Kapitel I. Einführung

§1. Polynome

Def. 1.1: (naive Def.) K Körper, $n \in \mathbb{N}$

Ein Polynom in n Variablen $X_1, \dots, X_n$ über K ist ein „formaler Ausdruck"

$$f = \sum_{i=(i_1,\dots,i_n) \in \mathbb{N}_0^n} a_i X_1^{i_1} \cdots X_n^{i_n}, \quad a_i \in K$$

mit $a_i = 0$ für fast alle $i \in \mathbb{N}_0^n$.

Die Menge aller Polynome über K in den Variablen $X_1, \dots, X_n$ wird mit $K[X_1, \dots, X_n]$ bezeichnet.

Anm: Ein Polynom ist ein „formaler Ausdruck", d.h. nichts weiter als die Familie seiner Koeffizienten, d.h. eine Abb. $f: \mathbb{N}_0^n \to K$ mit $f(i) = 0$ für fast alle $i \in \mathbb{N}_0^n$.

Bsp. 1.2: $f = \frac{4}{5} X Z^2 - \frac{1}{2} X^2 Y^3 \in \mathbb{Q}[X, Y, Z]$

Def. 1.3: K Körper, $n \in \mathbb{N}$

Ein Monom ist ein Polynom der Form

$$X_1^{i_1} \cdots X_n^{i_n}$$

mit $i_1, \dots, i_n \in \mathbb{N}_0$. Sei $i = (i_1, \dots, i_n) \in \mathbb{N}_0^n$

Kurzschreibweise: $X^i := X_1^{i_1} \cdots X_n^{i_n}$

$|i| := i_1 + \dots + i_n$ heißt der Totalgrad des Monoms X^i.

Bsp. 1.4: $X Y^2 Z^3 \in \mathbb{Q}[X, Y, Z]$ ist ein Monom vom Totalgrad $1+2+3 = 6$

Def. 1.5: Sei $f = \sum_{i \in \mathbb{N}_0^n} a_i X^i \in k[X_1, \dots, X_n]$

a_i heißt der Koeffizient des Monoms X^i.

Falls $a_i \neq 0$, dann heißt $a_i X^i$ ein Term von f

Falls $f \neq 0$, heißt $\deg f := \max_{i \in \mathbb{N}_0^n} \{ |i| \mid a_i \neq 0 \}$ der Totalgrad von f

Bsp. 1.6: $f = \frac{4}{5} XZ^2 - \frac{1}{2} X^2 Y^3 \in \mathbb{Q}[X,Y,Z]$ hat zwei Terme, nämlich $\frac{4}{5} XZ^2$ (Totalgrad 3) und $-\frac{1}{2} X^2 Z^3$ (Totalgrad 5). Der Totalgrad von f ist 5.

Bsp. 1.7: $f = 4XY^2Z^3 - \frac{1}{2} X^3 Z^3 + XYZ \in \mathbb{Q}[X,Y,Z]$ hat 3 Terme, Totalgrad 6;
f hat 2 Terme von Totalgrad 6

Def. 1.8: K Körper, $n \in \mathbb{N}$, $f = \sum_{i \in \mathbb{N}_0^n} a_i X^i$, $g = \sum_{i \in \mathbb{N}_0^n} b_i X^i \in K[X_1, \dots, X_n]$

Wir setzen

$$f+g := \sum_{i \in \mathbb{N}_0^n} (a_i + b_i) X^i, \quad f \cdot g := \sum_{k \in \mathbb{N}_0^n} \Big(\sum_{\substack{i,j \in \mathbb{N}_0^n \\ \text{mit } i+j=k}} a_i b_j \Big) X^k$$

Anm.: $+, \cdot$ sind wohldefiniert

- $K[X_1, \dots, X_n]$ ist ein kommutativer Ring bzgl. der oben def. Addition und Multiplikation und wird deshalb auch als Polynomring in den Variablen $X_1, \dots, X_n$ bezeichnet.

