Ein Einblick in die algebraische Geometrie

Janko Böhm
boehm@math.uni-sb.de

Universität des Saarlandes

10.04.2011

Algebraische Varietäten

Algebraische Varietäten

Sei K ein Körper. Eine **affine algebraische Varietät** ist die gemeinsame Nullstellenmenge

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

von Polynomen $f_1, ..., f_r \in K[x_1, ..., x_n]$

Sei K ein Körper. Eine **affine algebraische Varietät** ist die gemeinsame Nullstellenmenge

$$V\left(f_1, ..., f_r\right) = \{p \in K^n \mid f_1\left(p\right) = 0, ..., f_r\left(p\right) = 0\}$$

von Polynomen $f_1, ..., f_r \in K\left[x_1, ..., x_n\right]$

Beispiele:

- $V\left(1\right) = \emptyset$, $V\left(0\right) = K^n$,

Algebraische Varietäten

Sei K ein Körper. Eine **affine algebraische Varietät** ist die gemeinsame Nullstellenmenge

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

von Polynomen $f_1, ..., f_r \in K[x_1, ..., x_n]$

Beispiele:

- $V(1) = \emptyset$, $V(0) = K^n$,
- die Lösungsmenge eines linearen Gleichungssystems

$$A \cdot x - b = 0$$

Algebraische Varietäten

Sei K ein Körper. Eine **affine algebraische Varietät** ist die gemeinsame Nullstellenmenge

$$V\left(f_1,\dots,f_r\right)=\left\{p\in K^n \mid f_1\left(p\right)=0,\dots,f_r\left(p\right)=0\right\}$$

von Polynomen $f_1,\dots,f_r\in K\left[x_1,\dots,x_n\right]$

Beispiele:

- $V\left(1\right)=\emptyset$, $V\left(0\right)=K^n$,
- die Lösungsmenge eines linearen Gleichungssystems
$$A\cdot x-b=0$$
- Der Graph
$$\Gamma\left(g\right)=V\left(x_2\cdot b\left(x_1\right)-a\left(x_1\right)\right)\subset K^2$$
einer rationalen Funktion
$$g=\frac{a}{b}\in K\left(x_1\right)$$

Beispiele von Varietäten: Graphen

Beispiele von Varietäten: Graphen

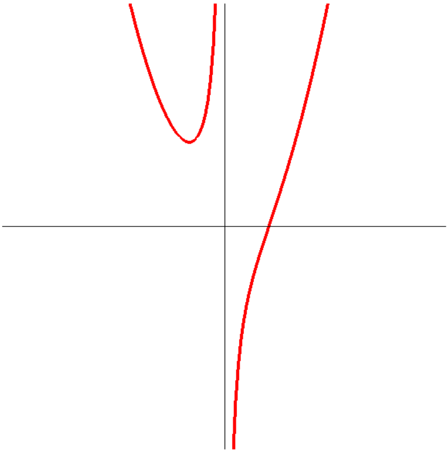
Der Graph von $g(x_1) = \frac{x_1^3 - 1}{x_1}$ ist

