x^2+x,2),$ $(x^2+2x+1,2)\,,(x^2+x,x+2)\,,(x^2+2x,x+2)\,,(x^2+1,x+2),$ $(x^2+2,x+2)\,,(x^2+x+2,2x+2)\,,(x^2+2x+2,2x+2)\}$
7	29	$f = x^5 + 2\,x + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(1,1)\,,(1,2)\,,(2,1)\,,(2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+2,1)\,,(x+2,2)\,,(x+1,1)\,,(x+1,2)\,,(x^2+2x+1,x),$ $(x^2+2,x)\,,(x^2+2x+2,x)\,,(x^2+2x+1,2x)\,,(x^2+2,2x)\,,(x^2+2x+2,2x),$ $(x^2+x,1)\,,(x^2+2x,1)\,,(x^2+1,1)\,,(x^2+2,1)\,,(x^2,x+1)\,,(x^2+2x,x+1),$ $(x^2+x+1,x+1)\,,(x^2+x,2x+1)\,,(x^2+x,2)\,,(x^2+2x,2)\,,(x^2+1,2),$ $(x^2+2,2)\,,(x^2+x,x+2)\,,(x^2,2x+2)\,,(x^2+2x,2x+2)\,,(x^2+x+1,2x+2)\}$

Beispiele: Nun betrachten wir hyperelliptische Kurven über $\mathbb{F}_3$ vom Geschlecht 2 mit $C(\mathbb{F}_3) = 3$. Die Beispiele zeigen verschiedene Möglichkeiten für $\mathrm{Pic}^0_{\mathbb{F}_3}(C)$.

$\#C(\mathbb{F}_3)$	$\#\mathrm{Pic}^0_{\mathbb{F}_3}(C)$	f, $C(\mathbb{F}_3)$, $\mathrm{Pic}^0_{\mathbb{F}_3}(C)$
3	4	$f = x^5 + x^3 + x^2 + 2x$ $C(\mathbb{F}_3) = \{\infty, (0,0), (2,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x,0), (x+1,0), (x^2+x, 0)\}$
3	5	$f = x^5 + x^2 + x + 2$ $C(\mathbb{F}_3) = \{\infty, (2,1), (2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+1,1), (x+1,2), (x^2+2x+1, x), (x^2+2x+1, 2x)\}$
3	6	$f = x^5 + x^2 + 2$ $C(\mathbb{F}_3) = \{\infty, (1,1), (1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+2,1), (x+2,2), (x^2+2x+2, 0), (x^2+x+1, x+1), (x^2+x+1, 2x+2)\}$
3	7	$f = x^5 + x^3 + x^2 + 2x + 2$ $C(\mathbb{F}_3) = \{\infty, (1,1), (1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+2,1), (x+2,2), (x^2+2x+2, x), (x^2+2x+2, 2x), (x^2+x+1, 1),$ $(x^2+x+1, 2)\}$
3	8	$f = x^5 + x^2 + x$ $C(\mathbb{F}_3) = \{\infty, (0,0), (1,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x,0), (x+2,0), (x^2+2x, 0), (x^2+x+2, x), (x^2+2x+2, x),$ $(x^2+x+2, 2x), (x^2+2x+2, 2x)\}$
3	9	$f = x^5 + x^3 + x^2 + 2$ $C(\mathbb{F}_3) = \{\infty, (2,1), (2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+1,1), (x+1,2), (x^2+1, 1), (x^2+2x+1, 1), (x^2+x+2, 2x+1),$ $(x^2+1, 2), (x^2+2x+1, 2), (x^2+x+2, x+2)\}$
3	10	$f = x^5 + x^2 + 2x + 1$ $C(\mathbb{F}_3) = \{\infty, (0,1), (0,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x,1), (x,2), (x^2+1, 0), (x^2, x+1), (x^2+x+2, 2x+1),$ $(x^2+2x+2, 2x+1), (x^2+x+2, x+2), (x^2+2x+2, x+2), (x^2, 2x+2)\}$
3	11	$f = x^5 + 2x^3 + x^2 + x + 2$ $C(\mathbb{F}_3) = \{\infty, (1,1), (1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+2,1), (x+2,2), (x^2+x+1, x), (x^2+x+1, 2x), (x^2+1, 1),$ $(x^2+x+2, 1), (x^2+2x+2, 2x+1), (x^2+1, 2), (x^2+x+2, 2), (x^2+2x+2, x+2)\}$

5. Addition in $\mathrm{Pic}^0_K(C)$

Wir identifizieren

$$\mathrm{Pic}^0_K(C) \simeq \{(a,b) \in K[x] \times K[x] : \mathrm{grad}(b) < \mathrm{grad}(a) \leq g, a \text{ normiert}, a \mid f - b^2\}.$$

Der folgende Algorithmus ist findet sich in [**Cohen-Frey**, S.308, Algorithm 14.7]. Er wird dort auch als **Algorithmus von Cantor** bezeichnet. (Wir werden die Richtigkeit des Algorithmus hier nicht beweisen.)

Eingabe: K, $f(x) \in K[x]$ separabel vom Grad $2g+1$
Eingabe: $(a_1, b_1), (a_2, b_2) \in \mathcal{P}(f, K)$
Ausgabe: $(a, b) \in \mathcal{P}(f, K)$ mit $(a, b) = (a_1, b_1) + (a_2, b_2)$ in $\mathrm{Pic}^0_K(C)$

1: $d_1 \leftarrow \mathrm{ggT}(a_1, a_2)$ und e_1, e_2 mit $d_1 = e_1 a_1 + e_2 a_2$
2: $d \leftarrow \mathrm{ggT}(d_1, b_1 + b_2)$ und c_1, c_2 mit $d = c_1 d_1 + c_2(b_1 + b_2)$
3: $s_1 \leftarrow c_1 e_1$, $s_2 \leftarrow c_1 e_2$, $s_3 \leftarrow c_2$
4: $a \leftarrow \frac{a_1 a_2}{d^2}$, $b \leftarrow \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a$
5: **while** $\mathrm{grad}(b) > g$ **do**
6: $\quad a \leftarrow \frac{f - b^2}{a}$
7: $\quad b \leftarrow (-b) \bmod a$
8: **end while**
9: Dividiere a durch den höchsten Koeffizienten, sodass a dann normiert ist
10: **return** (a, b)

Eine zugehörige SAGE-Funktion könnte so aussehen:

```
def hek_add(ab1,ab2,f,K):
  R.<x>=K[]
  f=R(f)
  g=(f.degree()-1)/2
  a1,b1=ab1
  a2,b2=ab2
  a1,b1,a2,b2=R(a1),R(b1),R(a2),R(b2)
  d1,e1,e2=a1.xgcd(a2)
  d,c1,c2=d1.xgcd(b1+b2)
  s1,s2,s3=c1*e1,c1*e2,c2
  a,_=(a1*a2).quo_rem(d^2)
  b,_=(s1*a1*b2+s2*a2*b1+s3*(b1*b2+f)).quo_rem(d)
  b=b%a
  while a.degree()>g:
    a,_=(f-b^2).quo_rem(a)
    b=(-b)%a
  if a.leading_coefficient()!=1:
    a=a/a.leading_coefficient()
  return (a,b)
```

Um in $\mathrm{Pic}_K^0(C)$ das n-fache von $\mathfrak{a}$ zu berechnen, benutzen wir eine „square-and-multiply“-Methode:
Eingabe: K, $f(x) \in K[x]$ separabel vom Grad $2g+1$
Eingabe: $\mathfrak{a} \in \mathrm{Pic}_K^0(C)$, $n \in \mathbb{N}_0$
Ausgabe: $n \cdot \mathfrak{a} \in \mathrm{Pic}_K^0(C)$

1: $\mathfrak{b} = (1,0)$, $\mathfrak{c} = \mathfrak{a}$
2: **while** $n > 0$ **do**
3: **if** $n \bmod 2 = 0$ **then**
4: $\mathfrak{c} \leftarrow \mathfrak{c} + \mathfrak{c}$, $n \leftarrow \left\lfloor \frac{n}{2} \right\rfloor$
5: **else**
6: $\mathfrak{b} \leftarrow \mathfrak{b} + \mathfrak{c}$, $n \leftarrow n - 1$
7: **end if**
8: **end while**
9: **return** $\mathfrak{b}$

Beispiel: Über $\mathbb{Q}$ betrachten wir die durch

$$f = -4\,x^5 + 8\,x^3 + 8\,x^2 + 4\,x + 1$$

definierte hyperelliptische Kurve C vom Geschlecht 2. In $C(\mathbb{Q})$ gibt es den Punkt $(0,1)$, der in $\mathrm{Pic}^0(C)$ durch $\mathfrak{a} = (x,1)$ dargestellt wird. Wir berechnen die Vielfachen:

n	$n \cdot \mathfrak{a}$
1	$(x, 1)$
2	$\left(x^2, 2x+1\right)$
3	$\left(x^2+x, -1\right)$
4	$(x+1, -1)$
5	$\left(x^2+x, 2x+1\right)$
6	$\left(x^2-x-1, -2x-1\right)$
7	$\left(x^2+2x+1, -4x-3\right)$
8	$\left(x^2+2x+1, 4x+3\right)$
9	$\left(x^2-x-1, 2x+1\right)$
10	$\left(x^2+x, -2x-1\right)$
11	$(x+1, 1)$
12	$\left(x^2+x, 1\right)$
13	$\left(x^2, -2x-1\right)$
14	$(x, -1)$
15	$(1, 0)$

Also hat $\mathfrak{a}$ Ordnung 15 in der Divisorenklassengruppe.

6. Anwendungen in der Kryptographie

Heutzutage werden elliptische Kurven über endlichen Körpern kryptographisch eingesetzt. Offizielle staatliche Informationen dazu gibt es beispielsweise in Deutschland beim BSI (Bundesamt für Sicherheit in der Informationstechnik) BSI TR-03111: Elliptic Curve Cryptography und in den USA beim NIST (National Institute of Standards and Technology) NIST: Elliptic Curve Cryptography.

Wir stellen hier ein **Schlüsseleinigungsverfahren** vor, das Diffie und Hellman in ihrer Arbeit „New Directions in Cryptography“ 1976 vorgeschlagen haben [**Diffie-Hellman**]. Aktuelle Informationen zum Thema „Schlüsseleinigungsverfahren“ findet man wieder beim Bundesamt für Sicherheit in der Informationstechnik BSI TR-02102-1.

Situation: Zwei Personen A und B (oder zwei durch das Internet verbundene Rechner oder ...) wollen sich auf einen gemeinsamen Schlüssel einigen um dann damit ein Verschlüsselungsverfahren mit dem gleichen Schlüssel benutzen zu können.