Def. 1.9: K Körper, $n \in \mathbb{N}$, $f, g \in K[X_1, \dots, X_n]$

$f \mid g \overset{\text{Def}}{\Leftrightarrow} \exists h \in K[X_1, \dots, X_n] : g = hf$ „f teilt g"

Bsp. 1.10: $K = \mathbb{Q}$, $X-1 \mid X^3-1$, denn $X^3-1 = (X-1)(X^2+X+1)$

Def. 1.11: K Körper, $n \in \mathbb{N}$, $f \in K[X_1, \dots, X_n]$ Polynom.
Dann induziert f eine Abbildung

$$f: K^n \to K, \quad (b_1, \dots, b_n) \mapsto \sum_{i=(i_1,\dots,i_n) \in \mathbb{N}_0^n} a_i b_1^{i_1} \cdots b_n^{i_n}$$

Bsp. 1.12: $K = \mathbb{F}_2$, $f = X^2 + X \in \mathbb{F}_2[X]$

Dann ist $f(0) = 0$, $f(1) = 1+1 = 0$

Also: $f \neq 0$, aber $f: \mathbb{F}_2 \to \mathbb{F}_2$ ist die Nullabbildung

Bem. 1.13: K Körper mit unendlich vielen Elementen, $n \in \mathbb{N}$, $f \in K[X_1, \dots, X_n]$.
Dann sind äquivalent:

(i) $f = 0$

(ii) $f: K^n \to K$ ist die Nullabbildung.

Bew.: (i) $\Rightarrow$ (ii) trivial

(ii) $\Rightarrow$ (i) Induktion nach Anzahl d. Variablen

$n=1$: Ist $f \in K[X]$, $f \neq 0$, $\deg(f) = m$

$\overset{\text{LA}}{\underset{\text{bzw. §4}}{\Rightarrow}}$ f hat höchstens m verschiedene Nullstellen

Nach Vor. ist $f(a)=0$ für unendlich viele $a \in K$.

$\Rightarrow f = 0$.

$n-1 \Rightarrow n$: Sei $f \in K[X_1, \dots, X_n]$ mit $f(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in K^n$

Wir schreiben f in der Form

$$f = \sum_{i=0}^{N} g_i X_n^i$$

mit $g_i \in K[X_1, \dots, X_{n-1}]$

zz.: $g_i = 0$ für $i = 0, \dots, N$ ($\Rightarrow$ Beh.)

Bew.: Sei $(a_1, \dots, a_{n-1}) \in K^{n-1}$

Dann ist $\tilde{f} := f(a_1, \dots, a_{n-1}, X_n) \in K[X_n]$, und es ist nach Vor. $\tilde{f}(a_n) = 0 \quad \forall a_n \in K$

$$\Rightarrow \tilde{f} = 0 \Rightarrow \sum_{i=0}^{N} g_i(a_1, \dots, a_{n-1}) X_n^i = 0 \Rightarrow g_i(a_1, \dots, a_{n-1}) = 0$$

für $i = 0, \dots, N$

$(a_1, \dots, a_{n-1}) \in K^{n-1}$ beliebig war, folgt mit IV: $g_i = 0$ für $i = 0, \dots, N$ □

Folgerung 1.14: K Körper mit unendlich vielen Elementen, $n \in \mathbb{N}$, $f, g \in K[X_1, \dots, X_n]$. Dann sind äquivalent:

(i) $f = g$

(ii) $f: K^n \to K$, $g: K^n \to K$ sind dieselben Abbildungen

Bew.: (i) $\Rightarrow$ (ii) trivial

(ii) $\Rightarrow$ (i) Sind $f, g: K^n \to K$ dieselben Abbildungen, dann ist $f-g: K^n \to K$ die Nullabbildung $\overset{1.13}{\Rightarrow} f - g = 0 \Rightarrow f = g$. □

§2. Affine Varietäten

Def. 2.1: K Körper, $n \in \mathbb{N}$

K^n heißt der n-dimensionale affine Raum über K

K^1 heißt die affine Gerade, K^2 heißt die affine Ebene über K.

Def. 2.2: K Körper, $n \in \mathbb{N}$, $f_1, \dots, f_s \in K[X_1, \dots, X_n]$

$$V(f_1, \dots, f_s) \overset{\text{Def}}{=} \{(a_1, \dots, a_n) \in K^n \mid f_i(a_1, \dots, a_n) = 0 \text{ für } i = 1, \dots, s\}$$

$V(f_1, \dots, f_s)$ heißt die durch $f_1, \dots, f_s$ definierte affine Varietät.
Ist $V = V(f_1, \dots, f_s)$, dann nennt man $f_1 = 0, \dots, f_s = 0$ auch eine implizite Darstellung von V.

