KAPITEL 2

Affine algebraische Mengen und ebene affine Kurven

Wir legen im Folgenden einen Körper K zugrunde, also beispielsweise

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

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

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

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

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

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

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

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

Die Menge aller solchen Polynome schreibt man als

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

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

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

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

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

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

Datei: algku2.tex. Version vom 19.7.2021

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

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

1. Affine algebraische Mengen

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

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

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

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

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

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

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

Beispiele:

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

  $$X \cup Y = \{f_1g_1 = \cdots = f_1g_s = f_2g_1 = \cdots = f_2g_s = \cdots = f_rg_1 = \cdots = f_rg_s = 0\}$$

  und der Durchschnitt

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

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

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

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

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

  Es ist

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

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

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

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

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

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

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

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

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

Zwei Geraden

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

und

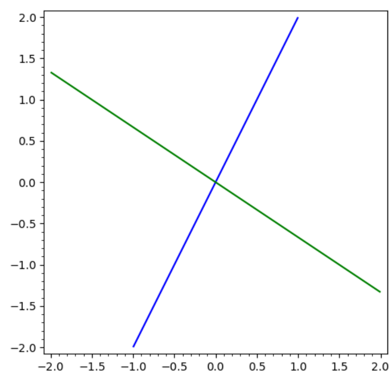
$$G_2 = \{(x, y) \in \mathbb{A}^2 : a_2 + b_2 x + c_2 y = 0\}$$

können in folgenden Beziehungen stehen:

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

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

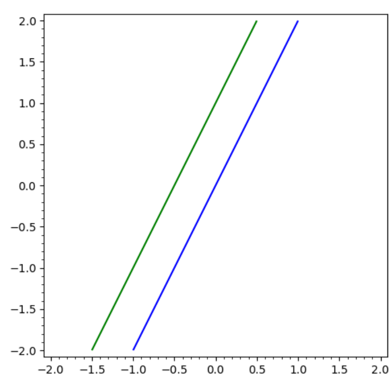
  eindeutig bestimmt ist. (G_1 und G_2 schneiden sich in einem Punkt.)



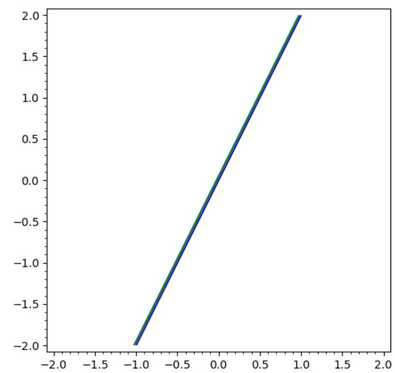
- Sind (b_1, c_1) und (b_2, c_2) linear abhängig, aber (a_1, b_1, c_1) und (a_2, b_2, c_2) linear unabhängig, so gilt

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

  (G_1 und G_2 sind parallel.)



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



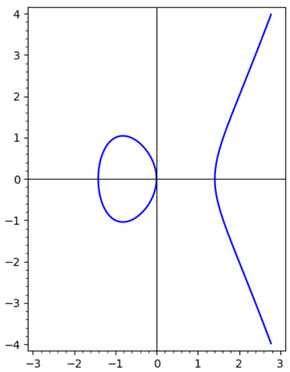
- Eine Gerade $G = \{(x, y) \in \mathbb{A}^2 : a + bx + cy = 0\}$ lässt sich in parametrisierter Form darstellen, d.h. man findet $\alpha, \beta, \gamma, \delta \in \overline{K}$ mit $(\beta, \delta) \neq 0$, sodass gilt:
$$G = \{(\alpha + \beta t, \gamma + \delta t) \in \mathbb{A}^2 : t \in \overline{K}\}.$$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

Definition.