Diffie-Hellman-Schlüsselaustausch (multiplikative Version)

- Sei G eine multiplikativ geschriebene Gruppe (oder Halbgruppe), in der sich zwei Elemente schnell multiplizieren lassen. (Dann lassen sich auch Potenzen a^n für $a \in G$ und $n \in \mathbb{N}$ mit einer „square-and-multiply“-Methode schnell berechnen.)
- Sei weiter $g \in G$.
- A wählt sich eine Zahl $e_A \in \mathbb{N}$ und berechnet
$$f_A = g^{e_A} \in G.$$
A gibt f_A als seinen öffentlichen Schlüssel (public key) bekannt. e_A ist der geheime Schlüssel (private key oder secret key) von A.
- B wählt sich eine Zahl $e_B \in \mathbb{N}$ und berechnet
$$f_B = g^{e_A} \in G.$$
B gibt f_B als seinen öffentlichen Schlüssel bekannt. e_B ist der geheime Schlüssel von B.
- Der gemeinsame Schlüssel von A und B ist
$$k_{AB} = g^{e_A e_B}.$$
A kann sich diesen gemeinsamen Schlüssel wegen $k_{AB} = g^{e_A e_B} = (g^{e_B})^{e_A} = f_B^{e_A}$ als
$$k_{AB} = f_B^{e_A}$$

berechnen, da A den öffentlichen Schlüssel f_B und seinen eigenen geheimen Schlüssel e_A kennt. Analog kann sich B den gemeinsamen Schlüssels mittels der Gleichung

$$k_{AB} = f_A^{e_B}$$

berechnen.

- Wann ist dieses Schlüsselaustauschverfahren sicher? Ein Außenstehender C kennt g, f_A, f_B bzw. g, g^{e_A}, g^{e_B}. Wie kann man aus diesen drei Größen $g^{e_A e_B}$ berechnen?

$$g, g^{e_A}, g^{e_B} \xrightarrow{\text{Wie erhält aus den Größen links, die Größe rechts?}} g^{e_A e_B}$$

  Dies nennt man das Diffie-Hellman-Problem.
- Wenn C einen **diskreten Logarithmus** von f_A zur Basis g in G berechnen kann, d.h. eine Zahl $\ell \in \mathbb{N}$ mit

$$g^\ell = f_A,$$

  so erhält C leicht den gemeinsamen Schlüssel:

$$k_{AB} = f_A^{e_B} = g^{\ell e_B} = f_B^\ell.$$

- Für die Sicherheit ist es daher ganz wichtig, dass sich diskrete Logarithmen in der Gruppe G (im Allgemeinen) praktisch nicht berechnen lassen.

Der (klassische) Diffie-Hellman-Schlüsselaustausch arbeitet mit der multiplikativen Gruppe $\mathbb{F}_p^*$ eines endlichen Körpers $\mathbb{F}_p$.

Beispiel: Als Gruppe wird $\mathbb{F}_p^*$ mit nachfolgender 256-Bit-Primzahl p. Öffentlich bekannt seien folgende Zahlen:

$$\begin{aligned}
p &= 115792089237316195423570985008687907853269984665640564039457584007913129603823,\\
g &= 5,\\
f_A &= 64962785370846188965139123186170717661240903020815441595800807346182307706906,\\
f_B &= 45104316737573767517415679239486371089462170346686659863014273814977828980340.
\end{aligned}$$

Man versuche, daraus den gemeinsamen Schlüssel $k_{AB} = g^{e_A e_B} \in \mathbb{F}_p^*$ zu berechnen.

Da die Verknüpfung auf elliptischen Kurven und in der Divisorenklassengruppe von hyperelliptischen Kurven additiv geschrieben wird, schreiben wir den Diffie-Hellman-Schlüsselaustausch auch noch additiv auf:

Diffie-Hellman-Schlüsselaustausch (additive Version)

- Sei G eine additiv geschriebene Gruppe (oder Halbgruppe), in der sich zwei Elemente schnell addieren lassen. (Dann lässt sich auch für $a \in G$ und $n \in \mathbb{N}$ das Produkt $n \cdot a$ mit einer „square-and-multiply“-Methode schnell berechnen.)
- Sei weiter $g \in G$.
- A wählt sich eine Zahl $e_A \in \mathbb{N}$ und berechnet

$$f_A = e_A \cdot g \in G.$$

  A gibt f_A als seinen öffentlichen Schlüssel bekannt. e_A ist der geheime Schlüssel von A.
- B wählt sich eine Zahl $e_B \in \mathbb{N}$ und berechnet

$$f_B = e_B \cdot g \in G.$$

  B gibt f_B als seinen öffentlichen Schlüssel bekannt. e_B ist der geheime Schlüssel von B.
- Der gemeinsame Schlüssel von A und B ist

$$k_{AB} = e_A e_B \cdot g,$$

  den sich A mittels der Gleichung

$$k_{AB} = e_A \cdot f_B$$

und B mittels der Gleichung

$$k_{AB} = e_B \cdot f_A$$

berechnen können.

- Das Diffie-Hellman-Problem schreibt sich additiv so:

$$g, \quad e_A \cdot g, \quad e_B \cdot g \xrightarrow{\text{Wie erhält man aus den Größen links die rechte Seite?}} e_A e_B \cdot g.$$

Der Diffie-Hellman-Schlüsselaustausch ist sicher, solange sich das Diffie-Hellman-Problem praktisch nicht lösen lässt.

- Kann ein Außenstehender C in G einen **diskreten Logarithmus** von f_A zur Basis g berechnen, d.h. ein $\ell \in \mathbb{N}$ mit

$$f_A = \ell \cdot g,$$

so kann sich C auch den gemeinsamen Schlüssel so berechnen:

$$k_{AB} = e_A e_B \cdot g = e_B \cdot (e_A \cdot g) = e_B \cdot f_A = e_B \cdot (\ell \cdot g) = \ell \cdot (e_B \cdot g) = \ell \cdot f_B.$$

(In Analogie zur multiplikativen Version spricht man auch hier von diskreten Logarithmen.)

- Die Gruppe G muss also so beschaffen sein, dass sich diskrete Logarithmen praktisch nicht berechnen lassen.

Beispiel: Wir starten mit der 128-Bit-Primzahl

$$p = 2^{128} - 2487 = 340282366920938463463374607431768208969$$

und der durch

$$y^2 = x^5 + 13x$$

über $\mathbb{F}_p$ definierten hyperelliptischen Kurve vom Geschlecht 2. Die Kurve enthält den Punkt

$$(-13, 285852928819727726285868778105170894 33),$$

der in Pic^0 durch das Polynompaar

$$g = (x + 13, 285852928819727726285868778105170894 33)$$

repräsentiert wird. Da die Anzahl der $\mathbb{F}_p$-rationalen Punkte in der Größenordnung von $p^2 \approx 2^{256}$ (mit 78 Dezimalstellen) ist, wählen sich A und B unabhängig voneinander geheim zufällige 78-stellige Zahlen:

$$\begin{aligned} e_A &= 580319470382655966752835662324659168309974697178860516645533695751153002193277, \\ e_B &= 239109625614480018658086848783454775487453455922591154544399323497106959176065 \end{aligned}$$

berechnen damit ihre öffentlichen Schlüssel $f_A = e_A \cdot g$ bzw. $f_B = e_B \cdot g$ (in Pic^0)

$$\begin{aligned} f_A &= (x^2 + 187463483300877865555744358426021948548x + 173980684735284072477484642855119428093, \\ &\quad 312665874328081155780823073521258635811x + 109239510534601665073609894657722958853, \\ f_B &= (x^2 + 315410667712437507494356901716774216242x + 174070099365157486861119806563952150122, \\ &\quad 273079014832786731550022518067456128940x + 293097856848975605637487900771010101861) \end{aligned}$$

und geben diese öffentlich bekannt. Der gemeinsame Schlüssel von A und B ist dann

$$\begin{aligned} k_{AB} &= (x^2 + 164581974200092893758430516115421764363x + 156551275646432782596354239240206 18353, \\ &\quad 242847628149725977241194695079710562435x + 228888472326255063036427011105138660978), \end{aligned}$$

wobei sich A und B den gemeinsamen Schlüssel über eine der Gleichungen

$$k_{AB} = e_A \cdot f_B = e_B \cdot f_B$$

berechnet haben. Will man eine einzige Zahl als Schlüssel haben, könnte man beispielsweise die Koeffizienten bei x und 1 der ersten Komponente von k_{AB} aneinanderhängen:

$$16458197420009289375843051611542176436315655127564643278259635423924020618353.$$

Aufgaben

Aufgabe 1: Bestimme alle Geraden in $\mathbb{R}^2$, die sowohl den Kreis $K_1(0,0)$ also auch den Kreis $K_2(4,0)$ berühren. Die folgenden Teilaufgaben sind als Anleitung gedacht:

(1) Unter welchen Bedingungen an a und b berührt die Gerade $y = ax + b$ den Kreis $K_1(0,0)$?
(2) Unter welchen Bedingungen an a und b berührt die Gerade $y = ax + b$ den Kreis $K_2(4,0)$?
(3) Bestimme alle reellen Zahlen a, b, für die die Gerade $y = ax + b$ beide Kreise berührt.
(4) Bestimme alle Geraden, die beide Kreise berühren.

Aufgabe 2: Sei $K = \{(x,y) \in \mathbb{Q} \times \mathbb{Q} : x^2 + y^2 = 1\} \setminus \{(0,1)\}$. In der Vorlesung wurde gezeigt, dass

$$\mu : \mathbb{Q} \to K, \quad t \mapsto (\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$$

bijektiv ist mit der Umkehrabbildung

$$\lambda : K \to \mathbb{Q}, \quad (x,y) \mapsto \frac{x}{1-y}.$$

Erfüllt $(x,y) \in \mathbb{Q} \times \mathbb{Q}$ die Bedingung $x^2 + y^2 = 1$, so gilt dies offensichtlich auch für die Punkte $(-x,y)$, $(x,-y)$, $(-x,-y)$, (y,x), $(-y,x)$, $(y,-x)$, $(-y,-x)$. Sei $(x,y) \in \mathbb{Q}\times\mathbb{Q}\setminus\{(\pm 1,0),(0,\pm 1)\}$ und $(x,y) = \mu(t)$. Bestimme in Abhängigkeit von t Zahlen $t_2, \ldots, t_8$ mit

$$\mu(t_2) = (-x,y), \quad \mu(t_3) = (x,-y), \quad \mu(t_4) = (-x,-y),$$
$$\mu(t_5) = (y,x), \quad \mu(t_6) = (-y,x), \quad \mu(t_7) = (y,-x), \quad \mu(t_8) = (-y,-x).$$

Aufgabe 3: Sei $P = \{(a,b,c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} : a^2 + b^2 = c^2, \mathrm{ggT}(a,b,c) = 1\}$ die Menge der primitiven pythagoräischen Tripel. In der Vorlesung wurde angegeben, dass die Abbildung

$$\alpha : P \to \mathbb{Q}_{>1}, \quad (a,b,c) \mapsto \frac{a}{c-b}$$

bijektiv ist mit der Umkehrabbildung

$$\beta : \mathbb{Q}_{>1} \to P, \quad \frac{m}{n} \mapsto \begin{cases} (2mn, m^2-n^2, m^2+n^2), & \text{falls } m \text{ oder } n \text{ gerade ist,} \\ (mn, \frac{m^2-n^2}{2}, \frac{m^2+n^2}{2}), & \text{falls } m \text{ und } n \text{ ungerade sind,} \end{cases}$$

wobei $m, n \in \mathbb{N}$, $\mathrm{ggT}(m,n) = 1$ und $m > n$ vorausgesetzt wird.
Mit (a,b,c) ist auch (b,a,c) ein primitives pythagoräisches Tripel. Ist nun $q = \alpha((a,b,c))$, so gibt es genau eine Zahl $\tau(q) \in \mathbb{Q}_{>1}$ mit $\tau(q) = \alpha((b,a,c))$. Beschreibe

$$\tau : \mathbb{Q}_{>1} \to \mathbb{Q}_{>1}$$

explizit.