Bsp. 2.3: (a) $f = 0 \in K[X_1, \dots, X_n]$. Dann ist $V(f) = K^n$

(b) $f = X^2 + Y^2 + 1 \in \mathbb{R}[X, Y]$. Dann ist $V(f) = \emptyset$

(c) $f = X^2 + Y^2 - 1 \in \mathbb{R}[X, Y]$ $V(f)$: Einheitskreis

(d) $f = X^2 - Y^2 \in \mathbb{R}[X, Y]$ $V(f)$:

(e) $f = Z^2 - X^2 - Y^2 \in \mathbb{R}[X, Y, Z]$

(f) $f = X^2 - Y^2 Z^2 + Z^3 \in \mathbb{R}[X, Y, Z]$

Anm.: Bsp. 2.3 (e) und (f) liefern Beispiele für „singuläre Punkte"
(in (e) Spitze im Ursprung, in (f) Selbstdurchdringung entlang Y-Achse)

Damit werden wir uns später beschäftigen.

Bsp. 2.4: $f = Y - X$, $g = Z - Y \in \mathbb{R}[X, Y, Z]$

$$V(f, g) = \{(a_1, a_2, a_3) \in \mathbb{R}^3 \mid a_2 - a_1 = 0,\ a_3 - a_2 = 0\} = \{(a_1, a_2, a_3) \in \mathbb{R}^3 \mid a_1 = a_2 = a_3\}$$

$$= \{t(1, 1, 1) \mid t \in \mathbb{R}\}$$

Bsp. 2.5: $f_1 = a_{11} X_1 + \dots + a_{1n} X_n - b_1 \in k[X_1, \dots, X_n]$,

$\dots$, $f_m = a_{m1} X_1 + \dots + a_{mn} X_n - b_m \in k[X_1, \dots, X_n]$

Man nennt $V(f_1, \dots, f_m)$ eine lineare Varietät.

Aus LA bekannt: $V(f_1, \dots, f_m)$ ist ein affiner Unterraum des K^n der Dimension $n - \text{Rang}((a_{ij}))$. Für affine Varietäten brauchen wir noch einen geeigneten Dimensionsbegriff.

Bsp. 2.6: $f = Y - X^2 \in \mathbb{R}[X,Y,Z]$, $g = Z - X^3 \in \mathbb{R}[X,Y,Z]$

$V(f,g)$ ist eine Kurve im $\mathbb{R}^3$ („twisted cubic")

Bsp. 2.7: $f = XZ$, $g = YZ \in \mathbb{R}[X,Y,Z]$

$$V(f,g) = \{(x,y,z) \in \mathbb{R}^3 \mid xz = yz = 0\}$$
$$= \{(x,y,0) \mid x,y \in \mathbb{R}\} \cup \{(0,0,z) \mid z \in \mathbb{R} \setminus \{0\}\}$$

Anm.: Affine Varietäten tauchen an vielen Stelle in reiner u. angew. Mathematik auf, z.B.

- Extremwertbestimmung durch Lagrange-Multiplikatoren (vgl. Übung)
- Bahnbeschreibungen in Robotik

Bem. 2.8: K Körper, $n \in \mathbb{N}$, $f_1,\dots,f_s, g_1,\dots,g_t \in K[X_1,\dots,X_n]$,
$V = V(f_1,\dots,f_s)$, $W = V(g_1,\dots,g_t)$. Dann gilt:

(a) $V \cap W$ ist eine affine Varietät, nämlich

$$V \cap W = V(f_1,\dots,f_s,g_1,\dots,g_t)$$

(b) $V \cup W$ ist eine affine Varietät, nämlich

$$V \cup W = V(f_i g_j \mid i = 1,\dots,s,\ j = 1,\dots,t)$$

Beweis: (a) Sei $a \in K^n$. Dann gilt:

$$a \in V \cap W \Leftrightarrow f_1(a) = 0,\dots,f_s(a) = 0,\ g_1(a) = 0,\dots,g_t(a) = 0$$
$$\Leftrightarrow a \in V(f_1,\dots,f_s,g_1,\dots,g_t)$$