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

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

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



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

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

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

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

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

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

- $X = \{1, i, -i\} \subseteq \mathbb{A}^1$ ist wegen $X = \{x \in \mathbb{A}^1 : (x-1)(x^2+1) = 0\}$ eine über $\mathbb{Q}$ definierte algebraische Menge mit $X(\mathbb{Q}) = \{1\}$.
- $X = \{(x,y) \in \mathbb{A}^2 : x^2 - 2y^2 = 0\}$ eine eine über $\mathbb{Q}$ definierte algebraische Menge. Die Menge der $\mathbb{Q}$-rationalen Punkte von X ist $X(\mathbb{Q}) = \{(0,0)\}$.
- Die algebraische Menge $X = \{(x,y) \in \mathbb{A}^2 : x - \sqrt{2}y = 0\}$ ist nicht über $\mathbb{Q}$ definiert, wohl aber über $\mathbb{Q}(\sqrt{2})$ (oder $\mathbb{R}$ oder $\mathbb{C}$).
- Sei $X = \{(1,i),(-1,-i)\} \subseteq \mathbb{A}^2$ (über $\mathbb{C}$ definiert). Wäre X über $\mathbb{R}$ definiert, so gäbe es Polynome $f_1, \ldots, f_r \in \mathbb{R}[x,y]$ mit
$$X = \{P \in \mathbb{A}^2 : f_1(P) = \cdots = f_r(P) = 0\}.$$
Wir können schreiben
$$f_j(x,y) = \sum_{k,l} a_{j,k,l} x^k y^l \text{ mit } a_{j,k,l} \in \mathbb{R}.$$
Aus $(1,i) \in X$ folgt $f_j(1,i) = 0$, d.h.
$$\sum_{k,l} a_{j,k,l} 1^k i^l = 0.$$
Komplexe Konjugation liefert
$$0 = \overline{\sum_{k,l} a_{j,k,l} 1^k i^l} = \sum_{k,l} a_{j,k,l} 1^k (-i)^l = f_j(1,-i).$$
Da dies für alle j gilt, würde $(1,-i) \in X$ folgen, ein Widerspruch. Daher ist X nicht über $\mathbb{R}$ definiert.
- Mit der gleichen Argumentation wie im letzten Beispiel erhält man Folgendes: Ist $X \subseteq \mathbb{A}^2$ eine über $\mathbb{R}$ definierte algebraische Menge, und gilt
$$\{(1,i),(-1,-i)\} \subseteq X,$$
so folgt
$$\{(1,i),(1,-i),(-1,-i),(-1,i)\} \subseteq X.$$

Affiner Koordinatenwechsel: Ein affiner Koordinatenwechsel wird gegeben durch eine Abbildung

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

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

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

Leicht beweist man folgendes Lemma:

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

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

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

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

Wir formen die Bedingung äquivalent um:

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

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

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

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

2. Ebene affine Kurven

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

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

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

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

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

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

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

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

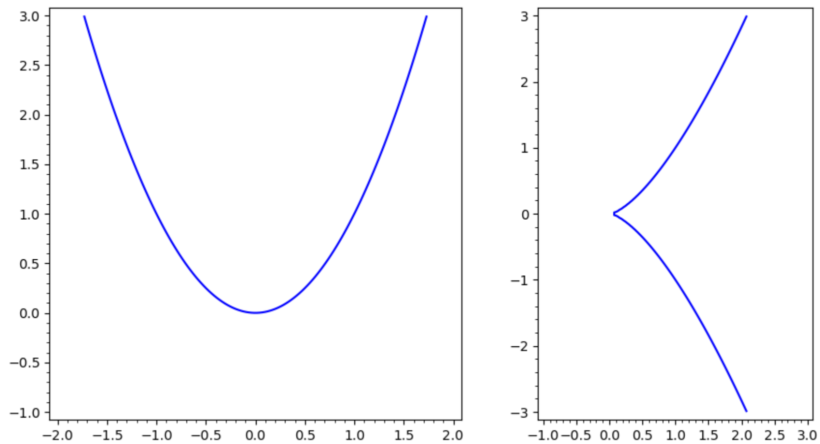
Beispiele:

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

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

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

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

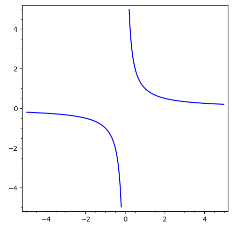


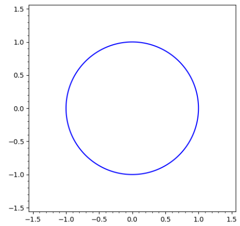
  (Die Bilder zeigen eigentlich die $\mathbb{R}$-rationalen Punkte der Kurven.)
- $f = x^2 - y^2 = (x-y)(x+y)$ definiert eine ebene Kurve C über $\mathbb{R}$ mit
$$\begin{aligned} C(\mathbb{R}) &= \{(x,y) \in \mathbb{R}^2 : (x-y)(x+y) = 0\} = \\ &= \{(x,y) \in \mathbb{R}^2 : y = x\} \cup \{(x,y) \in \mathbb{R}^2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

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

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

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





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

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

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

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

Wir wollen nun Kurven lokal um einen Punkt näher betrachten.

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

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

Es folgt

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

und damit

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

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

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

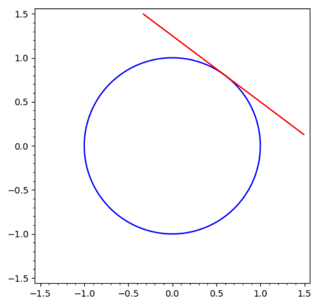
die lineare Approximation von f in P.

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

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

Beispiele:

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



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

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

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

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

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

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

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

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

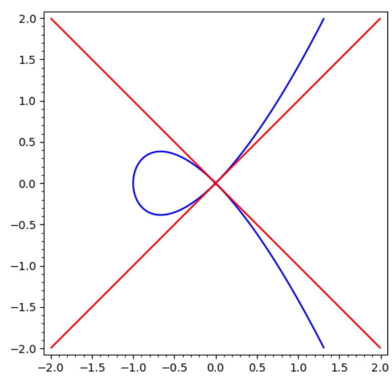
  Die Geraden $\alpha_i(x - x_0) + \beta_i(y - y_0) = 0$ nennt man (auch) **Tangenten** von C in P.

Beispiele:

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

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

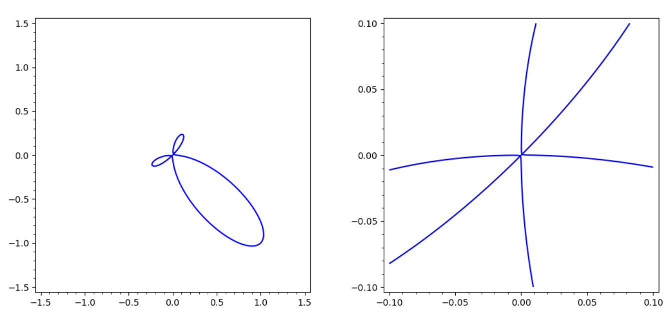
  daher ist die Multiplizität von C in P einfach 2 und $y = x$ und $y = -x$ sind die Tangenten.



- Wir betrachten die durch

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

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



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

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

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

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

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

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

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

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

Beispiel:

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

Wir schreiben f und g als Polynome in y:

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

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

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

Determinantenbildung liefert die Resultante:

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

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

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

Wir erhalten jetzt einfach folgenden Satz:

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

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

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

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

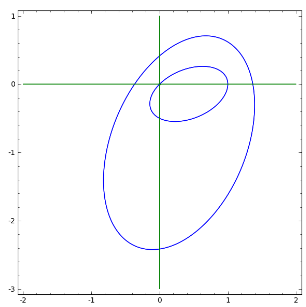
und

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

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

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

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



Wir wollen den Schnitt bestimmen. Wir bilden die Resultanten

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

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

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

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

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

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

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

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

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

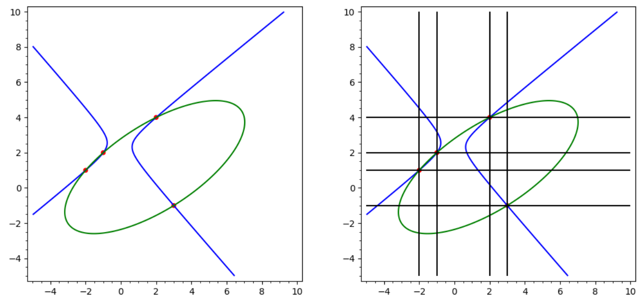
$$\begin{aligned} R_y(f,g)(x) &= 179372032x^4 - 358744064x^3 - 1255604224x^2 + 1434976256x + 2152464384 = \\ &= 179372032(x+2)(x+1)(x-2)(x-3), \\ R_x(f,g)(y) &= 179372032y^4 - 1076232192y^3 + 1255604224y^2 + 1076232192y - 1434976256 = \\ &= 179372032(y+1)(y-1)(y-2)(y-4). \end{aligned}$$

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

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

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

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



Wir geben eine Anwendung für die Singularitäten einer ebenen Kurve:

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

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

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

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

- *Fall 1:* $\frac{\partial f}{\partial y} \neq 0$. Wir schreiben
$$f(x,y) = a_0(x) + a_1(x)y + \cdots + a_m(x)y^m \quad \text{mit} \quad a_m(x) \neq 0.$$
Dann ist
$$\frac{\partial f}{\partial y}(x,y) = a_1(x) + \cdots + m a_m(x) y^{m-1}.$$
Da $f(x,y)$ irreduzibel ist, haben $f(x,y)$ und $\frac{\partial f}{\partial y}(x,y)$ keinen gemeinsamen Teiler. Also sind die beiden zugehörigen Resultanten $R_y(x)$ und $R_x(y)$ von 0 verschieden. Demnach haben $f(x,y) = 0$ und $\frac{\partial f}{\partial y}(x,y) = 0$ nur endlich viele Schnittpunkte, weswegen es auch nur endlich viele Singularitäten geben kann.
- *Fall 2:* $\frac{\partial f}{\partial x} \neq 0$. Diesen Fall behandelt man genauso wie Fall 1.
- *Fall 3:* $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$. Sei
$$f = \sum_{i,j} a_{ij} x^i y^j.$$
Dann ist
$$\frac{\partial f}{\partial x} = \sum_{i,j} i a_{ij} x^{i-1} y^j \quad \text{und} \quad \frac{\partial f}{\partial y} = \sum_{i,j} j a_{ij} x^i y^{j-1}$$
und damit $i a_{ij} = 0$ und $j a_{ij} = 0$. In Charakteristik 0 ist dies nicht möglich, da mindestens ein Indexpaar (i,j) mit $i > 0$ oder $j > 0$ existiert. Also ist die Charakteristik p. Im Fall $a_{ij} \neq 0$ gilt dann $i \equiv j \equiv 0 \bmod p$. Wählen wir $b_{ij} \in \overline{K}$ mit $b_{ij}^p = a_{pi,pj}$, so folgt
$$f = \sum_{i,j} a_{pi,pj} x^{pi} y^{pj} = \sum_{i,j} (b_{ij} x^i y^j)^p = (\sum_{i,j} b_{ij} x^i y^j)^p,$$
was der Irreduzibilität von f über $\overline{K}$ widerspricht. Also kann dieser Fall überhaupt nicht eintreten. ■

Beispiele:

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

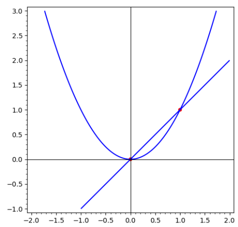
Schnittvielfachheiten: Sind C und D affine Kurven, so kann man eine Schnittvielfachheit $(C \cdot D)_P$ von C und D in einem Punkt $P \in \mathbb{A}^2$ definieren. Der Einfachkeit halber werden wir uns zunächst auf Schnitte von Kurven mit Geraden beschränken:

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

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

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

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



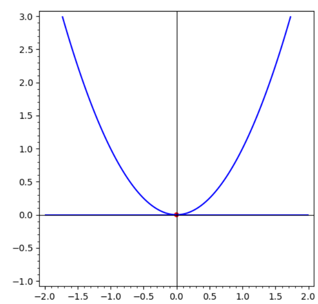
Nun betrachten wir wieder die Kurve $y = x^2$, die durch das Polynom $f(x, y) = y - x^2$ beschrieben wird, aber die Gerade G mit der Gleichung $y = 0$. Wegen

