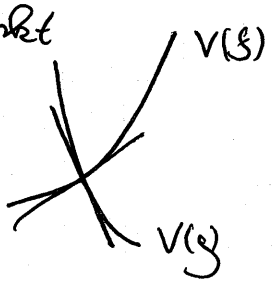
Bem: $i(f,g,0) = \infty$ gilt z.B wenn f und g einen gemeinsamen Faktor haben, der in 0 verschwindet

Übung (Satz) $f, g \in K[X,Y]$ von Multiplizität m und n in 0
Dann gilt
$$i(f,g,0) \geq \text{mult}_0 f \cdot \text{mult}_0 g$$
und Gleichheit gilt genau dann, wenn f und g in Nullpunkt keine gemeinsame Tangente haben
Im Fall $i(f,g,0) = 1$ folgt $V(f)$ und $V(g)$ sind glatt in 0 mit versch. Tangenten.
Man spricht in diesen Fall von einem transversalen Schnittpunkt



12.06.18 Im Kap 2 haben wir gesehen, dass wir mit Hilfe von ggT-Berechnung bzgl lex bzw. Produktordnung Variablen aus einem polynomialen Gleichungssystem eliminieren können.
Es gibt für diese Methode auch klassischere Methoden, die sich in gewisser Weise lesso verhalten.

Thm (Sylvester) Sei K Körper und
$$f = a_0 X^n + a_1 X^{n-1} + \dots + a_n$$
$$g = b_0 X^m + b_1 X^{m-1} + \dots + b_m$$
Polynome von Grad n bzw m in $K[X]$. f und g haben genau dann einen gemeinsamen Faktor, wenn die Sylvestermatrix

$$\text{syl}(f,g) = \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & & a_0 & b_{m-1} & & b_0 \\ a_n & \ddots & & b_m & \ddots & \\ & & a_n & & & b_m \end{pmatrix} \Bigg\} m+n$$

Determinante $R(S,g) = \det syl(S,g) = 0 \in K$ hat

Beweis: S und g haben einen gem. Faktor

äq zu $K[X]_{<m} \oplus K[X]_{<n} \xrightarrow{f}$

$(p, q) \longmapsto pS + qg$

hat einen nicht trivialen Kern.

äq zu $\deg(ggV(S,g)) < \deg(S,g)$

Denn: $(S,g) = (S_1 \cdot h, g_1 \cdot h)$ $\deg h > 0$

So $g_1 S_1 h = S_1 g_1 h = 0 \iff g_1 S - S_1 g = 0$

f ist K-linear und bzgl der Basis

$(X^{m-1}, 0) \dots (1,0), (0, X^{n-1}) \dots (0,1)$.

von $K[X]_{<m} \oplus K[X]_{<n}$ und der Basis $1, X, \dots, X^{n+m-1}$

von $K[X]_{<n+m-1}$ ist die Darstellungsmatrix gerade

$syl(S,g)$.

Bem: Die Sylvestermatrix macht Sinn für beliebige

Ringe R und $S, g \in R[X]$, insbesondere

$S, g \in \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m][X]$

$R(S,g) \in \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m]$

Für beliebige Ringe R erhalte die Resultante $R(S,g) \in R$

durch einsetzen der Koeff in die Resultante mit

Unbestimmten aus $\mathbb{Q}(Y)[X]$.

Im Gegensatz dazu vertauscht Einsetzen im allgemeinen nicht

mit ggT, gB Berechnungen

Übung: ZZ $R(S,g) \in (S,g) \subset \mathbb{Z}[a_0, \dots, b_0, \dots][X]$

Hinweis: Um eine Formel für die Koeff zu raten berechne

man die Koeff für feste n und m in

$\mathbb{Q}(a_0, \dots a_n, b_0, \dots b_m)[X]$

Kor: Sei $S, g \in K[X, Y]$ Polynome von Grad n und m

in X.

Es haben S und g genau dann einen gemeinsamen Faktor

in $K[X,Y] - K[Y]$, wenn

$R(S,g) = 0 \in K[Y]$

gilt.

