Ebene Algebraische Kurven: VL 3

Affine algebraische Kurven sind Teilmengen von $\mathbb{C}^2$ von der Form

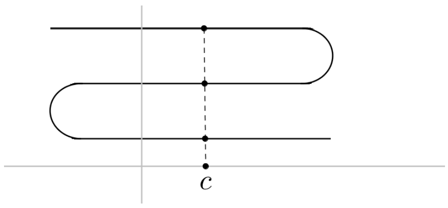
$$V(f) = \{(x, y) \subseteq \mathbb{C}^2 \mid f(x, y) = 0\},$$

wobei $f = f(X, Y) \in \mathbb{C}[X, Y]$.

(Wir notieren Variablen groß: X, Y und Werte klein: x, y.)

(2.4) Projektion; Schnitt mit Geraden

Die Abbildung $\pi : C \to \mathbb{C}$, $(x, y) \mapsto x$ mit $C \subset \mathbb{C}^2$ ist Projektion auf x-Achse.



Für $c \in \mathbb{C}$ ist $\pi^{-1}(c) = C \cap V(X - c)$, wobei $V(X - c)$ eine Gerade ist.

Wir schreiben $f(X, Y)$ in der Form

$$f(X, Y) = a_0(X)Y^d + a_1(X)Y^{d-1} + ... + a_d(X)$$

mit $a_0(X), a_1(X), ..., a_d(X) \in \mathbb{C}[X]$ und $a_0(X) \neq 0$. Setzen wir $X = c$ in f ein, erhalten wir:

$$f(c, Y) = a_0(c)Y^d + ... + a_d(c) \in \mathbb{C}[Y].$$

Außerdem ist $\pi^{-1}(c) = \{(c, d) \mid f(c, d) = 0\}$.

Wir unterscheiden nun die Fälle $d = 0$ und $d > 0$:

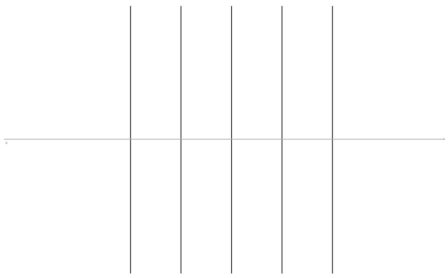
$\underline{d = 0}$: Wir erhalten

$$f(X, Y) = a_0(X),$$

also hängt die Gleichung nicht von Y ab. Außerdem erhalten wir

$$V(f) = \{(c, d) \mid a_0(c) = 0\},$$

welches eine Vereinigung von Grad(a_n)-vielen vertikalen Geraden ist.



$\underline{d > 0}$: Wir nehmen zusätzlich an, dass $a_0(c) \neq 0$. Also erhalten wir die Gleichung

$$a_0(c)Y^d + ... + a_d(c) = 0$$

und somit

$$Y^d + \frac{a_1(c)}{a_0(c)}Y^{d-1} + ... + \frac{a_d(c)}{a_0(c)} = 0.$$

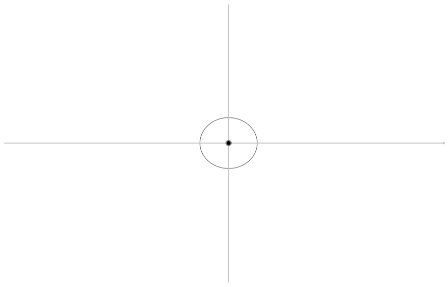
Daraus folgt

$$1 \leq \#C \cap V(X - c) \leq d.$$

Folgerung. *Jede affine algebraische Kurve enthält unendlich viele Punkte.*

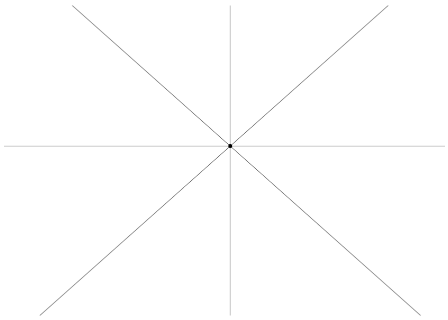
Beweis. Siehe oben. □

Beispiel: (1) $X^2 + Y^2 = 0$. Diese Gleichung hat nur eine reelle Lösung!