(b) „$\subset$" Sei $a \in V \Rightarrow f_1(a) = 0,\dots,f_s(a) = 0 \Rightarrow f_i(a)\,g_j(a) = 0 \quad \forall i = 1,\dots,s, j = 1,\dots,t$

$\Rightarrow a \in V(f_i g_j \mid i = 1,\dots,s,\ j = 1,\dots,t)$

Also: $V \subset V(f_i g_j \mid i = 1,\dots,s,\ j = 1,\dots,t)$

Analog: $W \subset V(f_i g_j) \Rightarrow V \cup W \subset V(f_i g_j)$

„$\supset$" Sei $a \in V(f_i g_j \mid i = 1,\dots,s,\ j = 1,\dots,t)$

Ann.: $a \notin V$. Dann ex. $i_0 \in \{1,\dots,s\}$ mit $f_{i_0}(a) \neq 0$

Wegen $f_{i_0} g_j(a) = 0$ für alle $j \in \{1,\dots,t\}$ folgt $g_j(a) = 0$ für alle $j \in \{1,\dots,t\}$

$\Rightarrow a \in V(g_1, \dots, g_t) = W$

$\Rightarrow$ „$\supset$"

Bsp. 2.9: siehe Bsp. 2.7: $V(XZ, YZ) \underset{2.8}{=} V(Z) \cup V(X,Y)$

Fragestellungen: Gegeben seien $f_1, \dots, f_s \in K[X_1, \dots, X_n]$. Wir wollen die folgenden Fragen studieren:

- Wie bestimmt man, ob $V(f_1, \dots, f_s) \neq \emptyset$ (d.h., ob $f_1 = f_2 = \dots = f_s = 0$ gemeinsame Lösungen besitzen)? „Konsistenz"
- Wie bestimmt man, ob $V(f_1, \dots, f_s)$ endlich? (Falls endlich, wie bestimmt man die Lösungen explizit?) „Endlichkeit"

Bem.+Def. 2.10: K Körper, $R = K[X_1, \dots, X_n]$. Dann gilt:

Auf $R \times R \setminus \{0\}$ wird durch

$$(f,g) \sim (f',g') \overset{\text{Def}}{\Leftrightarrow} fg' = f'g$$

eine Äquivalenzrelation definiert.

Für die Äquivalenzklasse von (f,g) schreiben wir $\frac{f}{g}$.

Die Menge d. Äquivalenzklassen wird mit $K(X_1, \dots, X_n)$ bezeichnet und heißt die Menge der rationalen Funktionen in $X_1, \dots, X_n$ über K.

Bew.: $\sim$ ist reflexiv: Wegen $fg = fg$ ist $(f,g) \sim (f,g)$ für $f, g \in R, g \neq 0$.

$\sim$ ist symmetrisch: Seien $f, f', g, g' \in R, g, g' \neq 0$ mit $(f,g) \sim (f',g')$

$\Rightarrow fg' = f'g \Rightarrow f'g = fg' \Rightarrow (f',g') \sim (f,g)$

$\sim$ ist transitiv: Sei $(f,g) \sim (f',g')$, $(f',g') \sim (f'',g'')$

$\Rightarrow fg' = f'g$, $f'g'' = f''g' \Rightarrow f'fg'' = ff'g'' = ff''g'$

$= f''fg' = f''f'g = f'f''g$

$\Rightarrow f'(fg'' - f''g) = 0 \Rightarrow fg'' - f''g = 0 \Rightarrow (f,g) \sim (f'',g'')$.

