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 $f_k g_l$ homogen vom Grad $k + l$. Dann ist
$$fg \quad = \quad \sum_{m \ge 0} \left(\sum_{k+l=m} f_k g_l \right) = \sum_{k_0+l_0 \le m \le k_1+l_1} \left(\sum_{k+l=m} f_k g_l \right).$$
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. ■

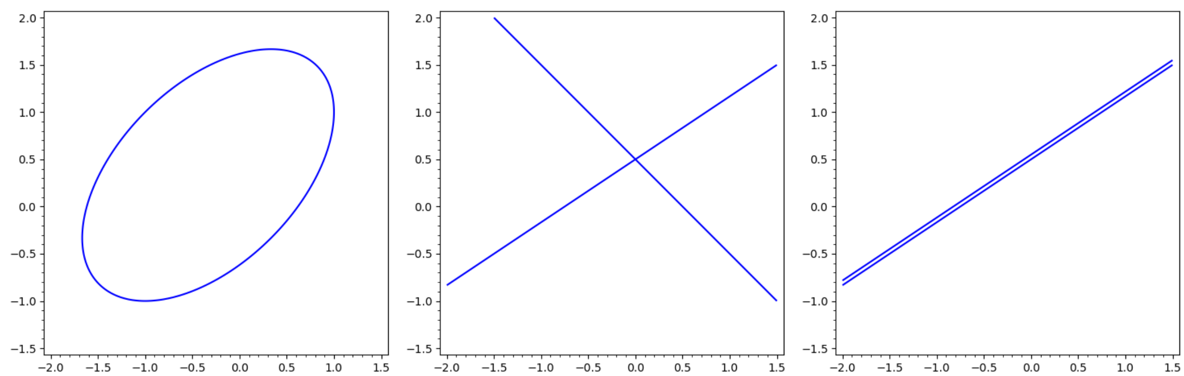
Ist nun $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2] \setminus \{0\}$ homogen vom Grad 2, so gibt es folgende Möglichkeiten für die Zerlegung von f in $\overline{K}[x_0, x_1, x_2]$:

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

Datei: algku4.tex. Version vom 19.7.2021

- **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 $\ell_1(x_0, x_1, x_2) = b_0 x_0 + b_1 x_1 + b_2 x_2$. Dann gilt:
$$\begin{aligned} P \text{ Singularität von } C \quad &\iff \quad \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0 \text{ für } i = 0, 1, 2 \quad \iff \\ &\iff \quad b_i \ell_2(p_0, p_1, p_2) = 0 \text{ für } i = 0, 1, 2 \quad \iff \\ &\iff \quad \ell_2(p_0, p_1, p_2) = 0. \end{aligned}$$
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 $\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = A_f \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$

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

Daher ist die Implikation $\Longrightarrow$ im obigen Lemma klar. Ist umgekehrt $\begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} \in \operatorname{Kern}(A_f)$, 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 $\operatorname{char}(K) \neq 2$ dann $f(P) = 0$, d.h. $P \in C(\overline{K})$, sodass P ein singulärer Punkt von C ist. ■

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

Satz. *(*$\operatorname{char}(K) \neq 2$*) 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* $\operatorname{Rang}(A_f) = 1$ *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 $\operatorname{Rang}(A_f) = 1$.

Beweis:

- $\operatorname{Rang}(A_f) = 1$ 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

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

  - **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

$$\begin{aligned} f &= a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = a_3x_1^2 + a_4x_1x_2 + \frac{a_4^2}{4a_3}x_2^2 = \\ &= \frac{1}{4a_3} \cdot \left(4a_3^2x_1^2 + 4a_3a_4x_1x_2 + a_4^2x_2^2\right) = \frac{1}{4a_3} \cdot \left(2a_3x_1 + a_4x_2\right)^2. \end{aligned}$$