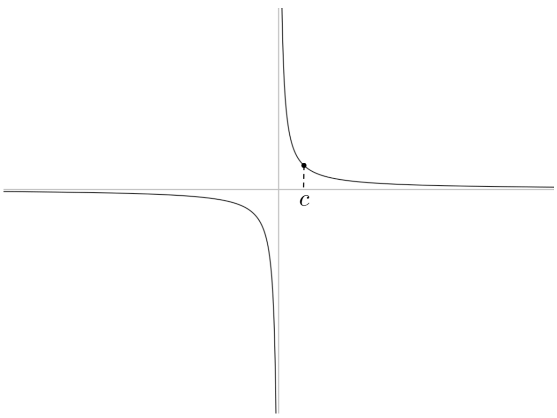


Die komplexen Lösungen erhalten wir durch $X^2 = -Y^2 = (iY)^2$, also $X = \pm iY$. Wir erhalten also als Faktorisierung $X^2 + Y^2 = (X + iY)(X - iY)$ und somit die komplex konjugierten Geraden $X + iY = 0$ und $X - iY = 0$.

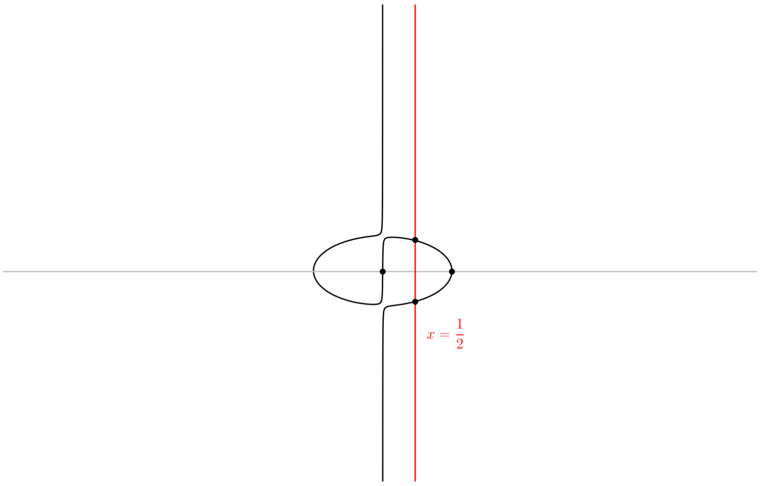
(2) $X^2 - Y^2 = 0$. Durch Faktorisierung erhalten wir $(X + Y)(X - Y) = 0$.



Beispiel: (1) $XY - 1 = 0$.



Es ist $f(c,Y) = cY - 1$. Für $c = 0$ erhalten wir $f(0,Y) = -1$ und $\pi^{-1}(c) = \pi^{-1}(0) = C \cap V(X) = \emptyset$ (vertikale Asymptote).
(2) $X(X^2 + Y^2 - 1) + \varepsilon Y = 0$, $\varepsilon \neq 0$.



Nach Ausmultiplizieren erhalten wir $XY^2 + \varepsilon Y + X^3 - X = 0$ mit $a_0 = X, a_1 = \varepsilon$ und $a_2 = X^3 - X$. Diese Gleichung hat 2 Lösungen. Setzen wir $X = 0$, liefert dies $\varepsilon Y = 0$ und somit eine Lösung, nämlich $Y = 0$. Für $x \to 0$ erhalten wir eine Lösung $\to 0$ und eine andere Lösung $\to \infty$.

Oben hatten wir uns den Fall $d > 0$ mit der zusätzlichen Annahme $a_0(c) \neq 0$ angeschaut. Nun werden wir den Fall $d > 0$ allgemein betrachten.