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

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

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

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

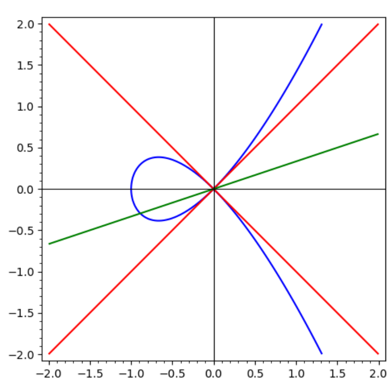


Bemerkung: Bei der Parametrisierung einer Geraden G muss man nicht künstlich einen Parameter t einführen, wenn eine andere Variable eventuell naheliegender ist. Wird die Gerade G beispielsweise durch $y = ax + b$ beschrieben, so ist

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

sodass man auch x als Parameter verwenden kann.

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



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

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

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

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

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

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

Die Schnittmultiplizität ist also 2.

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

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

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

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

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

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

Das vorangegangene Beispiel wird in folgendem Satz verallgemeinert.

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

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

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

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

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

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

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

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

Wir unterscheiden zwei Fälle:

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

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

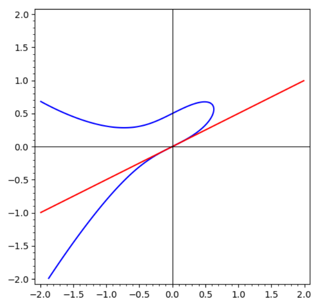
d.h. G ist Tangente. Wegen $\prod_{i=1}^{m}(\lambda_i \alpha + \mu_i \beta) = 0$ folgt $f(\alpha t, \beta t) = t^{m+1}(\dots)$, sodass $(C \cdot G)_P \geq m + 1$ gilt, wie behauptet.

- Für alle i ist $\lambda_i \alpha + \mu_i \beta \neq 0$. Dann ist

$$G = \{(\alpha t, \beta t) : t \in \overline{K}\} \nsubseteq \{\lambda_i x + \mu_i y = 0\}, \qquad \text{also} \qquad G \neq \{\lambda_i x + \mu_i y = 0\},$$

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

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



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

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

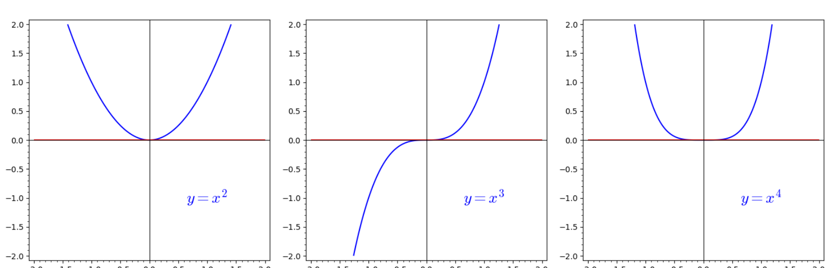
wählen wir als Parametrisierung $x = x$, $y = 0$ (mit Parameter x). Einsetzen in die Kurvengleichung ergibt

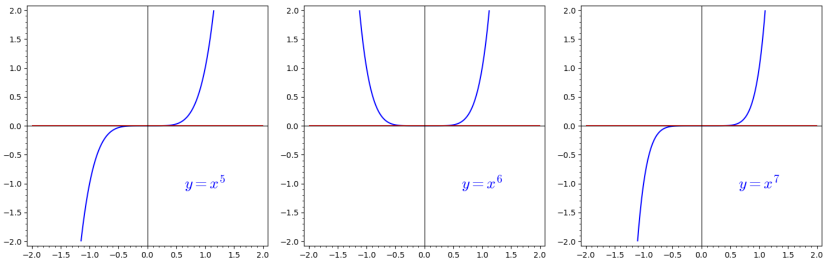
$$f(x, 0) = x^n.$$

Die Schnittmultiplizität ist also n:

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

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





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

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

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

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

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

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

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