Datei: algku_u.tex. Version vom 21.7.2021

Aufgabe 4: Sei N eine Kongruenzzahl und (a, b, c) ein zugehöriges rationales Tripel, d.h. $a, b, c \in \mathbb{Q}_{>0}$, $a^2 + b^2 = c^2$ und $N = \frac{1}{2}ab$. In der Vorlesung wurde gezeigt, dass dann der Punkt (x, y) mit

$$x = \frac{Na}{c-b}, \quad y = \frac{2N^2}{c-b}$$

ein Punkt der Kurve $y^2 = x^3 - N^2x$ ist.
Da auch (b, a, c) ein zu N gehöriges rationales Tripel ist, ist auch (x', y') mit

$$x' = \frac{Nb}{c-a}, \quad y' = \frac{2N^2}{c-a}$$

ein Punkt der Kurve $y^2 = x^3 - N^2x$. Auch $(N, 0)$ ist offensichtlich ein Punkt der Kurve $y^2 = x^3 - N^2x$. Zeige, dass die drei Kurvenpunkte

$$(x, y), \quad (x', y'), \quad (N, 0)$$

auf einer Geraden liegen.

Hinweis: Drei Punkte (x_1, y_1), (x_2, y_2), (x_3, y_3) liegen genau dann auf einer Geraden, wenn gilt

$$\begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix} = 0.$$

Aufgabe 5: Zeige für $N \in \mathbb{N}$:

(1) Gibt es $x, y, z \in \mathbb{Q}_{>0}$ mit

$$x^2 - N = y^2 \quad \text{und} \quad x^2 + N = z^2,$$

definiert man

$$a = z - y, \quad b = z + y, \quad c = 2x,$$

so gilt

$$a, b, c \in \mathbb{Q}_{>0}, \quad a^2 + b^2 = c^2, \quad N = \frac{1}{2}ab,$$

d.h. N ist Kongruenzzahl.

(2) Gibt es $a, b, c \in \mathbb{Q}_{>0}$ mit $a^2 + b^2 = c^2$, $a < b$ und $N = \frac{1}{2}ab$, definiert man

$$x = \frac{1}{2}c, \quad y = \frac{1}{2}(b - a), \quad z = \frac{1}{2}(b + a),$$

so gilt

$$x, y, z \in \mathbb{Q}_{>0}, \quad x^2 - N = y^2, \quad x^2 + N = z^2.$$

(3) N ist genau dann eine Kongruenzzahl, wenn für die über $\mathbb{Q}$ definierte algebraische Menge

$$X_N = \{(x, y, z) \in \mathbb{A}^3 : x^2 - N = y^2, x^2 + N = z^2\}$$

die Menge $X_N(\mathbb{Q})$ der $\mathbb{Q}$-rationalen Punkte nicht leer ist.

Bemerkung: Um 1220 hat Leonardo da Pisa (Fibonacci) gezeigt, dass gilt

$$(\frac{41}{12})^2 - 5 = (\frac{31}{12})^2, \quad (\frac{41}{12})^2 + 5 = (\frac{49}{12})^2,$$

und somit bewiesen, dass 5 eine Kongruenzzahl ist.

Aufgabe 6: Welche der folgenden Mengen sind algebraische Teilmengen des $\mathbb{A}^1$ (über $\mathbb{C}$)? (Begründung!)

(1) $\{1, 2, 3\}$.
(2) $\{i, -i\}$.
(3) $\{-\pi\}$.
(4) $\mathbb{Z}$.
(5) $\mathbb{R}$.

(6) $\mathbb{A}^1 \setminus \{0\}$.

Aufgabe 7: Zeige, dass die (über einem Körper K definierten) Kurven $y = x^2$ und $xy = 1$ nicht affin äquivalent sind.

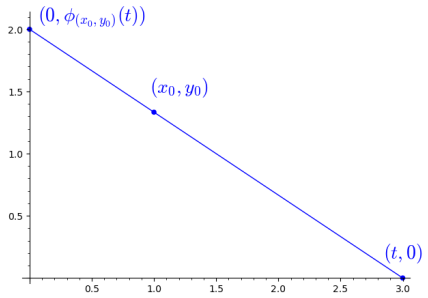
Aufgabe 8: Zeige:

(1) $S = \{(t, t^2, t^3) : t \in \mathbb{R}\}$ ist die Menge der $\mathbb{R}$-rationalen Punkte einer über $\mathbb{R}$ definierten algebraischen Menge in $\mathbb{A}^3$.
(2) $T = \{(t, \sin(t)) : t \in \mathbb{R}\}$ ist nicht die Menge der $\mathbb{R}$-rationalen Punkte einer über $\mathbb{R}$ definierten algebraischen Menge in $\mathbb{A}^2$.

Aufgabe 9: Durch die folgenden Gleichungen werden ebene Kurven über $\mathbb{R}$ definiert, die in $(0, 0)$ eine Singularität haben. Bestimme die Tangenten in $(0, 0)$ und skizziere die Kurven.

(1) $y^2 = x^4 + y^4$,
(2) $y^2 - x^2 = (x^2 + y^2)^2$,
(3) $y^2 - x^3 = (x^2 + y^2)^2$,
(4) $y^3 - 3x^2y = (x^2 + y^2)^2$,
(5) $4x^2y^2 = (x^2 + y^2)^3$.

Aufgabe 10: Sei K ein Körper. Zu $x_0, y_0 \in K \setminus \{0\}$ werde eine Abbildung $\phi_{(x_0,y_0)} : K \to K$ wie folgt definiert: Für $t \neq x_0$ sei $(0, \phi_{(x_0,y_0)}(t))$ der Schnittpunkt der Geraden durch $(t, 0)$ und (x_0, y_0) mit der Geraden $x = 0$. Für $t = x_0$ sei $\phi_{(x_0,y_0)}(x_0) = y_0$.



(1) Beschreibe $\phi_{(x_0,y_0)}(t)$ für $t \neq x_0$ durch eine Formel.
(2) Zeige, dass $\phi_{(x_0,y_0)} : K \to K$ bijektiv ist mit der Umkehrabbildung $\phi^{-1}_{(x_0,y_0)} = \phi_{(y_0,x_0)}$.
(3) Zeige, dass gilt $\phi_{(x_0,y_0)}(K^*) = K^*$.

Aufgabe 11: $y = x^2$ definiert eine ebene affine Kurve C über $\mathbb{R}$, $y = t(x + 1) - 1$ für $t \in \mathbb{R}$ eine Gerade G_t über $\mathbb{R}$.

(1) Bestimme die Schnittpunkte von C und G_t.
(2) Berechne die zugehörigen Schnittmultiplizitäten.
(3) Wann sind die Schnittpunkte reell?

Aufgabe 12: Durch $f(x,y) = xy + 1$ wird eine ebene affine Kurve C über $\mathbb{F}_2$ definiert.

(1) Zeige, dass C nichtsingulär ist.
(2) Bestimme für jeden Punkt $P = (x_0, y_0) \in C(\overline{\mathbb{F}}_2)$ die Tangente T_P an C in P.
(3) Zeige, dass alle Tangenten T_P durch einen Punkt gehen. Bestimme diesen. (Kurven mit dieser Eigenschaft werden *strange curves* - *seltsame Kurven* genannt.)

Aufgabe 13: Sei C die über $\mathbb{F}_3$ durch das Polynom $f = 1 + x^4 + y^4$ definierte ebene affine Kurve.

(1) Zeige, dass C nichtsingulär ist.
(2) Zeige, dass sich die Tangente T_P an C in einem Punkt $P = (x_0, y_0) \in C(\overline{\mathbb{F}}_3)$ durch
$$x = x_0 + y_0^3 t, \quad y = y_0 - x_0^3 t$$
parametrisieren lässt.
(3) Zeige, dass jeder Punkt $P \in C(\overline{\mathbb{F}}_3)$ ein Wendepunkt ist, d.h. es gilt $(C \cdot T_P)_P \geq 3$ für alle $P \in C(\overline{\mathbb{F}}_3)$.

Bei den folgenden Teilaufgaben sind Algebra-Kenntnisse sinnvoll. Sei $i \in \overline{\mathbb{F}}_3$ mit $i^2 = -1$.

(4) Zeige, dass $x^4 + 1$ über $\overline{\mathbb{F}}_3$ die vier Nullstellen $\pm 1 \pm i$ besitzt, und schreibe $x^4 + 1$ als Produkt von Linearfaktoren.
(5) Zeige, dass C absolut irreduzibel ist. (Hinweis: Betrachtet man f als Polynom in y mit Koeffizienten im Ring $\overline{\mathbb{F}}_3[x]$, so kann man das Eisenstein-Kriterium anwenden.)
(6) Bestimme alle Punkte $P \in C(\overline{\mathbb{F}}_3)$ mit $(C \cdot T_P)_P \geq 4$.

Aufgabe 14: Wir betrachten die projektive Ebene $\mathbb{P}^2$ über dem Körper $\mathbb{F}_2 = \{0, 1\}$.

(1) Gib alle $\mathbb{F}_2$-rationalen Punkte von $\mathbb{P}^2$ an. Wieviele gibt es?
(2) Gib alle über $\mathbb{F}_2$ definierten Geraden in $\mathbb{P}^2$ an. Wieviele gibt es?
(3) Stelle eine Inzidenzmatrix auf, wobei die Zeilen der Matrix mit den über $\mathbb{F}_2$ definierten Punkten von $\mathbb{P}^2$, die Spalten mit den über $\mathbb{F}_2$ definierten Geraden von $\mathbb{P}^2$ beschriftet werden, und trage 1 bzw. 0 ein, je nachdem, ob ein Punkt auf einer Geraden liegt oder nicht.
(4) Wieviele $\mathbb{F}_2$-rationale Punkte liegen auf einer über $\mathbb{F}_2$ definierten Geraden?
(5) Wieviele über $\mathbb{F}_2$ definierte Geraden gehen durch einen $\mathbb{F}_2$-rationalen Punkt?
(6) Versuche, die Konfiguration der $\mathbb{F}_2$-rationalen Punkte und der über $\mathbb{F}_2$ definierten Geraden von $\mathbb{P}^2$ zu skizzieren.

Aufgabe 15:

(1) Zeige: Sind P_1, P_2, P_3 Punkte in $\mathbb{P}^2$, die nicht auf einer Geraden liegen, so gibt es homogene Polynome $f, g \in K[x_0, x_1, x_2]$ vom Grad 2 mit
$$\{P_1, P_2, P_3\} = \{f = g = 0\}.$$
(2) Bestimme homogene Polynome $f, g \in K[x_0, x_1, x_2]$ vom Grad 2, sodass gilt
$$\{(1:0:0), (0:1:0), (0:0:1)\} = \{f = g = 0\}.$$
(3) Zeige: Sind P_1, P_2, P_3, P_4 Punkte in $\mathbb{P}^2$, von denen keine drei auf einer Geraden liegen, so gibt es homogene Polynome $f, g \in K[x_0, x_1, x_2]$ vom Grad 2 mit
$$\{P_1, P_2, P_3, P_4\} = \{f = g = 0\}.$$
(4) Bestimme homogene Polynome $f, g \in K[x_0, x_1, x_2]$ vom Grad 2, sodass gilt
$$\{(1:0:0), (0:1:0), (0:0:1), (1:1:1)\} = \{f = g = 0\}.$$

(Hinweis: Man kann f und g als Produkt von Linearformen wählen.)