$d > 0$ (allgemein):
$a_0(c) \neq 0$: $\mathrm{Grad}(f(c,Y)) = d \geq \#C \cap V(X-c) \geq 1$
$a_0(c) = 0$, $a_1(c) \neq 0$: $\mathrm{Grad}(f(c,Y)) = d - 1 \geq \#C \cap V(X-c) \geq 1$
...
$a_0(c) = ... = a_{k-1}(c) = 0, a_k(c) \neq 0$: $\mathrm{Grad}(f(c,Y)) = d - k \geq \#C \cap V(X-c) \geq 1$

$a_0(c) = 0 = ... = a_{d-1}(c) = 0, a_d(c) \neq 0$: $\#C \cap V(X-c) = \emptyset$
$a_0(c) = 0 = ... = a_d(c) = 0 : V(X-c) \subset C$

$a_0(X) = (X-c)b_0(X)$
...
$a_d(X) = (X-c)b_d(X)$

Wir folgern $f(X,Y) = (X-c)(b_0(X)Y^d + ... + b_d(X))$ und ziehen folgendes Fazit:

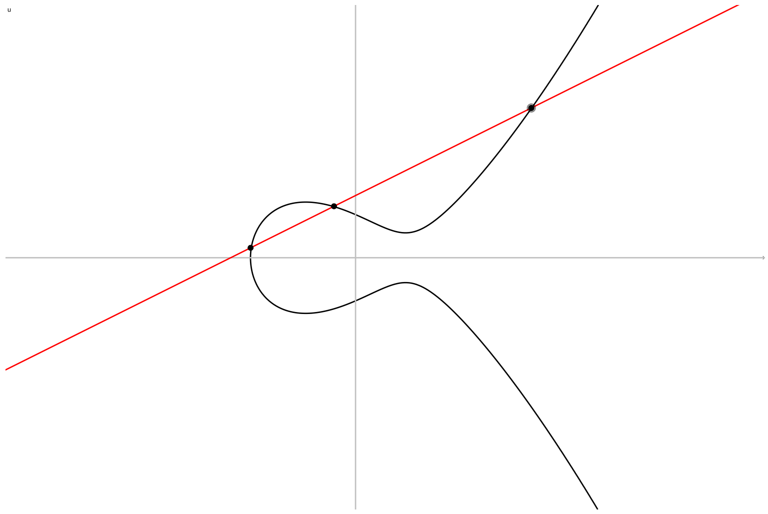
(a) Es existiert ein $k \in \{0, ..., d-1\}, a_k(c) \neq 0$, so dass $1 \leq \#C \cap V(X-c) \leq d$.
(b) Für alle k mit $a_k(c) = 0$ gilt: $V(X-c) \subset C$ und $(X-c)|f$.

Satz. *Sei $L = V(l)$ eine Gerade, $l = a + bX + cY$, und $C = V(f)$ eine affine algebraische Kurve. Dann gilt*:
(1) Ist $\#C \cap L < \infty$, dann $\#C \cap L \leq \mathrm{Grad}(f)$.
(2) Ist $\#C \cap L = \infty$, dann $L \subset C$ und $l|f$.

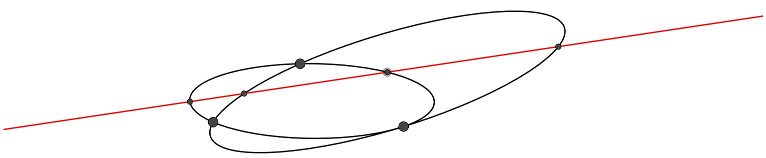
Beweis. Nach Koordinatentransformation erhalten wir $L = V(X), d \leq \mathrm{Grad}(f)$, etc. □

Beispiel:

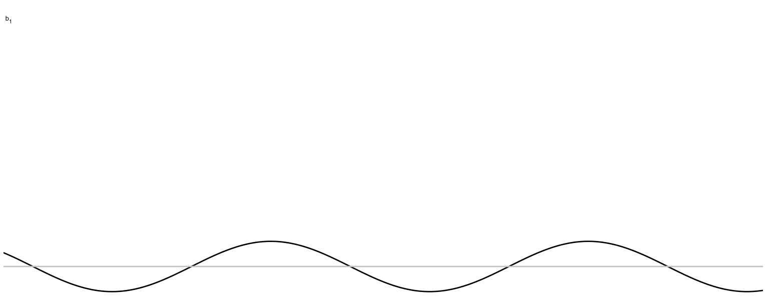
(1) $y^2 - x^3 + 3x - 3 = 0$



(2) $V(-5x^2 + 9xy - 8y^2 - 31x + 34y - 23) \cup V(-12x^2 - xy - 33y^2 - 10x + 4y - 12)$



(3) $y - sin(x) = 0$ ist keine affine algebraische Kurve



(4) Zykloide

Eine affine algebraische Kurve kann keine “Geradenstücke” enthalten.