Bew: Wir fassen f und g als Polynome $K(Y)[X]$ auf.
Dann gilt
$$R(f,g) = 0 \in K(Y)$$
gdw f, g haben gemeinsamen Faktor in $K(Y)[X]$
gdw (Gauß) f, g haben gem. Faktor in $K[Y,X] - K[Y]$

Kor
Es seien $f, g \in K[X,Y]$ zwei Polynome ohne gemeinsamen Faktor
Dann ist $V(f,g) \subset \mathbb{A}^2$ endlich.
Bew: Sei $(a,b) \in V(f,g)$. Das bedeutet, dass die Polynome $f(X,b), g(X,b) \in \bar{K}[X]$, sofern sie nicht Null sind $(X-a)$ als gemeinsamen Faktor haben.
Also
$$R(f(X,b), g(X,b)) = 0 \Leftrightarrow R_X(f,g)(b) = 0$$
Also b ist eine Nullstelle von $R_X(f,g) \in K[Y]$
Nach Kor ist dies nicht das Nullpolynom.
Also kommen für b nur endlich viele Werte in Frage kommen.
Genauso ist $R_Y(f,g) \in K[X]$ nicht das Nullpolynom und a ist eine Nullstelle dieses Polynoms
Insgesamt können nur endl. viele (a,b) als Punkte von $V(f,g)$ in Frage kommen. ☐

Betrachte $m = (X_1, \dots, X_n) \subset K[X_1, \dots, X_n] \subset K(X_1, \dots, X_n) \subset K((X_1, \dots, X_n))$
Der Divisionssatz terminiert nicht, $\mathcal{O}_{\mathbb{A}^n,0}$ $\mathcal{O}_{\mathbb{A}^n,0}$
konvergiert aber in $K((X_1, \dots, X_n))$.
z.B. $X = f_1$, $f_1 = 1 - X$ und $1 > X_1 >$ lokal
$X^{(0)} = X$, $X^{(1)} = X - X(1-X) = X^2$ $\frac{X}{1-X} = \sum_{k=0}^{\infty} X^{k+1}$
$X^{(2)} = X^2 - X^2(1-X) = X^3$ usw.
Andererseits ist $a = 1 - X \in \mathcal{O}_{\mathbb{A}^n,0}$ eine Einheit
und
$$X = \frac{X}{1-X}(1-X)$$ macht Sinn in $\mathcal{O}_{\mathbb{A}^n,0}$

Es wäre schön, wenn wir zu $f_1, \dots, f_r \in \mathcal{O}_{\mathbb{A}^n,0}$, $g \in \mathcal{O}_{\mathbb{A}^n,0}$ eine Darstellung

$$g = g_1 f_1 + \dots + g_r f_r + h$$

mit $g_i \in \mathcal{O}_{\mathbb{A}^n,0}$, $h \in \mathcal{O}_{\mathbb{A}^n,0}$ finden könnten mit den entsprechenden Leitterm Bedingungen
Das ist möglich, wenn wir Bed (2a), (2b) abschwächen.
Da wir uns für Ideal-membership nur interessieren können wir mit Einheiten durch multiplizieren und $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ annehmen

Satz (Mora)

Es seien $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ > eine Monomordnung
(In Anwendungen meist lokal).
Für jedes $g \in K[x_1, \dots, x_n]$ ex $g_1, \dots, g_r \in K[x_1, \dots, x_n]$
$u \in K[x_1, \dots, x_n]$ mit $u(0) \neq 0$ und $h \in K[x_1, \dots, x_n]$, sodass

(1) $u \cdot g = g_1 f_1 + \dots + g_r f_r + h$

(2a') $in_>(ug) \geq in_>(g_i f_i)$, sofern ug und $g_i f_i \neq 0$

(2b') Falls h nicht Null ist, ist $in(h)$ durch kein $in(f_i)$ teilbar.