Aufgabe 16: Laura und Lea haben zum Austausch von Nachrichten folgendes Verschlüsselungsverfahren vereinbart:
Laura und Lea haben sich auf eine natürliche Zahl s mit $2k$ Dezimalstellen geeinigt. (s hat die Funktion eines geheimen Schlüssels.)
Die Texte, die übermittelt werden, bestehen nur aus Großbuchstaben und Leerzeichen. Jeder Text wird in Blöcke mit jeweils k Buchstaben oder Leerzeichen unterteilt, wobei am Ende des Texts gegebenenfalls Leerzeichen angehängt werden, damit jeder Block genau k Zeichen enthält. In jedem Block wird jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt, sodass ein Block zu einer höchstens $2k$-stelligen Dezimalzahl a_i wird. Dann wird $b_i = a_i + s$ berechnet. Die Zahlenfolge b_i ist der Geheimtext und kann verschickt werden.
Laura schickt an Lea folgende Zahlenfolge:

```
4030937786, 3241866671, 4031008571, 3650817792, 5149817880, 5229947489, 3230946594,
4732897085, 3743857071, 3738957071, 3830898389, 3334018092, 5030078671, 4530847376,
4630047476, 3238847371, 4044868391, 3730008083, 4429868471, 3743857780, 3537817872,
4430046676, 5042868371, 5534996976, 4629888392, 5148817772, 5347826571.
```

Was will Laura ihrer Freundin Lea mitteilen? (Hinweis: Nachrichten beginnen oft mit einer Grußformel.)

Aufgabe 17: Durch $f = (x + 2y - 1)(x + 2y)(x + 2y + 2)$ wird eine ebene affine Kurve C (über $\mathbb{R}$) definiert.

(1) Bestimme den projektiven Abschluss $\overline{C}$ von C.
(2) Welche Punkte hat C im Unendlichen?
(3) Skizziere die Kurve in den affinen Teilen U_0 (mit den affinen Koordinaten x, y), U_1 (mit den affinen Koordinaten u, v) und U_2 (mit den affinen Koordinaten r, s).

Aufgabe 18: Durch $(x - a)^2 + (y - b)^2 = r^2$ wird für $a, b \in \mathbb{R}$ und $r \in \mathbb{R}_{>0}$ ein Kreis in der Ebene definiert, den man als über $\mathbb{R}$ definierte affine algebraische Kurve $K_{a,b,r}$ betrachten kann. Zeige:

(1) Der projektive Abschluss von $K_{a,b,r}$ geht durch die Punkte $(0 : 1 : i)$ und $(0 : 1 : -i)$.
(2) Hat die durch $f = a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2 \in \mathbb{R}[x, y] \setminus \mathbb{R}$ definierte ebene algebraische Kurve C mindestens zwei $\mathbb{R}$-rationale Punkte und geht der projektive Abschluss durch die Punkte $(0 : 1 : i)$ und $(0 : 1 : -i)$, so ist C ein Kreis.

Aufgabe 19: Sei C die durch die affine Gleichung $y^2 + y = x^3$ definierte projektive ebene Kurve über dem Körper $\mathbb{F}_2$.

(1) Bestimme ein C beschreibendes homogenes Polynom $f(x_0, x_1, x_2) \in \mathbb{F}_2[x_0, x_1, x_2]$.
(2) Zeige, dass C nichtsingulär ist.
(3) Bestimme $C(\mathbb{F}_2)$, die Menge der $\mathbb{F}_2$-rationalen Punkte von C.
(4) Bestimme für jeden Punkt $P \in C(\mathbb{F}_2)$ die Tangente T_P an C in P.
(5) Zeige, dass alle Punkte aus $C(\mathbb{F}_2)$ Wendepunkte sind.
(6) Bestimme alle Verbindungsgeraden zwischen den Punkten aus $C(\mathbb{F}_2)$.

Aufgabe 20: Durch $x_0^2x_1 - x_1^3 + x_2^3 = 0$ wird eine ebene projektive Kubik C über $\mathbb{R}$ definiert.

(1) Zeige, dass C nichtsingulär ist.
(2) Bestimme die Hessesche Kurve H_C zu C.
(3) Bestimme $H_C(\mathbb{R})$, die Menge der $\mathbb{R}$-rationalen Punkte von H_C.
(4) Bestimme alle reellen Wendepunkte von C.
(5) Skizziere $C(\mathbb{R})$ (und die reellen Wendepunkte) in den affinen Teilen U_0, U_1, U_2.

Aufgabe 21: Durch folgende Polynome aus $\mathbb{F}_3[x_0, x_1, x_2]$

$$\begin{aligned} f_1 &= x_0x_1 - x_0x_2 + x_1^2 - x_2^2, \\ f_2 &= x_0^2 + x_1^2 + x_2^2, \\ f_3 &= x_0^2 - x_0x_1 - x_0x_2 - x_1^2 - x_2^2, \\ f_4 &= x_0^2 + x_0x_1 - x_0x_2 + x_1^2 + x_1x_2 + x_2^2 \end{aligned}$$

werden ebene projektive Quadriken C_i, $i = 1, 2, 3, 4$, über $\mathbb{F}_3$ definiert. Löse für jedes Polynom f_i bzw. für jede Kurve C_i folgende Aufgaben:

(a) Bestimme die Hesse-Matrix $A_{f_i} = \left(\frac{\partial^2 f_i}{\partial x_j \partial x_k}\right)$.
(b) Ist C_i singulär? Wenn ja, bestimme alle Singularitäten von C_i.
(c) Ist f_i reduzibel über $\mathbb{F}_3$ oder über $\overline{\mathbb{F}}_3$? Wenn ja, zerlege f_i in Linearfaktoren.
(d) Bestimme die Menge $C_i(\mathbb{F}_3)$ der $\mathbb{F}_3$-rationalen Punkte von C_i.
(e) Bestimme eine Parametrisierung von C_i über $\mathbb{F}_3$, falls C_i nichtsingulär ist und einen $\mathbb{F}_3$-rationalen Punkt besitzt, d.h. bestimme homogene Polynome gleichen Grades $c_{i,0}(u,v), c_{i,1}(u,v), c_{i,2}(u,v) \in \mathbb{F}_3[u,v]$ mit

$$C_i(\overline{\mathbb{F}}_3) = \{(c_{i,0}(u,v) : c_{i,1}(u,v) : c_{i,2}(u,v)) : (u : v) \in \mathbb{P}^1(\overline{\mathbb{F}}_3)\}.$$

Aufgabe 22: Durch $f = x_0^2 + 2x_0x_1 + 3x_0x_2 - 3x_1^2 - 2x_1x_2 - x_2^2$ wird eine nichtsinguläre projektive ebene Quadrik C über $\mathbb{R}$ definiert.

(1) Bestimme die Tangenten an C, die durch den Punkt $P = (4 : -7 : 16)$ gehen.
(2) Skizziere die Kurve und die Tangenten in den affinen Teilen U_0, U_1, U_2.

Aufgabe 23: Durch $f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ werde eine nichtsinguläre ebene projektive Quadrik über einem algebraisch abgeschlossenen Körper der Charakteristik 2 definiert, d.h. in K gilt $1 + 1 = 0$. Für $(p_0, p_1, p_2) \in K^3 \setminus \{(0,0,0)\}$ sei

$$g_{(p_0,p_1,p_2)} = p_0\frac{\partial f}{\partial x_0} + p_1\frac{\partial f}{\partial x_1} + p_2\frac{\partial f}{\partial x_2} \in K[x_0, x_1, x_2].$$

Zeige:

(1) Es gibt genau einen Punkt $S = (s_0 : s_1 : s_2) \in \mathbb{P}^2$, sodass $g_{(s_0,s_1,s_2)}$ identisch verschwindet.
(2) Alle Tangenten an C gehen durch den Punkt S.

Aufgabe 24: Sei C eine über einem Körper K definierte ebene projektive Quadrik mit genau einem K-rationalen Punkt P, d.h. $C(K) = \{P\}$.

(1) Zeige, dass P ein singulärer Punkt von C ist.
(2) Zeige: Ist (nach eventuellem Koordinatenwechsel über K) o.E. $P = (1 : 0 : 0)$, so wird C durch ein Polynom

$$f = (x_2 - \alpha x_1)(x_2 - \beta x_1) \quad \text{mit} \quad \alpha, \beta \in \overline{K} \setminus K, \quad \alpha + \beta \in K, \quad \alpha\beta \in K$$

beschrieben.

(3) Gib Beispiele einer solchen Quadrik für die Körper $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{Q}$ und $\mathbb{R}$ an.

Aufgabe 25: Durch

$$f = x_0^2 - 2x_0x_1 + 3x_0x_2 - 4x_1^2 + 5x_1x_2 - 6x_2^2$$

wird eine nichtsinguläre projektive ebene Quadrik C über $\mathbb{Q}$ definiert, die den Punkt $(3 : -2 : -1)$ enthält.

(1) Bestimme eine über $\mathbb{Q}$ definierte Parametrisierung von C, d.h. homogene Polynome gleichen Grades $c_0(u,v), c_1(u,v), c_2(u,v) \in \mathbb{Q}[u,v]$ mit

$$C(\mathbb{Q}) = \{c_0(u,v) : c_1(u,v) : c_2(u,v)) : (u : v) \in \mathbb{P}^1(\mathbb{Q})\}.$$

(2) Bestimme mindestens 10 Punkte aus $C(\mathbb{Q})$.

Aufgabe 26: Durch die Polynome

$$f_1 = x_0^2 + 2x_1^2 + 3x_2^2, \quad f_2 = x_0x_1, \quad f_3 = x_1^2 + x_2^2, \quad f_4 = x_2^2$$

werden projektive ebene Kurven C_1, C_2, C_3, C_4 über $\mathbb{F}_{127}$ definiert. Bestimme

$$\#C_i(\mathbb{F}_{127}) \text{ für } i = 1, 2, 3, 4.$$

Aufgabe 27: Bestimme für folgende über $\mathbb{Q}$-definierte Quadriken eine Legendre-Normalform und eine zugehörige Transformationsmatrix:

(1) $f = 18x_0^2 - 20x_1^2 + 21x_2^2$.
(2) $f = 2x_0x_1 + 3x_0x_2 + 5x_1x_2$.
(3) $f = 15x_0^2 - 21x_1^2 + 35x_2^2$.
(4) $f = x_0^2 - 2x_0x_1 + x_0x_2 - 2x_1^2 + x_1x_2 - 2x_2^2$.

Aufgabe 28: (Bei dieser Aufgabe sind Kenntnisse des Legendre-Symbols sinnvoll.) Durch folgende Polynome werden über $\mathbb{Q}$ projektive ebene Quadriken in Legendre-Normalform definiert. Untersuche, ob sie einen $\mathbb{Q}$-rationalen Punkt besitzen.