$$V\left(x_2 x_1 - x_1^3 + 1\right) \subset K^2$$

Beispiele von Varietäten: Graphen

Der Graph von $g(x_1) = \frac{x_1^3 - 1}{x_1}$ ist

$$V\left(x_2 x_1 - x_1^3 + 1\right) \subset K^2$$



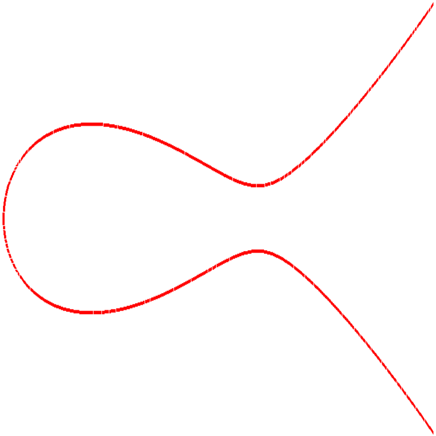
Beispiele von Varietäten: Kurven

Nicht jede Kurve in K^2 ist ein Graph, z.B. die **elliptische Kurve**

$$V\left(x_2^2 - x_1^3 - x_1^2 + 2x_1 - 1\right)$$

Nicht jede Kurve in K^2 ist ein Graph, z.B. die **elliptische Kurve**

$$V\left(x_2^2 - x_1^3 - x_1^2 + 2x_1 - 1\right)$$



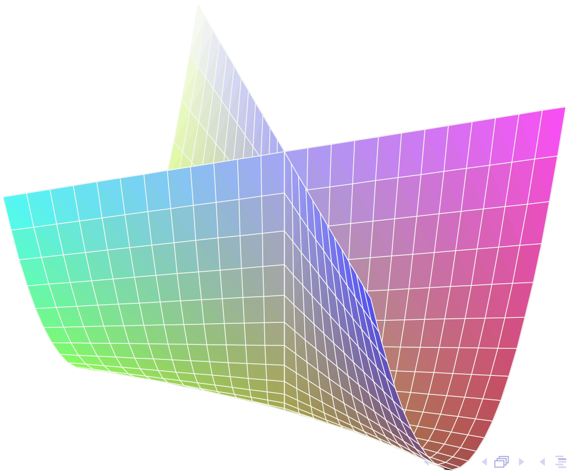
Beispiele von Varietäten: Flächen

Es gibt auch Varietäten höherer Dimension, z.B. der **Whitney-Umbrella**

$$V\left(y^2 - x^2 z\right)$$

Es gibt auch Varietäten höherer Dimension, z.B. der **Whitney-Umbrella**

$$V\left(y^2 - x^2 z\right)$$



Beispiele von Varietäten: Splines

Der kubische Spline $C \subset K^2$ parametrisiert durch

$$x_1(t) = p_0(1-t)^3 + 3p_1 t(1-t)^2 + 3p_2 t^2(1-t) + p_3 t^3$$
$$x_2(t) = q_0(1-t)^3 + 3q_1 t(1-t)^2 + 3q_2 t^2(1-t) + q_3 t^3$$

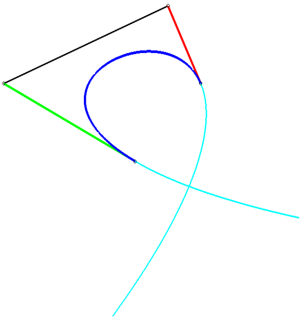
mit $t \in [0,1]$ geht durch die Punkte $(p_0, q_0), (p_3, q_3) \in K^2$ und die Tangenten an diesen Punkten durch (p_1, q_1) und (p_2, q_2).

Beispiele von Varietäten: Splines

Der kubische Spline $C \subset K^2$ parametrisiert durch

$$x_1(t) = p_0(1-t)^3 + 3p_1 t(1-t)^2 + 3p_2 t^2(1-t) + p_3 t^3$$
$$x_2(t) = q_0(1-t)^3 + 3q_1 t(1-t)^2 + 3q_2 t^2(1-t) + q_3 t^3$$

mit $t \in [0,1]$ geht durch die Punkte $(p_0, q_0), (p_3, q_3) \in K^2$ und die Tangenten an diesen Punkten durch (p_1, q_1) und (p_2, q_2).

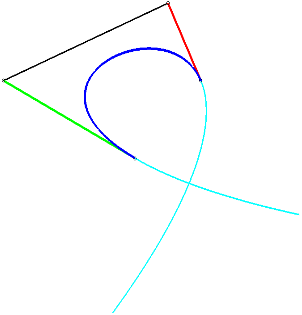


Beispiele von Varietäten: Splines

Der kubische Spline $C \subset K^2$ parametrisiert durch

$$x_1(t) = p_0(1-t)^3 + 3p_1 t(1-t)^2 + 3p_2 t^2(1-t) + p_3 t^3$$
$$x_2(t) = q_0(1-t)^3 + 3q_1 t(1-t)^2 + 3q_2 t^2(1-t) + q_3 t^3$$

mit $t \in [0,1]$ geht durch die Punkte $(p_0, q_0), (p_3, q_3) \in K^2$ und die Tangenten an diesen Punkten durch (p_1, q_1) und (p_2, q_2).



Das Kurvenstück C ist eine Teilmenge einer algebraischen Kurve $\overline{C}$. Diese ist der Abschluss von C in der **Zariski-Topologie**, bei der die abgeschlossenen Mengen die algebraischen Varietäten sind.