    * **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 $f = \ell_1\ell_2$.*

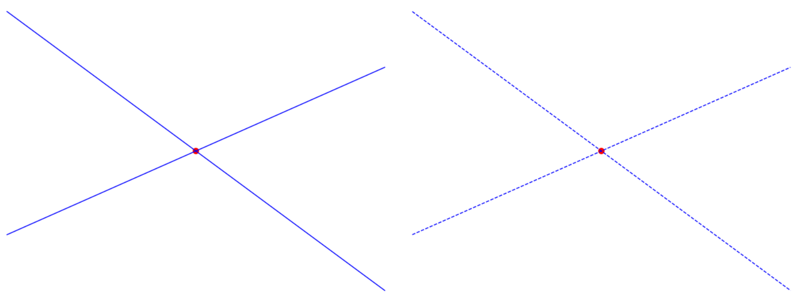
Der singuläre Punkt ist in diesem Fall $(p_0 : p_1 : p_2)$ mit $\mathrm{Kern}(A_f) = K \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix}$. Insbesondere ist $(p_0 : p_1 : p_2) \in C(K)$.

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

$$A_f = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2c \end{pmatrix} \text{ mit } \mathrm{Rang}(A_f) = 2 \text{ und } \mathrm{Kern}(A_f) = K \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

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. *(*$\mathrm{char}(K) \neq 2$*) 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:
- *C ist nichtsingulär.*
- $\mathrm{Rang}(A_f) = 3$.
- *$H_f \neq 0$, 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 $\mathrm{char}(K) = 2$ 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*
$$A_f = \begin{pmatrix} 0 & a_1 & a_2 \\ a_1 & 0 & a_4 \\ a_2 & a_4 & 0 \end{pmatrix} \quad \text{und} \quad \mathrm{Rang}(A_f) \in \{0, 2\}.$$
- *Ist $(a_1, a_2, a_4) = 0$, so gilt $\mathrm{Rang}(A_f) = 0$ 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 $\mathrm{Rang}(A_f) = 2$,*
$$\mathrm{Kern}(A_f) = K \begin{pmatrix} a_4 \\ a_2 \\ a_1 \end{pmatrix}$$
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:
$$C \text{ singulär} \quad \iff \quad a_0a_4^2 + a_1^2a_5 + a_1a_2a_4 + a_2^2a_3 = 0.$$
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 $\operatorname{char}(K) \neq 2$ 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

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

also

$$\begin{pmatrix} \frac{\partial f}{\partial x_0} \\ \frac{\partial f}{\partial x_1} \\ \frac{\partial f}{\partial x_2} \end{pmatrix} = \begin{pmatrix} 2a_0x_0 + a_1x_1 + a_2x_2 \\ a_1x_0 + 2a_3x_1 + a_4x_4 \\ a_2x_0 + a_4x_1 + 2a_5x_2 \end{pmatrix} = \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = 2Ax.$$

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

$$p^t A x = 0$$

die Tangente in P an C.
Ist P kein Kurvenpunkt, so wird durch

$$p^t A x = 0$$

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

$$\frac{\partial f}{\partial x_0}(P)x_0 + \frac{\partial f}{\partial x_1}(P)x_1 + \frac{\partial f}{\partial x_2}(P)x_2 = 2x^t A p = 2p^t A x = p_0 \frac{\partial f}{\partial x_0} + p_1 \frac{\partial f}{\partial x_1} + p_2 \frac{\partial f}{\partial x_2}.$$

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

$$p_0 \frac{\partial f}{\partial x_0} + p_1 \frac{\partial f}{\partial x_1} + p_2 \frac{\partial f}{\partial x_2} = 0$$

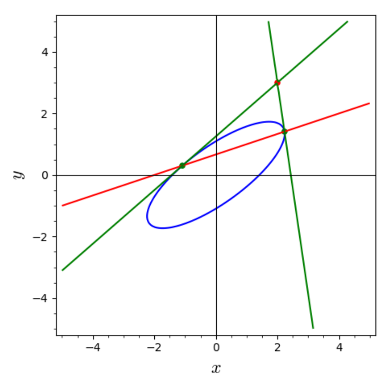
darstellen. Mittels der letzten Darstellung wird „Polare“ auch für Kurven höheren Grades definiert.