(1) $f = 2x_0^2 + 3x_1^2 + 5x_2^2$.
(2) $f = 3x_0^2 + 5x_1^2 - 7x_2^2$.
(3) $f = 5x_0^2 + 7x_1^2 - 13x_2^2$.
(4) $f = 33x_0^2 + 34x_1^2 - 35x_2^2$.
(5) $f = 22x_0^2 + 23x_1^2 - 15x_2^2$.

Aufgabe 29: Durch

$$f_{(u,v)} = u(3x_0 + 4x_1 + x_2)(4x_0 - x_2) + v(x_0x_2 - x_1^2)$$

wird ein Büschel ebener projektiver Quadriken über $\mathbb{R}$ definiert.

(1) Bestimme die Basispunkte des Büschels, d.h. die Punkte in $\mathbb{P}^2$, durch die alle Kurven des Büschels gehen.
(2) Bestimme die Parameter $(u : v) \in \mathbb{P}^1$, für die die Kurve $f_{(u,v)} = 0$ singulär ist. Skizziere die zugehörigen Kurven.

Aufgabe 30: (Bei dieser Aufgabe werden Kenntnisse über endliche Körper vorausgesetzt.) Sei p eine Primzahl und $\alpha \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$. In $\mathbb{P}^2$ über $\mathbb{F}_p$ betrachten wir die Punkte

$$P_0 = (1 : \alpha : \alpha^2), \quad P_1 = (1 : \alpha^p : \alpha^{2p}), \quad P_2 = (1 : \alpha^{p^2} : \alpha^{2p^2})$$

und in $\mathbb{F}_{p^3}[x_0, x_1, x_2]$ die Linearformen

$$g_{01} = \det \begin{pmatrix} x_0 & x_1 & x_2 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^p & \alpha^{2p} \end{pmatrix}, \quad g_{12} = \det \begin{pmatrix} x_0 & x_1 & x_2 \\ 1 & \alpha^p & \alpha^{2p} \\ 1 & \alpha^{p^2} & \alpha^{2p^2} \end{pmatrix}, \quad g_{20} = \det \begin{pmatrix} x_0 & x_1 & x_2 \\ 1 & \alpha^{p^2} & \alpha^{2p^2} \\ 1 & \alpha & \alpha^2 \end{pmatrix}.$$

(1) Zeige, dass P_0, P_1, P_2 nicht auf einer Geraden liegen.
(2) Zeige, dass die Geraden $\{g_{01} = 0\}$, $\{g_{12} = 0\}$ und $\{g_{20} = 0\}$ nicht durch einen Punkt gehen.
(3) Zeige, dass $f = g_{01} g_{12} g_{20} \in \mathbb{F}_p[x_0, x_1, x_2]$ gilt, d.h. f hat Koeffizienten in $\mathbb{F}_p$.
(4) Zeige, dass die durch $f = 0$ über $\mathbb{F}_p$ definierte ebene projektive Kubik C keine $\mathbb{F}_p$-rationalen Punkte besitzt, d.h. $C(\mathbb{F}_p) = \emptyset$.
(5) Bestimme das Polynom $f \in \mathbb{F}_2[x_0, x_1, x_2]$ für $\alpha \in \mathbb{F}_{2^3}$ mit $\alpha^3 + \alpha + 1 = 0$.

Aufgabe 31: Bestimme für folgende Büschel ebener Quadriken die Basispunkte, die singulären Kurven der Büschel, und skizziere die zu $(u : v) = (1 : 0), (0 : 1), (1 : 1), (1 : -1)$ gehörigen Kurven.

(1) $f_{(u,v)} = u(x_0^2 - x_1^2 - x_2^2) + v(x_0 x_1 + x_1^2)$.
(2) $f_{(u,v)} = u(x_0^2 - x_1^2 - x_2^2) + v(x_0^2 - x_1^2)$.
(3) $f_{(u,v)} = u(x_0^2 - x_1^2 - x_2^2) + v(x_0^2 + 2x_0 x_1 + x_1^2)$.

(Die Anzahl der Basispunkte ist $1, 2, 3$.)

Aufgabe 32: (Der Grundkörper sei algebraisch abgeschlossen mit Charakteristik $\neq 2$.) Ein Büschel $f_{(u,v)} = 0$ ebener projektiver Quadriken enthalte (mindestens) zwei Doppelgeraden.

(1) Zeige, dass es genau einen Basispunkt gibt. Wie kann man diesen Punkt beschreiben?
(2) Zeige, dass alle Kurven des Büschels singulär sind.
(3) Wieviele Doppelgeraden enthält das Büschel?

Aufgabe 33: Durch

$$f_{(u,v)} = u x_0 x_2 + v x_1 x_2 \quad \text{und} \quad g_{(u,v)} = u x_1^2 + v x_2^2$$

werden zwei Büschel ebener projektiver Quadriken definiert.

(1) Bestimme die Basispunkte jedes Büschels.
(2) Zeige, dass jede Kurve der beiden Büschel singulär ist.
(3) Zerlege $f_{(u,v)}$ und $g_{(u,v)}$ für alle $(u : v) \in \mathbb{P}^1$ in Linearfaktoren.

(Die beiden Büschel zeigen zwei Weisen, wie es passieren kann, dass jede Kurve eines Büschels singulär ist.)

Aufgabe 34: Gegeben sei

$$f = \frac{4x_0^4 - 4x_0^3 x_1 - 3x_0^2 x_1^2 + 4x_0 x_1^3 - x_1^4}{8x_0^4 + 8x_0^3 x_1 - 2x_0^2 x_1^2 - 4x_0 x_1^3 - x_1^4} \in \mathbb{C}(\mathbb{P}^1).$$

(1) Schreibe f als rationale Funktion in $x = \frac{x_1}{x_0}$.
(2) Schreibe f als rationale Funktion in $u = \frac{x_0}{x_1}$.

(3) Untersuche, ob f in den folgenden Punkten P definiert ist, und bestimme gegebenenfalls den Wert $f(P)$:
$$0, \quad 1, \quad -1, \quad 2, \quad -2, \quad \infty.$$
(4) Bestimme die Null- und Polstellen von f und die zugehörigen Vielfachheiten.

Aufgabe 35: Gegeben sei
$$f = \frac{2x^2 - 4x + 3}{x^2 - 1} \in \mathbb{C}(\mathbb{P}^1).$$
Da Zähler und Nenner (teilerfremde) Polynome vom Grad 2 sind, gibt es - nach Vorlesung - zu jedem $\lambda \in \mathbb{C}$ zwei (nicht notwendigerweise verschiedene) Punkte $P_\lambda, Q_\lambda \in \mathbb{P}^1$ mit
$$f(P_\lambda) = f(Q_\lambda) = \lambda, \quad \text{d.h.} \quad f^{-1}(\lambda) = \{P_\lambda, Q_\lambda\}.$$
Bestimme alle $\lambda \in \mathbb{C}$, für die die Punkte P_λ und Q_λ zusammenfallen, d.h. für die gilt
$$\# f^{-1}(\lambda) = 1.$$

Aufgabe 36: Sei $f \in \mathbb{C}(\mathbb{P}^1)^*$. Mit f' wird wie üblich die Ableitung von f bezüglich x bezeichnet.
(1) Zeige: Ist f in $P \in \mathbb{P}^1$ definiert, so auch f'.
(2) Zeige: Ist $\alpha \in \mathbb{C}$ mit $\operatorname{ord}_\alpha(f) \neq 0$, so gilt
$$\operatorname{ord}_\alpha(f') = \operatorname{ord}_\alpha(f) - 1.$$
(3) Sei f in α definiert und $f(\alpha) = \lambda$. Zeige die Äquivalenz:
$$\operatorname{ord}_\alpha(f - \lambda) \geq 2 \quad \Longleftrightarrow \quad f'(\alpha) = 0.$$
(4) Zeige: Ist $\operatorname{ord}_\infty(f) \neq 0$, so gilt
$$\operatorname{ord}_\infty(f') = \operatorname{ord}_\infty(f) + 1.$$

Aufgabe 37: Bestimme $\operatorname{div}(f_k)$ für folgende Funktionen $f_k \in \mathbb{C}(\mathbb{P}^1)$:
$$f_1 = x^2 + 1, \quad f_2 = \frac{x}{x^2 - 1}, \quad f_3 = \frac{x^2 - 1}{x}, \quad f_4 = \frac{x^2 - 2}{x^4 - 4}$$

Aufgabe 38:
(1) Welcher der folgenden Divisoren $D_k \in \operatorname{Div}(\mathbb{P}^1)$ ist ein Hauptdivisor? Bestimme gegebenenfalls eine Funktion $f_k \in \mathbb{C}(\mathbb{P}^1) \setminus \{0\}$ mit $D_k = \operatorname{div}(f_k)$.
$$D_1 = [1] + [2], \quad D_2 = 3[4] - 3[\infty], \quad D_3 = [1] + [2] - [3] - [4], \quad D_4 = 3[1] - 2[2] - [\infty].$$
(2) Zeige, dass es genau ein $n \in \mathbb{Z}$ gibt, sodass
$$D = n[1] + 7[2] - 3n[3] + 3[\infty]$$
ein Hauptdivisor ist. Bestimme n und $f \in \mathbb{C}(\mathbb{P}^1)^*$ mit $D = \operatorname{div}(f)$.

Aufgabe 39: Bestimme für folgende Divisoren $D_k \in \operatorname{Div}(\mathbb{P}^1)$ den Vektorraum $\mathcal{L}(D_k)$ durch Angabe einer Basis:

$D_1 = [1]+[2], \quad D_2 = [1]-[2]+[3], \quad D_3 = [1]-[2]-[3], \quad D_4 = [1]+2[2]+3[\infty], \quad D_5 = [1]+2[2]-3[\infty].$

Aufgabe 40: Seien $P_1, \dots, P_6 \in \mathbb{P}^1$ paarweise verschiedene Punkte, $D = m_1[Q_1]+\cdots+m_r[Q_r] \in \mathrm{Div}(\mathbb{P}^1)$ mit $\mathrm{grad}(D) = 3$ und $\{P_1, \dots, P_6\} \cap \{Q_1, \dots, Q_r\} = \emptyset$ und

$$\alpha : \mathcal{L}(D) \to K^6 \text{ mit } \alpha(f) = (f(P_1), \dots, f(P_6)).$$

(1) Zeige, dass α eine wohldefinierte K-lineare Abbildung ist. (Warum ist jedes $f \in \mathcal{L}(D)$ in den Punkten $P_1, \dots, P_6$ definiert?)