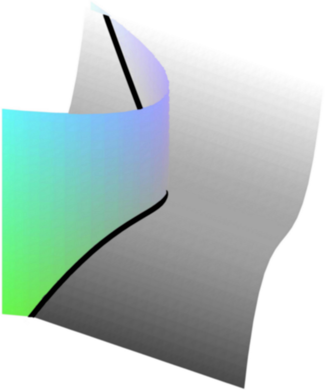
Projektionen

Die singuläre Kurve $\overline{C}$ erhält man als Projektion einer glatten Kurve im K^3, der **getwisteten Kubik**:

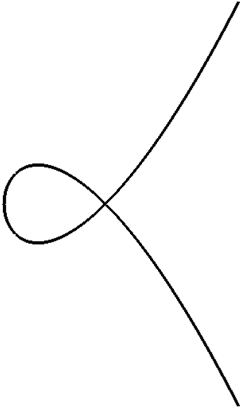
Projektionen

Die singuläre Kurve $\overline{C}$ erhält man als Projektion einer glatten Kurve im K^3, der **getwisteten Kubik**:

$$V\left(y - x^2, z - x^3\right)$$



$$\longrightarrow$$



Projektionen

(Loading twisted cubic.gif)

Ideale und Varietäten

Die affine Varietät $V(f_1, ..., f_r)$ hängt nur von dem von $f_1, ..., f_r \in R = K[x_1, ..., x_n]$ erzeugten Ideal

$$I = (f_1, ..., f_r) \subset R$$

ab: Ist $f_1(p) = 0, ..., f_r(p) = 0$, dann

$$\left(\sum_{i=1}^{r} s_i \cdot f_i\right)(p) = \sum_{i=1}^{r} s_i(p) f_i(p) = 0$$

für alle $s_i \in R$.

Ideale und Varietäten

Die affine Varietät $V(f_1, ..., f_r)$ hängt nur von dem von $f_1, ..., f_r \in R = K[x_1, ..., x_n]$ erzeugten Ideal

$$I = (f_1, ..., f_r) \subset R$$

ab: Ist $f_1(p) = 0, ..., f_r(p) = 0$, dann

$$\left(\sum_{i=1}^{r} s_i \cdot f_i\right)(p) = \sum_{i=1}^{r} s_i(p) f_i(p) = 0$$

für alle $s_i \in R$. Deshalb definiert man für ein Ideal $I \subset R$

$$V(I) = \{p \in K^n \mid f(p) = 0 \ \forall f \in I\}$$

Ideale und Varietäten

Die affine Varietät $V(f_1, \dots, f_r)$ hängt nur von dem von $f_1, \dots, f_r \in R = K[x_1, \dots, x_n]$ erzeugten Ideal

$$I = (f_1, \dots, f_r) \subset R$$

ab: Ist $f_1(p) = 0, \dots, f_r(p) = 0$, dann

$$\left(\sum_{i=1}^{r} s_i \cdot f_i\right)(p) = \sum_{i=1}^{r} s_i(p)\, f_i(p) = 0$$

für alle $s_i \in R$. Deshalb definiert man für ein Ideal $I \subset R$

$$V(I) = \{p \in K^n \mid f(p) = 0 \ \forall f \in I\}$$

Dies ist eine affine Varietät: Ein Ring heißt **noethersch**, wenn jedes Ideal endlich erzeugt ist.

Theorem (Hilberts Basissatz)

Sei R ein noetherscher Ring, dann ist $R[x]$ ebenfalls noethersch.

Ideale und Varietäten

Eine Varietät $V(I) \subset K^n$ heißt **irreduzibel**, wenn sie keine nicht-triviale Zerlegung

$$V(I) = V(J_1) \cup V(J_2)$$

hat.

Ideale und Varietäten

Eine Varietät $V(I) \subset K^n$ heißt **irreduzibel**, wenn sie keine nicht-triviale Zerlegung

$$V(I) = V(J_1) \cup V(J_2)$$

hat. Für eine Teilmenge $S \subset K^n$ definiere das **Verschwindungsideal**

$$I(S) = \{f \in R \mid f(p) = 0 \ \forall p \in S\}$$

Theorem

Damit ist

$$\{\mathit{Primideale\ von}\ R\} \quad \overset{V}{\underset{I}{\rightleftarrows}} \quad \{\mathit{irreduzible\ affine\ Var.\ in}\ K^n\}$$

eine $1:1-$*Korrespondenz.*

Projektion und Elimination

Der Gauß-Algorithmus parametrisiert die Lösungsmenge L eines linearen Gleichungssystems. Dies kann man als eine Projektion $L \longrightarrow K^r$ betrachten. Analog für nichtlineare Systeme:

Projektion und Elimination

Der Gauß-Algorithmus parametrisiert die Lösungsmenge L eines linearen Gleichungssystems. Dies kann man als eine Projektion $L \to K^r$ betrachten. Analog für nichtlineare Systeme:
Für ein Ideal $I \subset R = k[x_1, ..., x_n]$ betrachte das Eliminationsideal

$$I_m = I \cap k[x_{m+1}, ..., x_n]$$

und die Projektion

$$\begin{aligned} \pi_m : \quad & K^n \to K^{n-m} \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{aligned}$$

Projektion und Elimination

Der Gauß-Algorithmus parametrisiert die Lösungsmenge L eines linearen Gleichungssystems. Dies kann man als eine Projektion $L \to K^r$ betrachten. Analog für nichtlineare Systeme:
Für ein Ideal $I \subset R = k[x_1, ..., x_n]$ betrachte das Eliminationsideal

$$I_m = I \cap k[x_{m+1}, ..., x_n]$$

und die Projektion

$$\begin{aligned} \pi_m : \quad & K^n \to K^{n-m} \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{aligned}$$

Theorem

$$\overline{\pi_m(V(I))} = V(I_m)$$

Projektion und Elimination

Der Gauß-Algorithmus parametrisiert die Lösungsmenge L eines linearen Gleichungssystems. Dies kann man als eine Projektion $L \to K^r$ betrachten. Analog für nichtlineare Systeme:
Für ein Ideal $I \subset R = k[x_1, ..., x_n]$ betrachte das Eliminationsideal

$$I_m = I \cap k[x_{m+1}, ..., x_n]$$

und die Projektion

$$\begin{aligned} \pi_m : \quad & K^n \to K^{n-m} \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{aligned}$$

Theorem

$$\overline{\pi_m(V(I))} = V(I_m)$$

Zur Berechnung von I_m:

Division mit Rest

Für ein Ideal $I = (f_1, ..., f_r)$ in dem Hauptidealring $K[x]$ liefert der Euklidische Algorithmus den Erzeuger $I = (\mathrm{ggT}(f_1, ..., f_r))$. Wir können mit Division mit Rest testen, ob $f \in K[x]$ in I liegt.

Division mit Rest

Für ein Ideal $I = (f_1, ..., f_r)$ in dem Hauptidealring $K[x]$ liefert der Euklidische Algorithmus den Erzeuger $I = (\mathrm{ggT}(f_1, ..., f_r))$. Wir können mit Division mit Rest testen, ob $f \in K[x]$ in I liegt.
Für $f \in K[x_1, ..., x_n]$ muss man einen Leitterm $\mathrm{in}(f)$ auswählen, z.B. indem man die Variablen **lexikographisch** ordnet $x_1 > ... > x_n$.

Division mit Rest

Für ein Ideal $I = (f_1, ..., f_r)$ in dem Hauptidealring $K[x]$ liefert der Euklidische Algorithmus den Erzeuger $I = (\mathrm{ggT}(f_1, ..., f_r))$. Wir können mit Division mit Rest testen, ob $f \in K[x]$ in I liegt.
Für $f \in K[x_1, ..., x_n]$ muss man einen Leitterm in (f) auswählen, z.B. indem man die Variablen **lexikographisch** ordnet $x_1 > ... > x_n$.

Wir teilen $x^2y + xy^2 + y^2$ durch $xy - 1$ und $y^2 - 1$ bzgl. $x > y$:

$$
\begin{array}{l}
x^2y + xy^2 + y^2 = \quad x(xy-1) + y(xy-1) + x + 1\left(y^2-1\right) + y + 1 \\
x^2y - x \\
\hline
xy^2 + x + y^2 \\
xy^2 - y \\
\hline
x + y^2 + y \\
\hline
y^2 + y \\
y^2 - 1 \\
\hline
y + 1
\end{array}
$$

Gröbnerbasen

Teile $x^2 - y^2$ durch $x^2 + y$ und $xy + x$

$$\begin{array}{l} x^2 - y^2 = \quad 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y \\ \hline -y^2 - y \end{array}$$

Gröbnerbasen

Teile $x^2 - y^2$ durch $x^2 + y$ und $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

Seltsam, da

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

also $x^2 - y^2 \in \left(x^2 + y, xy + x\right)$, aber Rest nicht 0.