(2.5) Resultante

Sei R ein faktorieller Ring, $R[Y]$ der Polynomring mit Koeffizienten in R und

$$\begin{aligned} f &= a_0Y^n + a_1Y^{n-1} + ... + a_n \\ g &= b_0Y^m + b_1Y^{m-1} + ... + b_n \end{aligned}$$

zwei Polynome in $R[Y]$ mit $a_i, b_i \in R$ und $a_0 \neq 0, b_0 \neq 0$.

Definition. Wir nennen h *gemeinsamen Faktor* von f und g, falls wir f schreiben können als $f = \tilde{f}h$ mit $h \in R[Y]$ und g schreiben können als $g = \tilde{g}h$ mit $h \notin R$ oder $\mathrm{Grad}(h) \geq 1$.

Definition. Die $(m+n) \times (m+n)$ Matrix

$$\mathrm{Syl}_{f,g} = \begin{pmatrix} a_0 & a_1 & ... & & a_n & 0 & 0 & ... & 0 \\ 0 & a_0 & ... & & a_{n-1} & a_n & 0 & ... & 0 \\ 0 & 0 & a_0 & ... & & & & & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & ... & & a_0 & ... & & & a_n \\ b_0 & b_1 & ... & & & b_m & 0 & ... & 0 \\ 0 & b_0 & ... & & & & b_m & ... & 0 \\ 0 & 0 & b_0 & ... & & & & & 0 \\ 0 & 0 & 0 & b_0 & b_1 & ... & & & b_m \end{pmatrix}$$

heißt *Sylvester-Matrix* von f und g.

Definition. Die Resultante $R_{f,g} \in R$ von f und g ist die Determinante der Sylvester-Matrix von f und g.

Satz. *Es ist $R_{f,g} = 0$ genau dann, wenn f und g gemeinsamen Faktor haben.*

Beweis. Wir setzen

$$\begin{aligned} p &= c_0 Y^{m-1} + ... + c_{m-1} \in R[Y] \\ q &= d_0 Y^{n-1} + ... + d_{n-1} \in R[Y] \end{aligned}$$

und berechnen

$$\begin{aligned} f \cdot p + g \cdot q &= (a_0 Y^n + a_1 Y^{n-1} + ...) \cdot (c_0 Y^{m-1} + c_1 Y^{m-2} + ...) \\ &+ (b_0 Y^m + b_1 Y^{m-1} + ...) \cdot (d_0 Y^{n-1} + d_1 Y^{n-2} + ...) \\ &= (a_0 c_0 + b_0 d_0) Y^{n+m-1} + a_1 c_0 + a_0 c_1 + (b_1 d_0 + b_0 d_1) Y^{n+m-2} + ... \end{aligned}$$

Die Koeffizienten von $Y^{n+m-1-i}$ des Polynoms $f \cdot p + g \cdot q$, wir bezeichnen sie im Folgenden mit e_i, erhält man durch

$$\begin{pmatrix} a_0 & 0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & 0 & b_1 & b_0 & 0 \\ a_2 & a_1 & a_0 & b_2 & b_1 & b_0 \\ \vdots & & & \vdots & & \\ a_n & & & b_m & & \\ & \ddots & & & \ddots & \\ & & a_0 & & & b_0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} e_0 \\ \\ \\ \vdots \\ \\ \\ e_{n+m-1} \end{pmatrix}$$