(2) Zeige: Sind $i_1, i_2, i_3, i_4 \in \{1, \dots, 6\}$ mit $\#\{i_1, i_2, i_3, i_4\} = 4$, so gilt für $f \in \mathcal{L}(D)$ die Implikation

$$f(P_{i_1}) = f(P_{i_2}) = f(P_{i_3}) = f(P_{i_4}) = 0 \quad \Longrightarrow \quad f = 0.$$

(3) Zeige: Sind $i_1, i_2, i_3 \in \{1, \dots, 6\}$ mit $\#\{i_1, i_2, i_3\} = 3$, so gibt es eine Funktion $f \in \mathcal{L}(D)$ mit

$$f(P_{i_1}) = f(P_{i_2}) = f(P_{i_3}) = 0, \quad \text{aber} \quad f \neq 0.$$

Für diese Funktion f gilt:

$$d_{\mathrm{Hamming}}(\alpha(f), 0) = 3.$$

(4) Sei $C = \mathrm{Bild}(\alpha)$. Bestimme

$$\dim(C) \quad \text{und} \quad d(C) = \min\{d_{\mathrm{Hamming}}(v, 0) : v \in C \setminus \{0\}\}.$$

(C ist ein $[6, \dim(V), d(C)]$-Code über K.)

Aufgabe 41: Sei K ein Körper der Charakteristik 2, $t \in K$ und C die durch $y^2 = x^3 + t$ definierte ebene affine Kurve. Zeige:

(1) C ist absolut irreduzibel.
(2) C besitzt genau eine Singularität $S \in C(\overline{K})$.
(3) Ist K vollkommen, so gilt $S \in C(K)$.
(4) Ist $K = \mathbb{F}_2(t) = \{\frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{F}_2[t], g(t) \neq 0\}$ der rationale Funktionenkörper in t über $\mathbb{F}_2$, so gilt $S \notin C(K)$. (Die Singularität ist also über dem Grundkörper nicht „sichtbar“.)

Aufgabe 42: Im $\mathbb{P}^5$ der ebenen Quadriken (über $\mathbb{C}$) betrachte man

$$X = \{Q \text{ ebene Quadrik} : (1:0:0) \in Q, (0:1:0) \in Q, Q \text{ reduzibel}\}.$$

(1) Beschreibe X durch Gleichungen (in den Variablen $a_0, a_1, a_2, a_3, a_4, a_5$).
(2) Zerlege X in irreduzible Komponenten.
(3) Wie sehen die zu den Komponenten von X gehörigen Quadriken aus?

Aufgabe 43: Im Polynomring $K[x, y]$ sei $\mathfrak{a}$ das von den Polynomen

$$f_n = x^n - y^{n+1} \text{ für } n \in \mathbb{N}$$

erzeugte Ideal, d.h. $\mathfrak{a} = (\{f_n : n \in \mathbb{N}\})$. Da $K[x, y]$ ein noetherscher Ring ist, besitzt $\mathfrak{a}$ ein endliches Erzeugendensystem. Bestimme ein solches.

Aufgabe 44: Durch $x_0x_2^2 = x_1^3 - x_0^3$ wird eine irreduzible nichtsinguläre projektive ebene Kurve C über $\mathbb{C}$ definiert. Durch

$$(x_0 : x_1 : x_2) \mapsto ((x_0 : x_1), (x_0 : x_2))$$

erhält man eine rationale Abbildung $\phi : C \to \mathbb{P}^1 \times \mathbb{P}^1$.

(1) Die angegebene Darstellung für ϕ ist im Punkt $(0 : 0 : 1)$ nicht definiert. Zeige durch eine geeignete explizite Beschreibung, dass ϕ auch in $(0 : 0 : 1)$ definiert ist. (Also ist ϕ sogar ein Morphismus.)

(2) Zeige, dass ϕ injektiv ist.
(3) Da ϕ ein Morphismus und C projektiv ist, ist $\phi(C)$ eine abgeschlossene Teilmenge von $\mathbb{P}^1 \times \mathbb{P}^1$. Beschreibe $\phi(C)$ durch Gleichungen. (Hinweis: $\phi(C)$ genügt einer Gleichung vom Bigrad $(3,2)$.)
(4) Zeige, dass $\phi(C)$ singulär ist. (Also ist ϕ kein Isomorphismus.)

Aufgabe 45:

(1) Durch
$$\alpha(x,y) = (x + x^2 - 2xy + y^2, y + x^2 - 2xy + y^2)$$
wird ein Morphismus $\alpha : \mathbb{A}^2 \to \mathbb{A}^2$ definiert. Zeige, dass α ein Automorphismus ist (durch Bestimmung von α^{-1}).
(2) Für $f \in K[x]$ wird durch
$$\beta_f(x,y) = (x, y + f(x))$$
ein Morphismus $\beta_f : \mathbb{A}^2 \to \mathbb{A}^2$ definiert.
(a) Zeige, dass für $f, g \in K[x]$ gilt
$$\beta_{f+g} = \beta_f \circ \beta_g.$$
(b) Zeige, dass β_f ein Automorphismus ist.

(Die obigen Beispiele zeigen, dass es Automorphismen von $\mathbb{A}^2$ gibt, die keine Koordinatenwechsel sind.)

Aufgabe 46: K sei ein algebraisch abgeschlossener Körper, versehen mit der Zariski-Topologie. Durch
$$f_1(t) = \begin{cases} \frac{1}{t} & \text{für } t \neq 0 \\ 0 & \text{für } t = 0 \end{cases}, \quad f_2(t) = \begin{cases} 1 & \text{für } t \neq 0 \\ 0 & \text{für } t = 0 \end{cases}, \quad f_3(t) = \begin{cases} t & \text{für } t \neq 0 \\ 1 & \text{für } t = 0, \end{cases}, \quad f_4(t) = \begin{cases} -t & \text{für } t \neq 0 \\ 1 & \text{für } t = 0 \end{cases}$$
werden Funktionen $K \to K$ definiert.

(1) Welche der Funktionen f_1, f_2, f_3, f_4 ist stetig?
(2) Gib stetige Funktionen $g, h : K \to K$ an, sodass die Funktion $g + h : K \to K$, $t \mapsto f(t) + g(t)$, nicht stetig ist.
(3) Gib stetige Funktionen $g, h : K \to K$ an, sodass die Funktion $g \cdot h : K \to K$, $t \mapsto g(t)h(t)$, nicht stetig ist.

Aufgabe 47: Sei K ein algebraisch abgeschlossener Körper der Charakteristik $\neq 2$. Durch $x_1^2 + x_2^2 = x_0^2$ wird eine nichtsinguläre projektive ebene Quadrik C über K definiert.

(1) Zeige, dass gilt
$$(x_0 + x_1 : x_2) = (x_2 : x_0 - x_1) \text{ für alle } (x_0 : x_1 : x_2) \in C \setminus \{(1:1:0), (1:-1:0)\}.$$
Daher wird durch
$$\phi : C \to \mathbb{P}^1, \quad (x_0 : x_1 : x_2) \mapsto \begin{cases} (x_0 + x_1 : x_2) & \text{für } (x_0 : x_1 : x_2) \neq (1:-1:0), \\ (x_2 : x_0 - x_1) & \text{für } (x_0 : x_1 : x_2) \neq (1:1:0) \end{cases}$$
ein Morphismus definiert.

(2) Zeige, dass es keine homogenen Polynome gleichen Grades $f, g \in K[x_0, x_1, x_2]$ gibt, sodass für alle $(x_0 : x_1 : x_2) \in C$ gilt
$$\phi((x_0 : x_1 : x_2)) = (f(x_0, x_1, x_2) : g(x_0, x_1, x_2)).$$
(Die obige Fallunterscheidung in der Definition von ϕ läßt sich also nicht umgehen.)

Aufgabe 48: Eine Ordnungsfunktion (oder diskrete Bewertung) v eines Körpers K ist eine surjektive Abbildung $v : K^* \to \mathbb{Z}$, sodass gilt

- $v(ab) = v(a) + v(b)$ für alle $a, b \in K^*$,
- $v(a + b) \geq \min(v(a), v(b))$ für alle $a, b \in K^*$ mit $a + b \neq 0$.

Dann gilt auch die Implikation

$$a, b \in K^* \text{ mit } v(a) \neq v(b) \quad \Longrightarrow \quad a + b \neq 0 \text{ und } v(a + b) = \min(v(a), v(b)).$$

Sei nun K algebraisch abgeschlossen. Jede Funktion $f \in K(x)^*$ lässt sich dann eindeutig in der Form

$$f = c \cdot \prod_{\alpha \in K} (x - \alpha)^{e(\alpha)}$$

schreiben mit $c \in K^*$, $e(\alpha) \in \mathbb{Z}$ und $\#\{\alpha \in K : e(\alpha) \neq 0\} < \infty$. In der Vorlesung haben wir folgende Ordnungsfunktionen auf $K(x)$ kennengelernt: $\operatorname{ord}_\alpha$ für alle $\alpha \in K$ und $\operatorname{ord}_\infty$ mit

$$\operatorname{ord}_\alpha(f) = e(\alpha) \quad \text{und} \quad \operatorname{ord}_\infty(f) = -\sum_{\alpha \in K} e(\alpha),$$

wobei außerdem noch

$$\operatorname{ord}_\alpha(c) = \operatorname{ord}_\infty(c) = 0 \text{ für alle } c \in K^*$$

gilt.
Zeige: Ist v eine Ordnungsfunktion auf $K(x)$ mit $v(c) = 0$ für alle $c \in K^*$, so ist v eine der obigen Ordnungsfunktionen $\operatorname{ord}_\alpha$ oder $\operatorname{ord}_\infty$.

Aufgabe 49: Sei $\pi : X \to \mathbb{A}^2$ die Aufblasung von $\mathbb{A}^2$ in $O = (0, 0)$, $E = \pi^{-1}(O)$ die exzeptionelle Faser, $f(x, y)$ ein Polynom vom Grad d, C die durch $f(x, y) = 0$ definierte ebene affine Kurve und

$$\lambda(f) = \#\left(E \cap \overline{\pi^{-1}(C \setminus \{O\})}\right),$$

d.h. $\lambda(f)$ gibt an, in wievielen Punkten das eigentliche Urbild von C die exzeptionelle Faser schneidet.
Zeige:

(1) Es gilt: $O \in C \iff \lambda(f) \geq 1$.
(2) Es gilt: $\lambda(f) \leq d$.
(3) Genau dann ist $\lambda(f) = d$, wenn C Vereinigung von d verschiedenen Geraden ist, die durch O gehen.

Aufgabe 50: Sei C der projektive Abschluss der durch $x^2y + xy^2 = x^4 + y^4$ definierten ebenen Kurve (über einem algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2$).

(1) Zeige, dass $P = (1 : 0 : 0)$ der einzige singuläre Punkt von C ist.
(2) Beschreibe eine zu C birational äquivalente nichtsinguläre projektive Kurve $\widetilde{C}$ (durch Aufblasung und affine Überdeckungen) und den zugehörigen Morphismus $\phi : \widetilde{C} \to C$.
(3) Zeige, dass $\phi^{-1}(P)$ aus 3 verschiedenen Punkten P_1, P_2, P_3 besteht.
(4) Bestimme Funktionen $t_i \in K(\widetilde{C})$ (als rationale Funktionen in x und y), sodass für alle $i, j \in \{1, 2, 3\}$ gilt

$$\operatorname{ord}_{P_j}(t_i) = \begin{cases} 1 & \text{im Fall } i = j, \\ 0 & \text{im Fall } i \neq j. \end{cases}$$

Aufgabe 51: Sei C der projektive Abschluss der Kurve $x^2 + y^2 = 1$ über einem algebraisch abgeschlossenen Körper der Charakteristik $\neq 2$. Bestimme den Divisor der Differentialform dx.