Teile $x^2 - y^2$ durch $x^2 + y$ und $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

Seltsam, da

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

also $x^2 - y^2 \in \left(x^2 + y, xy + x\right)$, aber Rest nicht 0. Problem: Leitterme kürzen sich.

Gröbnerbasen

Teile $x^2 - y^2$ durch $x^2 + y$ und $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

Seltsam, da

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

also $x^2 - y^2 \in \left(x^2 + y, xy + x\right)$, aber Rest nicht 0. Problem: Leitterme kürzen sich.

Lösung: Nehme zu den Divisoren alle Polynome, die man durch Kürzen von Leittermen erhält. Das ist die Notation einer **Gröbnerbasis.**

Gröbnerbasen

Teile $x^2 - y^2$ durch $x^2 + y$ und $xy + x$

$$\begin{array}{l}
x^2 - y^2 = \quad 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\
\underline{x^2 + y \qquad\quad} \\
-y^2 - y
\end{array}$$

Seltsam, da

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

also $x^2 - y^2 \in \left(x^2 + y, xy + x\right)$, aber Rest nicht 0. Problem: Leitterme kürzen sich.

Lösung: Nehme zu den Divisoren alle Polynome, die man durch Kürzen von Leittermen erhält. Das ist die Notation einer **Gröbnerbasis.**

Gröbnerbasis oben:

$$G = \left\{y^2 + y, x^2 + y, xy + x\right\}$$

Theorem

Ist $G = \{g_1, ..., g_r\}$ *eine lexikographische Gröbnerbasis von* $I \subset k[x_1, ..., x_n]$, *dann ist*

$$G_m = G \cap k[x_{m+1}, ..., x_n]$$

eine lexikographische Gröbnerbasis von $I_m \subset k[x_{m+1}, ..., x_n]$.

Gröbnerbasen und Projektion

Theorem

Ist $G = \{g_1, ..., g_r\}$ *eine lexikographische Gröbnerbasis von* $I \subset k[x_1, ..., x_n]$, *dann ist*

$$G_m = G \cap k[x_{m+1}, ..., x_n]$$

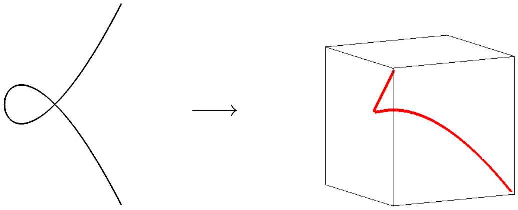
eine lexikographische Gröbnerbasis von $I_m \subset k[x_{m+1}, ..., x_n]$.

Damit kann man auch das Bild von $V(I)$ unter einer rationalen Abbildung $\varphi = (\varphi_1, ..., \varphi_r)$ mit $\varphi_i \in k(x_1, ..., x_n)$ durch Projektion des Graphen beschreiben.

$$\begin{tikzcd} & \Gamma(\varphi) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ V(I) \arrow[rr] & & K^r \end{tikzcd} \qquad = \{(x, \varphi(x)) \mid x \in V(I)\} \subset K^n \times K^r$$

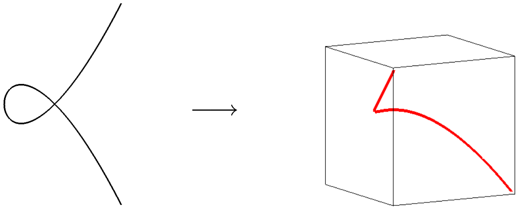
Der ganze Abschluss und Integralbasen

Wie findet man eine (fast überall) bijektive Abbildung einer singulären Kurve $C = V(I)$ auf eine glatte Kurve?



Der ganze Abschluss und Integralbasen

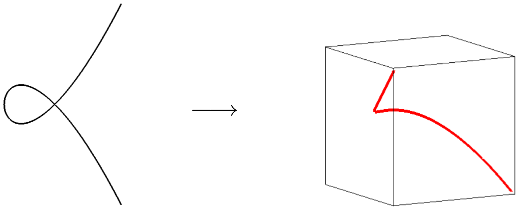
Wie findet man eine (fast überall) bijektive Abbildung einer singulären Kurve $C = V(I)$ auf eine glatte Kurve?