$\downarrow$

$0 \neq f' \neq 0$. □

Bem. 2.11: K Körper. Dann gilt:

$K(X_1,\dots,X_n)$ ist ein Körper bzgl. der wie folgt definierten Verknüpfungen:

$$\frac{f_1}{g_1}+\frac{f_2}{g_2}:=\frac{f_1g_2+f_2g_1}{g_1g_2}\quad,\quad \frac{f_1}{g_1}\cdot\frac{f_2}{g_2}:=\frac{f_1f_2}{g_1g_2}$$

Bew.: Man zeigt zunächst daß die Verknüpfungen wohldefiniert sind:

Für „+": Sei $(f_1,g_1)\sim(f_1',g_1'),\ (f_2,g_2)$

$$\Rightarrow (f_1g_2+f_2g_1)g_1'g_2' = f_1g_2g_1'g_2' = f_1'g_2g_1g_2' = (f_1'g_2'+f$$

$$\Rightarrow (f_1g_2+f_2g_1,g_1g_2)\sim(f_1'g_2'+f_2'$$

Einsetzen in rat. Fkt. nicht verträglich mit „$\sim$" aus Def von $k(X)$!

-wahl

Analog für „·".

Die Körperaxiome sind leicht nachzurechne

□

Def. 2.12: K Körper, $V\subset K^n$ affine Varietät.

Eine rationale Parameterdarstellung von V ist ein n-Tupel $(r_1,\dots,r_n)\in(K(t_1,\dots,t_m))^n$, sd. gilt:

(a) $(r_1(a_1,\dots,a_m),\dots,r_n(a_1,\dots,a_m))\in V$ für alle $(a_1,\dots,a_m)\in K^m$, für die die $r_i(a_1,\dots,a_m)$ wohldef. sind

(b) V ist die kleinste Varietät, die alle diese Punkte enthält, d.h.:

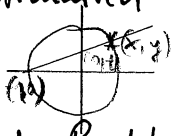
Ist $W\subset K^n$ eine affine Varietät mit $(r_1(a_1,\dots,a_m),\dots,r_n(a_1,\dots,a_m))\in W$ für alle $(a_1,\dots,a_m)\in K^m$, dann ist $V\subset W$.

Sind $r_1,\dots,r_n\in K[t_1,\dots,t_m]$, spricht man auch von einer polynomialen Parameterdarstellung.

Bsp. 2.13: Sei $V=V(X^2+Y^2-1)\subset\mathbb{R}^2$ (Einheitskreis)

Wir konstruieren eine rationale Parameterdarstellung von V

Idee: Jede nicht vertikale Gerade durch $(-1,0)$ trifft die y-Achse in einem Punkt $(0,t)$ und den Kreis in einem eind. bestimmten Punkt (x,y)



Variiert man t von $-\infty$ bis $+\infty$ auf der y-Achse, so wird jeden Punkt auf dem Kreis außer $(-1,0)$ getroffen.

Explizit: Sei $(x,y) \in (-1,0) \vee (0,t)$, $(x,y) \neq (-1,0)$

$$\Rightarrow \frac{t-0}{0-(-1)} = \frac{y-0}{x-(-1)} \Rightarrow t = \frac{y}{x+1} \Rightarrow y = t(x+1)$$

Dann gilt: $(x,y) \in V \Leftrightarrow x^2 + t^2(x+1)^2 = 1 \Leftrightarrow x^2 - 1 + t^2(x+1)^2 = 0$

$$\Leftrightarrow (x+1)\big((x-1) + t^2(x+1)\big) = 0 \Leftrightarrow (x+1)\big((1+t^2)x - (1-t^2)\big) = 0$$

$$\overset{(x,y)\neq(-1,0)}{\Leftrightarrow} x = \frac{1-t^2}{1+t^2}, \quad y = t(x+1) = \frac{2t}{1+t^2}$$

Setze $r_1 := \frac{1-t^2}{1+t^2}$, $r_2 := \frac{2t}{1+t^2} \in \mathbb{R}(t)$

Es ist $\{(r_1(a), r_2(a)) \mid a \in \mathbb{R}\} = V \setminus \{(-1,0)\}$

$V \setminus \{(1,0)\}$ ist selbst keine affine Varietät, denn:

Wäre $V \setminus \{(1,0)\} = V(g_1, \dots, g_k)$ für $g_1, \dots, g_k \in \mathbb{R}[X,Y]$,

und fassen wir $g_1, \dots, g_k$ als stetige Funktionen $\mathbb{R}^2 \to \mathbb{R}$ auf,

dann wäre $V \setminus \{(1,0)\} = V(g_1) \cap \dots \cap V(g_k) = g_1^{-1}(\{0\}) \cap \dots \cap g_m^{-1}(\{0\})$

abg. in $\mathbb{R}^2$ ↯

Also ist V die kleinste affine Varietät, die alle Punkte der Form

$(r_1(a), r_2(a))$, $a \in \mathbb{R}$, enthält

Damit ist $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ eine rationale Parametrisierung von V

<u>Frage:</u> Existiert zu jeder affinen Varietät eine rationale Parameterdarstellung?
(Leider nein.)