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

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

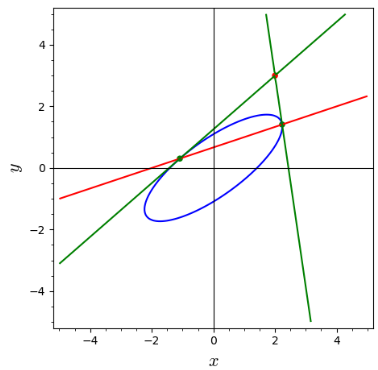
beschrieben. Damit gilt:

$$\begin{aligned} P \in T_Q \quad &\iff \quad p_0 \frac{\partial f}{\partial x_0}(q_0, q_1, q_2) + p_1 \frac{\partial f}{\partial x_1}(q_0, q_1, q_2) + p_2 \frac{\partial f}{\partial x_2}(q_0, q_1, q_2) = 0 \quad \iff \\ &\iff \quad g(q_0, q_1, q_2) = 0. \end{aligned}$$

Dies beweist die Behauptung. ■

Wir formulieren den vorangegangenen nochmals etwas genauer für Quadriken.

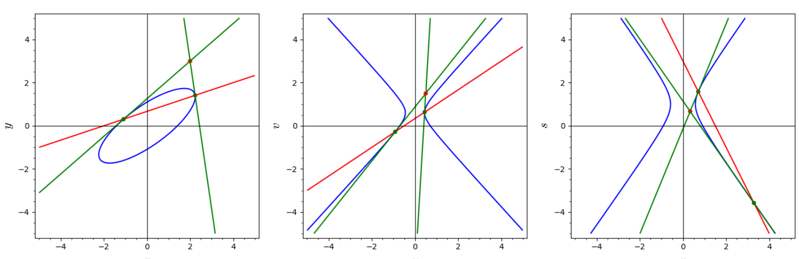
Satz. ($\mathrm{char}(K) \neq 2$) *Sei C eine nichtsinguläre projektive ebene Quadrik und $P \in \mathbb{P}^2 \setminus C(\overline{K})$. Dann gibt es genau zwei Tangenten an C, die durch P gehen. Die Berührpunkte dieser Tangenten mit C sind genau die Schnittpunkte der Polaren des Punktes P mit C.*



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:
  $$\begin{aligned} &P \text{ liegt auf der Tangente (in } Q \text{ an } C) \quad \iff \quad q^t A p = 0 \quad \iff \\ \iff \quad &p^t A q = 0 \quad \iff \quad Q \text{ liegt auf der Polaren des Punktes } P \text{ bezüglich } C. \end{aligned}$$
  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.

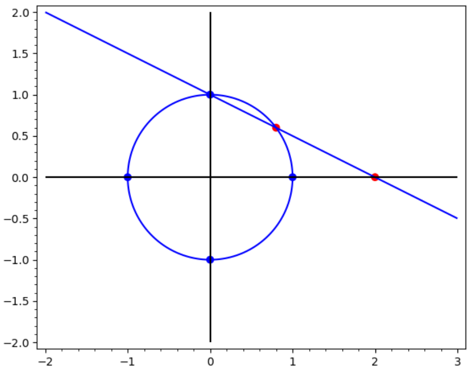


Bemerkung: ($\mathrm{char}(K) \neq 2$) Gegeben sei eine nichtsinguläre projektive ebene Quadrik C durch ein Polynom $f(x_0, x_1, x_2)$ und ein Punkt $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2 \setminus C(\overline{K})$. Wie bestimmt man die Geraden, die Tangenten an C sind und durch P gehen?