Aufgabe 52: Sei C die projektive ebene Kurve, die affin durch $y^3 = x^4 - 1$ gegeben wird (über einem algebraisch abgeschlossenen Körper der Charakteristik 0), und ϕ der durch $\phi = (1 : x)$ definierte Morphismus $\phi : C \to \mathbb{P}^1$.

(1) Zeige, dass C nichtsingulär ist.
(2) Bestimme für jeden Kurvenpunkt eine Uniformisierende.
(3) Bestimme $\operatorname{grad}(\phi)$.
(4) Bestimme alle Verzweigungsindizes $e_\phi(P)$.
(5) Bestimme den Verzweigungsdivisor von ϕ.
(6) Bestimme das Geschlecht von C mit Hilfe der Riemann-Hurwitz-Formel.

Aufgabe 53: Sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Eine Funktion $f \in K(x) \setminus K$ definiert dann einen nichtkonstanten Morphismus $\mathbb{P}^1 \to \mathbb{P}^1$, der hier ebenfalls mit f bezeichnet sei.

(1) Zeige folgendes Kriterium für Verzweigtheit: Ist $\alpha \in K$ mit $f(\alpha) \in K$, so gilt

$$f \text{ verzweigt in } \alpha, \text{ d.h. } e_f(\alpha) \geq 2 \quad \Longleftrightarrow \quad f'(\alpha) = 0.$$

(Das Kriterium sagt nichts aus über das Verzweigungsverhalten in den Punkten der Menge $\{\infty\} \cup f^{-1}(\infty)$.)
(2) Bestimme für die nachfolgenden Funktionen $f \in K(x)$ alle Verzweigungsindizes $e_f(P)$ (für $P \in \mathbb{P}^1$) und zeige, dass alle Verzweigungspunkte in der Menge $f^{-1}(\{0, 1, \infty\})$ enthalten sind.
(a)

$$f = (2x^2 - 1)^2$$

(b)

$$f = \frac{(x+2)^9 x^{18} (x^2-2)^{18} (x-2)}{(x+1)^{16} (x^3 - 3x + 1)^{16}}$$

(Ist C eine irreduzible, nichtsinguläre, projektive Kurve, so heißt ein Morphismus $\phi : C \to \mathbb{P}^1$ eine **Belyi-Abbildung**, wenn alle Verzweigungspunkte in $\phi^{-1}(\{0, 1, \infty\})$ enthalten sind. Obige Abbildungen $\mathbb{P}^1 \to \mathbb{P}^1$ sind also Beispiele von Belyi-Abbildungen.)

Aufgabe 54: Sei C das nichtsinguläre Modell der durch $y^2 = x^p$ definierten Kurve in Charakteristik $p > 2$.

(1) Es ist $dy = 0$. Bestimme ein $z \in K(C)$ mit $y = z^p$.
(2) C ist birational äquivalent zu $\mathbb{P}^1$.

Aufgabe 55: Sei C eine Kurve vom Geschlecht 2. Dann gibt es einen kanonischen Divisor $K_C = [P_1] + [P_2]$ und eine Funktion $f \in K(C)$ mit $\mathcal{L}(K_C) = \overline{K} + \overline{K} f$.

(1) Bestimme $\operatorname{ord}_{P_i}(f)$.
(2) Zeige, dass $\ell(2K_C) = 3$ gilt.
(3) Bestimme eine $\overline{K}$-Basis f_0, f_1, f_2 von $\mathcal{L}(2K_C)$.
(4) Beschreibe das Bild des durch $\phi = (f_0 : f_1 : f_2)$ definierten Morphismus $\phi : C \to \mathbb{P}^2$.

Aufgabe 56: Über $\mathbb{F}_7$ wird durch $f = x_0^3 + 2x_1^3 + 3x_2^3$ eine nichtsinguläre ebene Kubik C definiert, die den Punkt $P = (1 : 1 : 3)$ enthält. C hat Geschlecht 1.

(1) Zeige, dass $\ell(4[P]) = 4$ gilt, und bestimme eine Basis f_0, f_1, f_2, f_3 von $\mathcal{L}(4[P])$ mit $f_0, f_1, f_2, f_3 \in \mathbb{F}_7(C)$.

(2) Zeige, dass der Divisor $4[P]$ sehr ampel ist. Daher definiert die rationale Abbildung $\phi = (f_0 : f_1 : f_2 : f_3)$ eine Einbettung von C in $\mathbb{P}^3$. Zeige, dass $I(\phi(C))$ von zwei quadratischen Polynomen erzeugt wird durch explizite Angabe der Polynome. ($\phi(C)$ ist also durch Durchschnitt zweier Quadriken im $\mathbb{P}^3$.)

(Der Einsatz eines Computeralgebrasystems wie SAGE ist sinnvoll.)

Aufgabe 57: Sei $C \subseteq \mathbb{P}^n$ eine absolut irreduzible, nichtsinguläre, projektive Kurve, die in keiner Hyperebene enthalten ist. Für eine von 0 verschiedene Linearform $h = a_0x_0 + a_1x_1 + \cdots + a_nx_n$ wird der Hyperebenenschnitt $\operatorname{div}(h)$ durch

$$\operatorname{div}(h) = \sum_{P \in C} n_P[P] \quad \text{mit} \quad n_P = \operatorname{ord}_P(\frac{h}{x_k}), \text{ falls } P \in U_k = \{x_k \neq 0\},$$

der Grad der Kurve $\operatorname{grad}(C)$ als $\operatorname{grad}(\operatorname{div}(h))$ definiert. Zeige:

(1) Ist $P \in C \cap U_k \cap U_l$, so gilt $\operatorname{ord}_P(\frac{h}{x_k}) = \operatorname{ord}_P(\frac{h}{x_l})$. (Dies zeigt, dass obige Zahl n_P wohldefiniert ist.)
(2) Alle Hyperebenenschnitte sind linear äquivalent.
(3) Die Funktionen

$$\frac{x_0}{h}, \quad \frac{x_1}{h}, \quad \cdots \quad \frac{x_n}{h}$$

sind linear unabhängige Funktionen aus $\mathcal{L}(\operatorname{div}(h))$. Insbesondere gilt $\ell(\operatorname{div}(h)) \geq n + 1$.
(4) Es gilt $\operatorname{grad}(C) \geq n$.
(5) Ist $\operatorname{grad}(C) = n$, so hat C Geschlecht 0.

Aufgabe 58: Sei $C \subseteq \mathbb{P}^2$ eine nichtsinguläre ebene Quartik über einem algebraisch abgeschlossenen Körper. Nach der Adunktionsformel sind die effektiven kanonischen Divisoren genau die Geradenschnitte, insbesondere gibt es zu zwei Punkten $P_1, P_2 \in C$ genau einen effektiven kanonischen Divisor K_{P_1,P_2} mit $[P_1] + [P_2] \leq K_{P_1,P_2}$, nämlich den Geradenschnitt $\operatorname{div}(g)$, wo $g = 0$ im Fall $P_1 \neq P_2$ die Gerade durch P_1, P_2 beschreibt, im Fall $P_1 = P_2$ die Tangente ist.

(1) Für jeden effektiven Divisor D vom Grad 2 gilt $\ell(D) = 1$.
(2) Sind $P_1, P_2, P_3 \in C$ drei verschiedene Punkte, die nicht auf einer Geraden liegen, so gilt

$$\ell(K_C - [P_1] - [P_2] - [P_3]) = 0 \quad \text{und} \quad \ell([P_1] + [P_2] + [P_3]) = 1.$$

Ist $P_4 \in C$ ein von P_1, P_2, P_3 verschiedener Punkt und

$$D = [P_1] + [P_2] + [P_3] - [P_4],$$

so gilt

$$\operatorname{grad}(D) = 2 \quad \text{und} \quad \ell(D) = 0.$$

(3) $P \in C$ ist genau dann ein Wendepunkt, wenn gilt $\ell(3[P]) = 2$.

Aufgabe 59: Sei C eine absolut irreduzible, nichtsinguläre, projektive Kurve vom Geschlecht 3, sodass $\ell(D) \leq 1$ für jeden Divisor D vom Grad 2 gilt, und K_C ein kanonischer Divisor.

(1) Zeige, K_C sehr ampel ist.
(2) Zeige, dass $\phi_{K_C}(C)$ eine nichtsinguläre ebene Quartik ist.

Aufgabe 60: Durch

$$\begin{aligned} f_1 &= 5x_0^2 - 2x_0x_1 + 3x_0x_2 - 5x_1^2 + 2x_1x_2 + 2x_2^2, \\ f_2 &= 5x_0^2 + 5x_0x_1 - 7x_0x_2 + 10x_1^2 - x_1x_2 - 8x_2^2, \\ f_3 &= 7x_0^2 - 5x_0x_1 - 8x_0x_2 - 10x_1^2 - 9x_1x_2 + 2x_2^2 \end{aligned}$$

werden drei nichtsinguläre, ebene Quadriken C_1, C_2, C_3 über $\mathbb{Q}$ definiert.

(1) Transformiere jede Quadrik C_i in die Form $a_i y_0^2 + b_i y_1^2 = y_2^2$.
(2) Bestimme für jede Quadrik C_i die Menge $\Psi(C_i) = \{p \text{ Primzahl} : C_i(\mathbb{Q}_p) = \emptyset\}$.
(3) Welche der Quadriken sind über $\mathbb{Q}$ isomorph? Bestimme gegebenenfalls einen expliziten Isomorphismus, falls möglich.

Aufgabe 61: Gegeben sei eine Kurve E vom Geschlecht 1 und zwei Punkte $O, \widetilde{O} \in E$. Dann sind

$$\psi : E \to \mathrm{Pic}^0(E) \text{ mit } \psi(P) = \overline{[P] - [O]} \quad \text{und} \quad \widetilde{\psi} : E \to \mathrm{Pic}^0(E) \text{ mit } \widetilde{\psi}(P) = \overline{[P] - [\widetilde{O}]}$$

Bijektionen. Durch

$$P_1 \oplus P_2 = \psi^{-1}(\psi(P_1) + \psi(P_2)) \quad \text{und} \quad P_1 \widetilde{\oplus} P_2 = \widetilde{\psi}^{-1}(\widetilde{\psi}(P_1) + \widetilde{\psi}(P_2))$$

erhält man Verknüpfungen auf E, die E zu einer abelschen Gruppe machen mit O bzw. $\widetilde{O}$ als neutralem Element. Zeige, dass durch

$$\alpha : E \to E \text{ mit } \alpha(P) = P \oplus \widetilde{O}$$

ein Gruppenisomorphismus

$$(E, \oplus, O) \to (E, \widetilde{\oplus}, \widetilde{O})$$

definiert wird.

Aufgabe 62: Sei C eine nichtsinguläre ebene Kubik und seien $P_1, P_2, Q_1, Q_2 \in C$. Zeige, dass genau dann

$$[P_1] + [P_2] \sim [Q_1] + [Q_2]$$

gilt, wenn sich die Gerade durch P_1, P_2 und die Gerade durch Q_1, Q_2 in einem Kurvenpunkt schneiden.