Berechne für $A = K[x, y] / I$ den ganzen Abschluss $A \subset \overline{A} \subset Q(A)$.

Der ganze Abschluss und Integralbasen

Wie findet man eine (fast überall) bijektive Abbildung einer singulären Kurve $C = V(I)$ auf eine glatte Kurve?

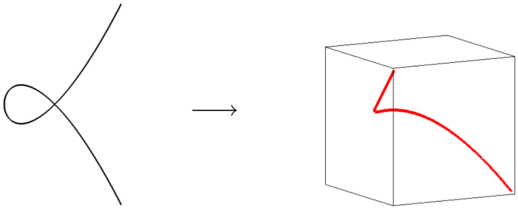


Berechne für $A = K[x,y]/I$ den ganzen Abschluss $A \subset \overline{A} \subset Q(A)$.
Beispiel: Für $I = (x^3 + x^2 - y^2)$ ist eine Darstellung von $\overline{A}$ als A-Modul

$$\overline{A} = \left\langle 1, \frac{y}{x} \right\rangle_A$$

Der ganze Abschluss und Integralbasen

Wie findet man eine (fast überall) bijektive Abbildung einer singulären Kurve $C = V(I)$ auf eine glatte Kurve?



Berechne für $A = K[x, y]/I$ den ganzen Abschluss $A \subset \overline{A} \subset Q(A)$.
Beispiel: Für $I = (x^3 + x^2 - y^2)$ ist eine Darstellung von $\overline{A}$ als A-Modul

$$\overline{A} = \left\langle 1, \frac{y}{x} \right\rangle_A$$

B., Decker, Laplagne, Seelisch: Computing integral bases via localization.
" A new algorithm for computing the adjoint ideal.

Abbildung auf eine nicht-singuläre Kurve

$$C = V\left(x^3 + x^2 - y^2\right) \xrightarrow{\varphi} K^1,\ (x,y) \mapsto t = \frac{y}{x}$$

mit Graph

$$I\left(\Gamma\left(\varphi\right)\right) = (x^3 + x^2 - y^2,\ x \cdot t - y,\ \overbrace{w \cdot x - 1}^{\Rightarrow x \neq 0}) \subset K\left[w, x, y, t\right]$$

Abbildung auf eine nicht-singuläre Kurve

$$C = V\left(x^3 + x^2 - y^2\right) \xrightarrow{\varphi} K^1, \; (x, y) \mapsto t = \frac{y}{x}$$

mit Graph

$$I\left(\Gamma\left(\varphi\right)\right) = \left(x^3 + x^2 - y^2, \; x \cdot t - y, \; \overset{\Rightarrow x \neq 0}{w \cdot x - 1}\right) \subset K\left[w, x, y, t\right]$$

Elimination mit $w > x > y > t$:

$x^3 + x^2 - y^2$		w		
$xt - y$	$-w$		wy	$-wt$
$wx - 1$	t	$x^2 - x$		1
$-wy + t$	1		xt	t
$-wy^2 + x^2 + x$		1	-1	
$-x^2 + xt^2 - x$			1	w
$-x + t^2 - 1$				1
$\vdots$				

Abbildung auf eine nicht-singuläre Kurve

$$C = V\left(x^3 + x^2 - y^2\right) \xrightarrow{\varphi} K^1,\ (x, y) \mapsto t = \frac{y}{x}$$

mit Graph

$$I\left(\Gamma\left(\varphi\right)\right) = (x^3 + x^2 - y^2,\ x \cdot t - y,\ \overset{\Rightarrow x \neq 0}{w \cdot x - 1}) \subset K\left[w, x, y, t\right]$$

Elimination mit $w > x > y > t$:

$x^3 + x^2 - y^2$		w		
$xt - y$	$-w$		wy	$-wt$
$wx - 1$	t	$x^2 - x$		1
$-wy + t$	1		xt	t
$-wy^2 + x^2 + x$		1	-1	
$-x^2 + xt^2 - x$			1	w
$-x + t^2 - 1$				1
$\vdots$				

$$K^1 \xrightarrow{\varphi^{-1}} C$$
$$t \mapsto \left(t^2 - 1, t^3 - t\right)$$

Abbildung auf eine Gerade

(Loading node.gif)

Abbildung auf eine Gerade

$C = V\left(x^4 - y^2 + x^5\right)$ und $t = \frac{y}{x^2}$

(Loading A3.gif)