- 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**

$\quad T \leftarrow T \begin{pmatrix} 1 & 0 & -\frac{a_2}{2a_0} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_3, a_4, a_5 - \frac{a_2^2}{4a_0})$
$\quad$ Quadratische Ergänzung
end if
$\triangleright$ 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.
if $a_3 = 0$ **then** $\qquad \triangleright$ $f = a_0x_0^2 + a_4x_1x_2 + a_5x_2^2$. Was macht man nun?
$\quad$ **if** $a_5 \neq 0$ **then**
$\qquad T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_5, a_4, 0)$ $\qquad \triangleright$ Vertausche x_1 und x_2.
$\quad$ **else if** $a_4 \neq 0$ **then**
$\qquad T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_4, a_4, 0)$
$\quad$ **else**
$\qquad$ **return** $(a_0, 0, 0, 0, 0, 0)$,T $\qquad \triangleright$ $f = a_0x_0^2$
$\quad$ **end if**
end if
$\triangleright$ Nun ist $f = a_0x_0^2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2$ mit $a_0, a_3 \neq 0$.
if $a_4 \neq 0$ **then**
$\quad T \leftarrow T \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{a_4}{2a_3} \\ 0 & 0 & 1 \end{pmatrix}$, $(a_0, a_1, a_2, a_3, a_4, a_5) \leftarrow (a_0, 0, 0, a_3, 0, a_5 - \frac{a_4^2}{4a_3})$
end if
return $(a_0, a_1, a_2, a_3, a_4, a_5)$,$T$ $\qquad \triangleright$ 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 $\mathbb{R}$-rationale Punkte?

Gegeben sei eine über $\mathbb{R}$ definierte projektive ebene Quadrik C durch ein Polynom

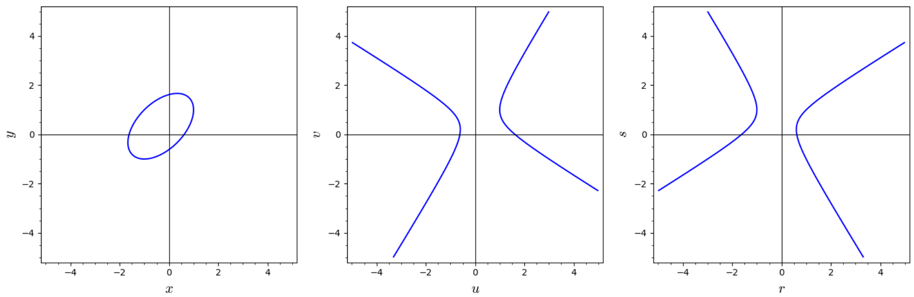
$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in \mathbb{R}[x_0, x_1, x_2].$$

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

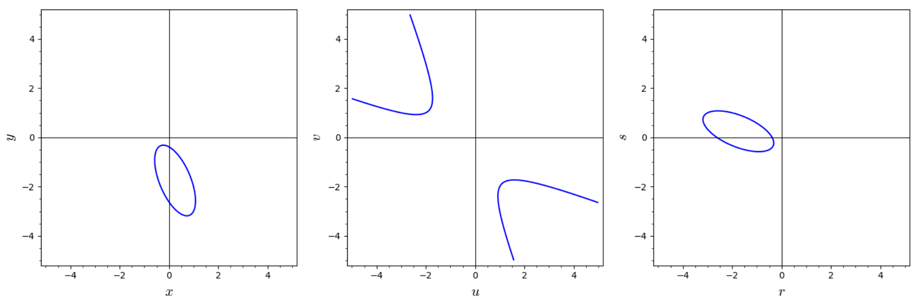
$$\{(x, y) \in \mathbb{R}^2 : f(1, x, y) = 0\},$$
$$\{(u, v) \in \mathbb{R}^2 : f(u, 1, v) = 0\},$$
$$\{(r, s) \in \mathbb{R}^2 : f(r, s, 1) = 0\}$$

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:

$$C(\mathbb{R}) \neq \emptyset \quad \iff \quad \begin{cases} 4a_0a_3 - a_1^2 \leq 0 \\ \text{ oder} \\ a_0(4a_0a_3a_5 + a_1a_2a_4 - a_0a_4^2 - a_3a_2^2 - a_5a_1^2) \leq 0. \end{cases}$$

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:

$$f \text{ ist positiv definit} \quad \iff \quad d_1 > 0 \quad \text{und} \quad d_2 > 0 \quad \text{und} \quad d_3 > 0.$$

  Das Hauptminorenkriterium für Definitheit kann man nachlesen bei *G. Fischer. Lineare Algebra. 18. Auflage. Springer Spektrum, 2014* auf Seite 327.