Aufgabe 63: Sei C eine Kurve vom Geschlecht 1. Ist D ein Divisor vom Grad 2, so gibt es wegen $\ell(D) = 2$ Funktionen $f_0, f_1 \in K(C)$ mit

$$\mathcal{L}(D) = K \cdot f_0 + K \cdot f_1.$$

Zugehörig definiert man einen Morphismus

$$\phi_{D,f_0,f_1} : C \to \mathbb{P}^1 \text{ mit } \phi_{D,f_0,f_1} = (f_0 : f_1).$$

Da D Grad 2 hat, ist ϕ_{D,f_0,f_1} ein Morphismus vom Grad 2 und $\phi^*_{D,f_0,f_1}(K(\mathbb{P}^1))$ ein Unterkörper von $K(C)$ vom Index 2. Zeige:

(1) Es gilt

$$\phi^*_{D,f_0,f_1}(K(\mathbb{P}^1)) = K(\frac{f_1}{f_0}).$$

(2) Ist g_0, g_1 eine andere Basis von $\mathcal{L}(D)$, so gilt

$$K(\frac{g_1}{g_0}) = K(\frac{f_1}{f_0}).$$

Daher ist der Unterkörper unabhängig von der gewählten Basis von $\mathcal{L}(D)$ und wir können schreiben

$$\phi^*_D(K(\mathbb{P}^1)) = K(\frac{f_1}{f_0}) = K(\frac{g_1}{g_0}).$$

(3) Sind D_1, D_2 zwei Divisoren vom Grad 2, so gilt:

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \phi^*_{D_1}(K(\mathbb{P}^1)) = \phi^*_{D_2}(K(\mathbb{P}^1)).$$

Aufgabe 64: Sei C eine nichtsinguläre ebene Kubik in Charakteristik $\neq 2, 3$, P ein nicht auf C liegender Punkt und G eine Gerade, die P nicht enthält. Eine Abbildung $\pi : C \to G$ wird wie folgt definiert: Ist $Q \in C$, so sei $\pi(Q)$ der Schnittpunkt der Verbindungsgeraden von P und Q mit G. Man kann sehen, dass π ein Morphismus ist.

(1) Welchen Grad hat π?
(2) Welche Verzweigungsindizes $e_\pi(Q)$ treten auf?
(3) Welche geometrische Bedeutung haben die Verzweigungspunkte?
(4) Wieviele Geraden durch P sind Tangenten an C? (Eventuell muss man mit Vielfachheiten zählen.)

Aufgabe 65: Sei $f(x) \in K[x]$ ein separables Polynom vom Grad $n \geq 1$, $\mathrm{char}(K) \neq 2$ und C die durch $y^2 = f(x)$ definierte ebene projektive Kurve. Zeige:

(1) Im Fall $n = 1$ oder $n = 2$ ist C eine nichtsinguläre projektive ebene Quadrik und hat Geschlecht 0.
(2) Im Fall $n = 3$ ist C eine nichtsinguläre projektive ebene Kubik und hat Geschlecht 1.

Aufgabe 66: Sei C eine Kurve vom Geschlecht 1 und $D_1, D_2 \in \mathrm{Div}(C)$.

(1) Zeige die Implikation:

$$\mathrm{grad}(D_1) \geq 2 \quad \text{und} \quad \mathcal{L}(D_1) = \mathcal{L}(D_2) \quad \Longrightarrow \quad D_1 = D_2.$$

(2) Zeige an Hand eines Beispiels:

$$\mathcal{L}(D_1) = \mathcal{L}(D_2) \quad \not\Longrightarrow \quad D_1 = D_2.$$

Aufgabe 67: Eine hyperelliptische Kurve C vom Geschlecht $g \geq 2$ werde über einem Körper K der Charakteristik $\neq 2$ definiert durch eine Gleichung

$$y^2 = f(x) \text{ mit } f(x) = a_0 x^{2g+2} + a_1 x^{2g+1} + \cdots + a_{2g+1} x + a_{2g+2},$$

wo $f(x)$ ein separables Polynom vom Grad $2g + 2$ ist. C besitzt 2 zwei Punkte im Unendlichen, die mit ∞_1 und ∞_2 bezeichnet werden, und für die $\mathrm{ord}_{\infty_1}(x) = \mathrm{ord}_{\infty_2}(x) = -1$ gilt.
Zeige: Ist a_0 kein Quadrat in K, so gilt $\infty_1, \infty_2 \notin C(K)$.
Hinweis: Ist $P \in C(K)$, so gilt für alle $f \in \mathcal{O}_{C,P} \cap K(C)$ natürlich $f(P) \in K$.

Aufgabe 68: Gib Beispiele für hyperelliptische Kurven C vom Geschlecht 2 an, die über einem der folgenden Körper K definiert sind und keinen K-rationalen Punkt besitzen. Folgende Körper sollen betrachtet werden:

$$\mathbb{R}, \quad \mathbb{F}_3, \quad \mathbb{F}_5, \quad \mathbb{F}_7, \quad \mathbb{F}_{11}.$$

Aufgabe 69: Unter den Namen *Hasse-Weil Bound* [1] oder *Weil-Schranke* [2] ist folgende Abschätzung für die Anzahl der $\mathbb{F}_p$-rationalen Punkte einer über $\mathbb{F}_p$ definierten, absolut irreduziblen, nichtsingulären, projektiven Kurve vom Geschlecht g bekannt:

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}.$$

Zeige mit Hilfe dieser Abschätzung folgende Aussagen:

(1) Jede über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 1 hat mindestens einen $\mathbb{F}_p$ rationalen Punkt.
(2) Ist C eine über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 2 mit $C(\mathbb{F}_p) = \emptyset$, so gilt $p \in \{2, 3, 5, 7, 11, 13\}$.

Aufgabe 70: Sei C eine über einem algebraisch abgeschlossenen Körper K mit von 2 verschiedener Charakteristik durch die Gleichung $y^2 = f(x)$ definierte hyperelliptische Kurve vom Geschlecht g, wobei $f(x) \in K[x]$ ein separables Polynom vom Grad $2g+1$ ist. Mit der *Mumford representation* erhält man eine Beschreibung der Divisorenklassengruppe $\mathrm{Pic}^0(C)$ durch eine Menge von Polynompaaren:

$$\mathrm{Pic}^0(C) = \{(a,b) : a, b \in K[x], a \text{ normiert}, \mathrm{grad}(b) < \mathrm{grad}(a) \leq g, a \mid f - b^2\}.$$

Die Addition in $\mathrm{Pic}^0(C)$ wird dann durch den *Algorithmus von Cantor* beschrieben [3]:

Eingabe: $(a_1, b_1), (a_2, b_2) \in \mathrm{Pic}^0(C)$
Ausgabe: $(a, b) \in \mathrm{Pic}^0(C)$ mit $(a, b) = (a_1, b_1) + (a_2, b_2)$ in $\mathrm{Pic}^0(C)$

1: $d_1 \leftarrow \mathrm{ggT}(a_1, a_2)$ und e_1, e_2 mit $d_1 = e_1 a_1 + e_2 a_2$
2: $d \leftarrow \mathrm{ggT}(d_1, b_1 + b_2)$ und c_1, c_2 mit $d = c_1 d_1 + c_2(b_1 + b_2)$
3: $s_1 \leftarrow c_1 e_1$, $s_2 \leftarrow c_1 e_2$, $s_3 \leftarrow c_2$
4: $a \leftarrow \frac{a_1 a_2}{d^2}$, $b \leftarrow \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a$
5: **while** $\mathrm{grad}(b) > g$ **do**
6: $\quad a \leftarrow \frac{f - b^2}{a}$
7: $\quad b \leftarrow (-b) \bmod a$
8: **end while**
9: Dividiere a durch den höchsten Koeffizienten, sodass a dann normiert ist
10: **return** (a, b)

Mit der angegebenen Identifikation ist $(1, 0)$ das neutrale Element in $\mathrm{Pic}^0(C)$.

(1) Zeige, dass $(a, b) + (a, -b) = (1, 0)$ gilt.
(2) Zeige, dass $2 \cdot (a, b) = (1, 0)$ genau dann gilt, wenn $b = 0$ gilt.
(3) Welche Elemente in $\mathrm{Pic}^0(C)$ haben die Gestalt $(a, 0)$?
(4) Beschreibe die Untergruppe der 2-Torsionselemente

$$A = \{(a, b) \in \mathrm{Pic}^0(C) : 2 \cdot (a, b) = (1, 0)\}$$

von $\mathrm{Pic}^0(C)$.
(5) Zeige folgende Isomorphie von Gruppen

$$A \simeq (\mathbb{Z}/2\mathbb{Z})^{2g},$$

und damit $\#A = 2^{2g}$.

---

[1] J. W. P. Hirschfeld, G. Korchmaros, F. Torres. Algebraic Curves over a Finite Field. Princeton University Press, 2008. S.343, Theorem 9.18 (Hasse-Weil Bound)

[2] W. Lütkebohmert. Codierungstheorie. Vieweg, 2003. S.162, Satz 7.4.1 (Weil-Schranke)

[3] Henri Cohen, Gerhard Frey et al. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2006. S.308, Algorithm 14.7

Literaturverzeichnis

[Barth] Wolf P. Barth. Ebene Algebraische Kurven. Vorlesungsskript. Erlangen, 2004.

[Brieskorn-Knoerrer] Egbert Brieskorn, Horst Knörrer. Plane Algebraic Curves. Birkhäuser, 1986.

[Cohen-Frey] Henri Cohen, Gerhard Frey et al. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2006.

[Diffie-Hellman] Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976.

[Forster1] Otto Forster. Analysis 1. 12. Auflage. Springer Spektrum, 2016.

[Fulton] William Fulton. Algebraic Curves. 2008.

[Geer-Lint] G. van der Geer, J. H. van Lint. Introduction to Coding Theory and Algebraic Geometry. Birkhäuser, 1988.

[Gille-Szamuely] Philippe Gille, Tamas Szamuely. Central Simple Algebras and Galois Cohomology. Second Edition. Cambridge University Press, 2017.

[Hartshorne] Robin Hartshorne. Algebraic Geometry. Springer, 1977.

[HKT] J. W. P. Hirschfeld, G. Korchmaros, F. Torres. Algebraic Curves over a Finite Field. Princeton University Press, 2008.

[Hulek] Klaus Hulek. Elementare Algebraische Geometrie. 2. Auflage. Springer Spektrum, 2012.

[Luetkebohmert] Werner Lütkebohmert. Codierungstheorie. Vieweg, 2003.

[Serre 1970] Jean-Pierre Serre. Cours d'arithmétique. Presses Universitaires de France, 1970.

[Serre] Jean-Pierre Serre. A Course in Arithmetic. Springer, 1973.

[SerreLF] Jean-Pierre Serre. Local Fields. Springer, 1979.

[Silverman] Joseph H. Silverman. The Arithmetic of Elliptic Curves. Second Edition. Springer, 2009/2016.

[Stichtenoth] Henning Stichtenoth. Algebraic Function Fields and Codes. Second Edition. Graduate Texts in Mathematics **254**. Springer, 2009.

[Tunnell] J. B. Tunnell. A Classical Diophantine Problem and Modular Forms of Weight 3/2. Invent. math. **72**, 323-334 (1983).