<u>Bsp. 2.14:</u> Gegeben sei die Parameterdarstellung $(1+t, 1+t^2)$

Existiert eine affine Varietät, die man so rational parametrisieren kann?

Ist $x = 1+t$, $y = 1+t^2$, dann ist $t = x-1$, also

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

$$\rightarrow y - x^2 + 2x - 2 = 0$$

Ist umgekehrt $f = Y - X^2 + 2X - 2$, dann ist

$$V(f) = \{(x,y) \in K^2 \mid y - x^2 + 2x - 2 = 0\}$$
$$= \{(x,y) \in K^2 \mid y - 1 = (x-1)^2\}$$
$$\underset{x-1=t}{=} \{(1+t, 1+t^2) \mid t \in K\}$$

Also ist $(1+t, 1+t^2)$ eine polynomiale Parameterdarstellung von $V(f)$.

Frage: Es sei eine Parameterdarstellung einer affinen Varietät gegeben. Wie kann man eine implizite Darstellung für V finden (→ Eliminationstheorie)

§3. Ideale im Polynomring

Def. 3.1: K Körper, Eine Teilmenge $\mathfrak{I} \subset K[X_1, \dots, X_n]$ heißt Ideal, wenn die folgenden Bedingungen erfüllt sind:

(a) $0 \in \mathfrak{I}$

(b) $f, g \in \mathfrak{I} \Rightarrow f+g \in \mathfrak{I}$

(c) $f \in \mathfrak{I}$, $h \in K[X_1, \dots, X_n] \Rightarrow hf \in \mathfrak{I}$

Bsp. 3.2: (a) $\{0\} \subset K[X_1, \dots, X_n]$ ist ein Ideal

(b) $K[X_1, \dots, X_n] \subset K[X_1, \dots, X_n]$ ist ein Ideal

(c) $\mathfrak{I} := K[X] \subset K[X,Y]$ ist kein Ideal, denn: 3.1 (a), (b) sind zwar erfüllt, aber 3.1 (c) nicht: $X \in \mathfrak{I}$, $Y \in K[X,Y]$, aber $XY \notin \mathfrak{I}$

Bsp. 3.3: Sei $\mathfrak{I} = \{f \in \mathbb{R}[X,Y] \mid f((1,2)) = 0\}$

$\mathfrak{I}$ ist ein Ideal in $\mathbb{R}[X,Y]$, denn:

- $0 \in \mathfrak{I}$
- Sind $f, g \in \mathfrak{I}$, d.h. $f((1,2)) = 0$ und $g((1,2)) = 0$, dann ist $(f+g)((1,2)) = f((1,2)) + g((1,2)) = 0 + 0 = 0$, d.h. $f+g \in \mathfrak{I}$
- Ist $f \in \mathfrak{I}$, $h \in \mathbb{R}[X,Y]$, dann ist $(h \cdot f)((1,2)) = h(1,2) \cdot f(1,2) = h(1,2) \cdot 0 = 0$ $\Rightarrow hf \in \mathfrak{I}$.

Bem.+Def. 3.4: K Körper, $f_1,\dots,f_s \in K[X_1,\dots,X_n]$. Dann gilt:

$$\langle f_1,\dots,f_s\rangle \overset{\text{Def}}{=} \{h_1f_1+\dots+h_sf_s \mid h_1,\dots,h_s \in K[X_1,\dots,X_n]\}$$

ist ein Ideal in $K[X_1,\dots,X_n]$, heißt *das von $f_1,\dots,f_s$ erzeugte Ideal*.