- Nun gilt:

$$f \text{ ist positiv definit} \quad \iff \quad d_1 > 0, \quad d_2 > 0, \quad d_3 > 0$$

  und

$$f \text{ ist negativ definit} \quad \iff \quad -f \text{ ist positiv definit} \quad \iff \quad d_1 < 0, \quad d_2 > 0, \quad d_3 < 0.$$

  Mit dem vorangegangenen Lemma folgt

$$\begin{aligned} C(\mathbb{R}) = \emptyset \quad &\iff \quad f \text{ ist positiv definit oder } f \text{ ist negativ definit} \quad \iff \\ &\iff \quad (d_1 > 0, d_2 > 0, d_3 > 0) \quad \text{oder} \quad (d_1 < 0, d_2 > 0, d_3 < 0). \end{aligned}$$

  Da nun aber gilt:

$$d_1d_3 > 0 \quad \iff \quad (d_1 > 0, d_3 > 0) \quad \text{oder} \quad (d_1 < 0, d_3 < 0)$$

  können wir weiter schreiben

$$C(\mathbb{R}) = \emptyset \quad \iff \quad d_1d_3 > 0 \text{ und } d_2 > 0.$$

  Die Negation liefert

$$C(\mathbb{R}) \neq \emptyset \quad \iff \quad d_1d_3 \leq 0 \text{ oder } d_2 \leq 0.$$

  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 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 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

$$b_0 + b_1x^2 = 0 \quad \text{bzw.} \quad x^2 = -\frac{b_0}{b_1}.$$

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
$$b_i x_i^2 = b_i' c_i^2 x_i^2 = b_i'(c_i x_i)^2$$
führen wir neue Koordinaten y_0, y_1, y_2 durch
$$y_i = c_i x_i \text{ bzw. } x_i = \frac{1}{c_i} y_i$$
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
$$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2$$
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
$$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \quad \text{mit} \quad b_0 \in \mathbb{N}, \quad b_1 \in \mathbb{N}, \quad b_2 \in \mathbb{Z} \setminus \{0\}$$
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*
$$f = b_0x_0^2 + b_1x_1^2 + b_2x_2^2$$
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 nicht-singuläre 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

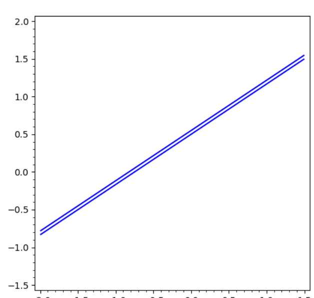
$$f_p = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 \in \mathbb{F}_p[x_0, x_1, x_2].$$

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

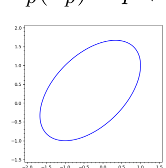
$$f_2 = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 = (b_0x_0 + b_1x_1 + b_2x_2)^2 \in \mathbb{F}_2[x_0, x_1, x_2].$$

  C_2 ist also eine Doppelgerade.

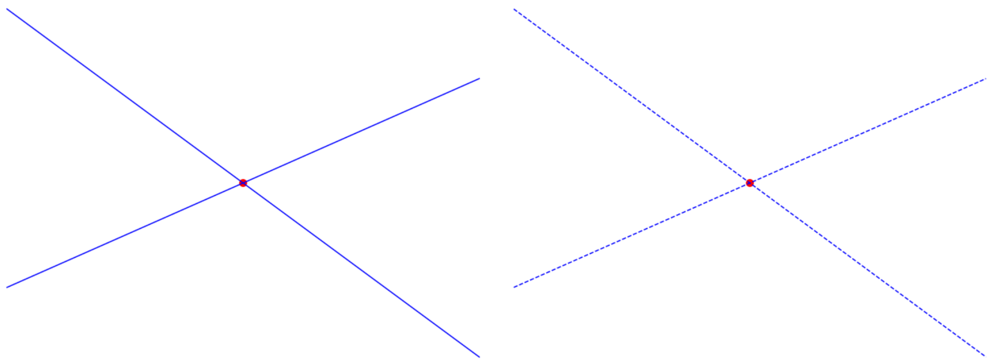


- **Fall $p > 2$, $p \nmid b_0b_1b_2$:** Betrachtet man b_0, b_1, b_2 in $\mathbb{F}_p$, so gilt $b_0, b_1, b_2 \in \mathbb{F}_p^*$. Dann hat C_p Rang 3, ist also nichtsingulär und