Also gilt:

$$f \cdot p + g \cdot q = 0$$

genau dann, wenn

$$Syl_{f,g}^T \cdot \begin{pmatrix} c_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Das heißt es gilt:

$$R_{f,g} = 0$$

genau dann, wenn

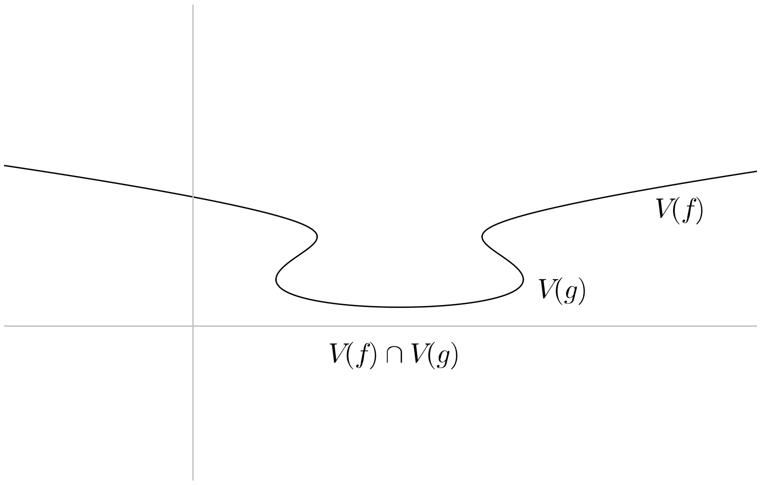
$$p \neq 0 \text{ und } q \neq 0 \text{ existieren mit} f \cdot p + g \cdot q = 0.$$

Nachdem wir die nötige Vorarbeit geleistet haben, werden wir nun zunächst die Rückrichtung zeigen. Wir nehmen also an, dass f und g gemeinsamen Faktor haben, also können wir f und g darstellen als $f = \tilde{f} \cdot h$ und $g = \tilde{g} \cdot h$. Daraus folgt $f \cdot \tilde{g} + g \cdot (-\tilde{f}) = 0$. Da $\tilde{g} \neq 0$ und $\tilde{f} \neq 0$, folgt $R_{f,g} = 0$.
Für die Hinrichtung nehmen wir $R_{f,g} = 0$ an. Dann gibt es $p \neq 0$ und $q \neq 0$ mit $f \cdot p + g \cdot q = 0$, das heißt $f \cdot p = -g \cdot q$ mit $\mathrm{Grad}(q) < \mathrm{Grad}(f)$. Da nicht alle irreduziblen Faktoren von f in q aufgehen können, haben f und g gemeinsamen Faktor. □

Satz (Lemma von Study). *Es sei $f \in \mathbb{C}[X,Y]$ mit $\mathrm{Grad}(f) \geq 1$ und Nullstellenmenge $V(f) = C$ und es sei $g \in \mathbb{C}[X,Y]$ irreduzibel. Falls $\#V(g) \cap V(f) = \infty$, dann gilt $V(g) \subset V(f)$ und $g \mid f$.*

Folgerung. *Falls $V(f) = V(\tilde{f})$, dann besitzen f und $\tilde{f}$ die gleichen irreduziblen Faktoren.*

Beweis. Für $\text{Grad}(g) = 1$ haben wir dies bereits in (2.4) gezeigt. Wir nehmen also an, dass $\text{Grad}(g) \geq 2$. Die Nullstellenmenge $V(g)$ von g kann keine Gerade enthalten!



Für die Resultante von f und g gilt $R_{f,g} \in \mathbb{C}[X, Y]$. Außerdem ist

$$R_{f,g}(c) = R_{f(c,Y),g(c,Y)},$$

falls $a_0(c) \neq 0, b_0(c) \neq 0$. Wir finden unendlich viele c mit $a_0(c) \neq 0$ und $b_0(c) \neq 0$ als x-Koordinaten von Schnittpunkten von $V(f)$ und $V(g)$. Also ist $Rf, g(c) = 0$ für unendlich viele c und somit ist $R_{f,g} \equiv 0$. Folglich haben f, g gemeinsamen Faktor. Da g irreduzibel ist, folgt $g \mid f$. $\square$