Bew.: Sei $I=\langle f_1,\dots,f_s\rangle$

① $0\in I$, denn $0=0\cdot f_1+\dots+0\cdot f_s$

② Seien $f,g\in I$, etwa $f=p_1f_1+\dots+p_sf_s$, $g=q_1f_1+\dots+q_sf_s$

$\Rightarrow f+g=(p_1+q_1)f_1+\dots+(p_s+q_s)f_s\in I$

③ $f\in I$ wie in ②, $h\in K[X_1,\dots,X_n]$

$\Rightarrow hf=(hp_1)f_1+\dots+(hp_s)f_s\in I$. □

Anm.: Startet man mit einem polynomialen Gleichungssystem

$$f_1=0,\dots,f_s=0$$

und wählt man $h_1,\dots,h_s\in K[X_1,\dots,X_n]$ beliebig, dann gilt natürlich auch

$$h_1f_1+\dots+h_sf_s=0$$

Die linke Seite durchläuft alle Elemente von $\langle f_1,\dots,f_s\rangle$

Das Ideal $\langle f_1,\dots,f_s\rangle$ besteht also aus allen „polynomialen Konsequenten" der obigen Gleichungen.

Def. 3.5: K Körper, $I\subset K[X_1,\dots,X_n]$ Ideal

I heißt *endlich erzeugt* $\overset{\text{Def}}{\Leftrightarrow}$ Es existieren Polynome $f_1,\dots,f_s\in K[X_1,\dots,X_n]$, so daß $I=\langle f_1,\dots,f_s\rangle$

In diesem Fall heißt $f_1,\dots,f_s$ eine *Basis* von I.

Anm.: Wir werden später zeigen, daß jedes Ideal in $K[X_1,\dots,X_n]$ endlich erzeugt ist (Hilbertscher Basissatz)

Bsp. 3.6: Sei $I=\langle X,Y\rangle\subset\mathbb{R}[X,Y]$

Offenbar sind $X+Y=1\cdot X+1\cdot Y$, $X-Y=1\cdot X-1\cdot Y\in I$

$\Rightarrow \langle X+Y, X-Y\rangle \subset]$

Umgekehrt ist $X \in \langle X+Y, X-Y\rangle$, denn $X = \frac{1}{2}(X+Y) + \frac{1}{2}(X-Y)$,

$Y \in \langle X+Y, X-Y\rangle$, denn $Y = \frac{1}{2}(X+Y) - \frac{1}{2}(X-Y)$

$\Rightarrow] = \langle X, Y\rangle \subset \langle X+Y, X-Y\rangle$

$\Rightarrow \langle X, Y\rangle = \langle X+Y, X-Y\rangle = \langle X+Y, X-Y, X, Y\rangle$

Ein Ideal kann also viele verschiedene Basen haben, diese können auch von unterschiedlicher Kardinalität sein.

Bem. 3.7: K Körper, $f_1, \dots, f_s, g_1, \dots, g_t \in K[X_1, \dots, X_n]$ mit $\langle f_1, \dots, f_s\rangle = \langle g_1, \dots, g_t\rangle$.

Dann gilt: $V(f_1, \dots, f_s) = V(g_1, \dots, g_t)$

Bew.: „$\subset$" Sei $a \in V(f_1, \dots, f_s) \Rightarrow f_1(a) = \dots = f_s(a) = 0$

Wegen $g_i \in \langle f_1, \dots, f_s\rangle$ für $i = 1, \dots, t$ ist g_i von der Form

$$g_i = h_{i,1} f_1 + \dots + h_{i,s} f_s \quad \text{mit } h_{i,1}, \dots, h_{i,s} \in K[X_1, \dots, X_n]$$

$\Rightarrow g_i(a) = h_{i,1}(a) f_1(a) + \dots + h_{i,s}(a) f_s(a) = 0$ für alle $i = 1, \dots, t$

$\Rightarrow a \in V(g_1, \dots, g_t)$

„$\supset$" Durch analoges Argument mit f, g vertauscht.

Bsp. 3.8: $f = 2X^2 + 3Y^2 - 11$, $g = X^2 - Y^2 - 3 \in \mathbb{R}[X, Y]$. Was ist $V(f, g)$

Übung: $\langle f, g\rangle = \langle X^2 - 4, Y^2 - 1\rangle$

$\Rightarrow V(f, g) \underset{3.7}{=} V(X^2 - 4, Y^2 - 1) = \{(\pm 2, \pm 1)\}$

Also: Durch Übergang zu einen „schönen" Basis konnten wir die Varietät explizit bestimmen.