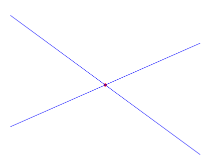
$$\#C_p(\mathbb{F}_p) = p + 1.$$



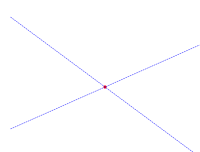
- **Fall $p > 2$, $p \mid b_0b_1b_2$:** Da die b_i paarweise teilerfremd sind, teilt p genau eine der Zahlen b_0, b_1, b_2, also o.E. b_0. Dann gilt
$$f_p = b_1x_1^2 + b_2x_2^2 \in \mathbb{F}_p[x_0, x_1, x_2], \quad b_1, b_2 \neq 0 \text{ in } \mathbb{F}_p.$$
C_p hat Rang 2 und genau eine Singularität, 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:*
$$C(\mathbb{Q}) \neq \emptyset \quad \Longrightarrow \quad \begin{cases} \textit{für alle ungeraden Primteiler } p \textit{ von } b_0b_1b_2 \\ \textit{zerfällt } f_p \textit{ in zwei verschiedene Linearfaktoren} \\ \textit{über } \mathbb{F}_p, \ \textit{d.h. } \#C_p(\mathbb{F}_p) = 2p+1. \end{cases}$$

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
$$f_p \quad = \quad b_1 x_1^2 + b_2 x_2^2 = b_1 x_1^2 - b_1 \frac{q_1^2}{q_2^2} x_2^2 = b_1 (x_1 - \frac{q_1}{q_2} x_2)(x_1 + \frac{q_1}{q_2} x_2),$$
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 $f = 101 x_0^2 + x_1^2 - 5 x_2^2$. 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

$$f_{(u,v)}(x_0, x_1, x_2) = ug(x_0, x_1, x_2) + vh(x_0, x_1, x_2).$$

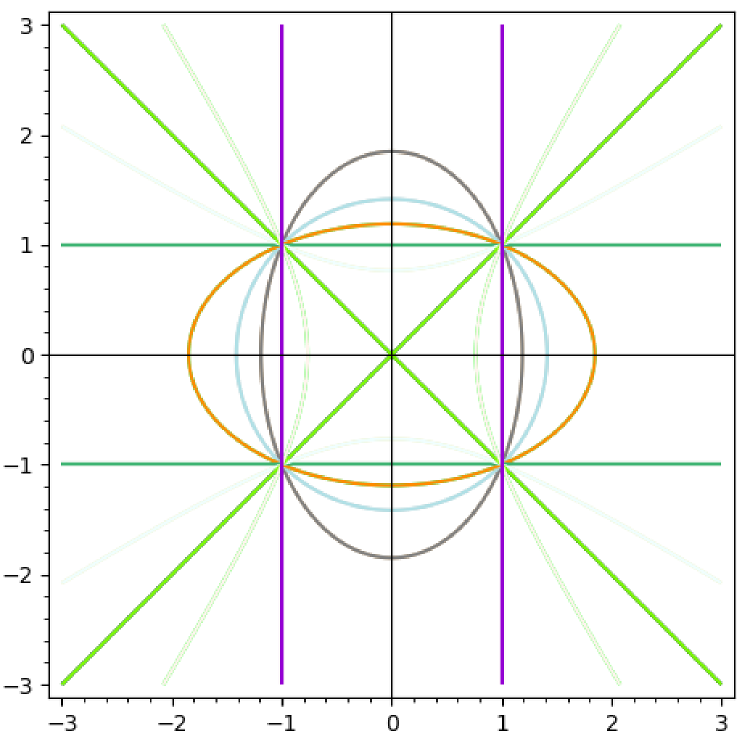
Es ist klar, dass die Nullstellenmenge $f_{(u,v)} = 0$ nur von $(u : v) \in \mathbb{P}^1$ abhängt. (Statt u, v verwenden wir auch manchmal andere Parameter.)
Beispiel: Die folgende Zeichnung zeigt einige Kurven des Büschels