Moras Algorithmus:

Input: > Monomordnung $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ $g \in K[x_1, \dots, x_n]$

Output: Mora Darstellung für g mit Rest h

1. Setze $h = g$ und $D = \{f_1, \dots, f_r\}$
2. while ($h \neq 0$ and $D_h := \{f \in D \mid in(h)$ wird von $in(f)$ geteilt $\} \neq \emptyset$)
   - do
     - Wähle $f \in D_h$ mit $e.card(f) = deg f - deg\, in(f)$ minimal aus.
     - Wenn $ecart(f) > ecart(h)$, dann $D = D \cup \{h\}$
     - Setze $h = h - \frac{in(h)}{in(f)} \cdot f$
3. Return h.

(genauere Buchführung gibt auch u und g_1, g_r)
Der Schlüssel für den Algorithmus ist

$$ecart(S) = deg(S) - deg(in\, S) \geq 0$$

da Ecart von S und gewisse h's die im Algorithmus auftauchen ebenfalls zu teilen.
Ein Austausch (1) mit (2a') (2b') wie im Satz nennt man eine Mora Standarddarstellung von g bzgl $S_1, \dots, S_r$ und $>$

Bem: Sind $S_1, \dots, S_r$ und g homogen, dann ist der $ecart(h) = 0$ und unsere Menge von Paaren D wird nicht größer.
In jedem Schritt verkleinern wir den Leitterm $in(h)$ und da es nur endlich viele Monome von Grad $deg(g)$ gibt, terminiert der Algorithmus.

Beweis:
Terminierung: Wir gehen in zwei Schritten vor.
Im ersten Schritt zeigen wir, dass die Menge D der Teiler nur endlich oft vergrößert wird.
Anschließend homogenisieren wir die Situation mit Hilfe einer zusätzlichen Variable und argumentieren mit der obigen Berechnung.
Wir bezeichnen mit h_k und D_k die Werte von h und D nach k Iterationen.
Wir starten mit $h_0 = g$ und $D_0 = \{S_1, \dots, S_r\}$
Der Algorithmus wird fortgeführt, wenn

$$0 \neq in(h_k) \in (in(S) \mid S \in D_k)$$

Im diesem Fall nehme h_{k+1} zu D_k hinzu, falls $x_0^{ecart(h_k)} in(h_k)$ kein Element von

$$I_k = (x_0^{ecart(S)} in(S) \mid S \in D_k) \subset K[x_0, \dots, x_n]$$

Nach Gordans Lemma wird die Kette

$$I_0 \subset I_1 \subset \dots \subset I_k \subset K[x_0, \dots, x_n]$$

stationär, etwa $I_N = I_{N+1}$
Dann gilt auch $D_N = D_{N+1}$ usw,
etwa $D_N = \{S_1, \dots, S_r, \dots, S_{r'}\}$

Terminierung folgt, wenn wir zeigen können, dass nach endlich vielen weiteren Schritten $h = 0$ oder $\Omega_h = \emptyset$ gelt.
Wir homogenisieren h_{N+1} und die S_i mit der zusätzlichen Variable X_0:

$$H_{N+1} = X_0^{\deg h_{N+1}} h_{N+1}\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right)$$

$$F_i = X_0^{\deg S_i} S_i\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right) \in K[X_0, \dots, X_n]$$

Auf $K[X_0, \dots, X_n]$ betrachten wir folgende Monomordnung $>_g$

$$X_0^c X^\alpha >_g X_0^d X^\beta \iff \deg(X_0^c X^\alpha) > \deg(X_0^d X^\beta)$$
$$\text{oder } \deg(X_0^c X^\alpha) = \deg(X_0^d X^\beta) \text{ und } X^\alpha > X^\beta$$

Das ist eine globale Monomordnung

$$in_{>_g}(f_i) = X_0^{ecart(S_i)}\, in(S_i)$$

Also wenn wir h_{N+1} durch die S_i dividieren folgen wir Maras Algorithmus für homogene Polynome H_{N+1}, f_i bzgl. globaler Monomordnung, welcher terminiert.