$$u(x_1^2 - x_0^2) + v(x_2^2 - x_0^2) = 0,$$

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

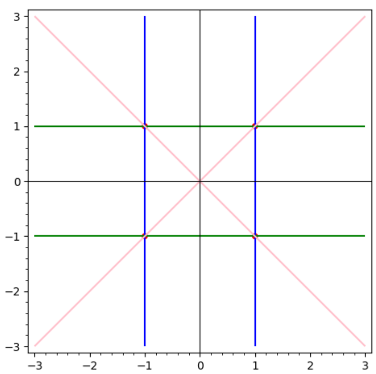
$$-8(u+v)uv.$$

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:
$$\begin{aligned} f(P_1) = f(P_2) = f(P_3) = f(P_4) = 0 \quad &\iff \quad a_0 = a_3 = a_5 = 0 \text{ und } a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = 0 \quad \iff \\ &\iff \quad a_0 = a_3 = a_5 = 0 \text{ und } a_4 = -a_1 - a_2. \end{aligned}$$
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 $1 \leq i < j \leq 4$ 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:

$$\begin{aligned} f \text{ definiert eine singuläre Quadrik} \quad &\iff \quad \operatorname{Rang}(A_f) \leq 2 \quad \iff \\ &\iff \quad \det(A_f) = 0 \quad \iff \\ &\iff \quad f \text{ zerfällt in 2 Linearfaktoren.} \end{aligned}$$

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

$$\begin{aligned} D &= \{ \text{ Doppelgeraden } \} = \\ &= \big\{4a_0a_3 - a_1^2 = 0, 4a_0a_5 - a_2^2 = 0, 4a_3a_5 - a_4^2 = 0, \\ &\quad 2a_0a_4 - a_1a_2 = 0, 2a_1a_5 - a_2a_4 = 0, 2a_2a_3 - a_1a_4 = 0\big\}. \end{aligned}$$

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 $a_0, \dots, a_5$ 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 $P_1, P_2, P_3, \dots$ vor und wollen alle Quadriken bestimmen, die durch diese Punkte gehen.
Jeder Punkt liefert für $a_0, \dots, a_5$ eine lineare Gleichung.

Quadriken durch 5 vorgegebene Punkte: Seien $P_1, \dots, P_5 \in \mathbb{P}^2$ 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.

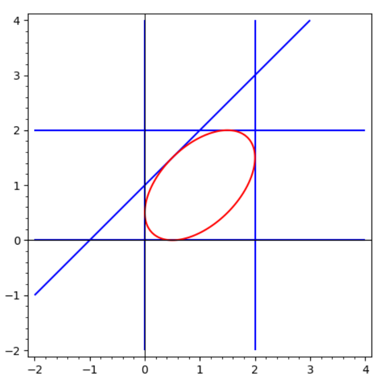
Geometrische Bedingungen: Die vorangegangenen Betrachtungen kann man verallgemeinern. Man sucht dann alle Quadriken, die bestimmte Bedingungen erfüllen.

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 $a_0x_0^2 + a_1x_0x_1 + \cdots + a_5x_2^2 = 0$ definierten Quadrik, indem wir $x_0 = 0$ einsetzen: $a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 = 0$. Die Quadrik berührt die Gerade, wenn es genau einen Schnittpunkt gibt, d.h. wenn gilt $a_4^2 - 4a_3a_5 = 0$ (Diskriminantenbedingung). Also folgt
$$\tau_{\{x_0=0\}} = \{(a_0 : a_1 : a_2 : a_3 : a_4 : a_5) \in \mathbb{P}^2 : a_4^2 - 4a_3a_5 = 0\},$$
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.