Frage: Gegeben sei eine Varietät $V = V(f_1, \dots, f_s) \subset K^n$.

Die Polynome $f_1, \dots, f_s$ (als Funktionen $K^n \to K$ betrachtet) sind auf V identisch Null. Welche Polynome außer $f_1, \dots, f_s$ verschwinden noch auf V?

Bem. + Def. 3.9: K Körper, $V \subset K^n$ affine Varietät. Dann gilt:

$$\mathcal{I}(V) := \{ f \in K[X_1, \dots, X_n] \mid f(a) = 0 \quad \forall a \in V \}$$

ist ein Ideal in $K[X_1, \dots, X_n]$.

$\mathcal{I}(V)$ heißt das Verschwindungs-Ideal von V.

Bew.: ① $0 \in \mathcal{I}(V)$ klar

② $f, g \in \mathcal{I}(V)$. Dann gilt für $a \in V$: $(f+g)(a) = f(a) + g(a) = 0 + 0 = 0$

Also ist $f + g \in \mathcal{I}(V)$.

③ Sei $f \in \mathcal{I}(V)$, $h \in K[X_1, \dots, X_n]$. Dann gilt für $a \in V$: $(hf)(a) = h(a) f(a) = 0$.

Bsp. 3.10: Sei $V = K^n (= V(0)$, vgl. Bsp. 2.3(a)$)$

Es ist $\mathcal{I}(V) = \mathcal{I}(K^n) = \{ f \in K[X_1, \dots, X_n] \mid f(a) = 0 \quad \forall a \in K^n \}$

Falls K unendlich viele Elemente hat, ist wg 1.14: $\mathcal{I}(K^n) = \{0\}$ $(= \mathcal{I}(V(0))$

Bsp. 3.11: Sei $V = V(X, Y) = \{(0,0)\} \subset K^2$.

Beh.: $\mathcal{I}(V) = \langle X, Y \rangle$

Bew.: „$\supset$" Sei $f \in \langle X, Y \rangle \Rightarrow f = h_1 X + h_2 Y$ mit $h_1, h_2 \in K[X, Y]$

$\Rightarrow f((0,0)) = h_1((0,0)) \cdot 0 + h_2((0,0)) \cdot 0 = 0$

„$\subset$" Sei $f = \sum_{i,j} a_{ij} X^i Y^j \in K[X, Y]$ mit $f((0,0)) = 0$

$\Rightarrow a_{00} = 0$

$$\Rightarrow f = \sum_{\substack{i,j \\ i>0}} (a_{ij} X^{i-1} Y^j) X + \sum_{j>0} (a_{0j} Y^{j-1}) Y \in \langle X, Y \rangle$$

Frage: Gegeben seien Polynome $f_1, \dots, f_s \in K[X_1, \dots, X_n]$.

Polynome	⟶	Varietät	⟶	Ideal
$f_1, \dots, f_s$		$V(f_1, \dots, f_s)$		$\mathcal{I}(V(f_1, \dots, f_s))$

Was ist der Zusammenhang zwischen $\langle f_1, \dots, f_s \rangle$ und $\mathcal{I}(V(f_1, \dots, f_s))$?
(Leider sind diese im allg. nicht gleich).

Bem. 3.12: K Körper, $f_1, \dots, f_s \in K[X_1, \dots, X_n]$. Dann gilt:

$$\langle f_1, \dots, f_s \rangle \subset \mathcal{J}(V(f_1, \dots, f_s))$$

Bew.: Sei $f \in \langle f_1, \dots, f_s \rangle \Rightarrow f = \sum_{i=1}^{s} h_i f_i$ für $h_1, \dots, h_s \in K[X_1, \dots, X_n]$

Sei $a \in V(f_1, \dots, f_s) \Rightarrow f(a) = \sum_{i=1}^{s} h_i(a) f_i(a) = 0 \Rightarrow f \in \mathcal{J}(V(f_1, \dots, f_s))$ □

Bsp. 3.13: Sei $f_1 = X^2, f_2 = Y^2 \in K[X, Y]$.

Es ist $V(f_1, f_2) = \{(0,0)\}$.

Wg. Bsp. 3.11 ist $\mathcal{J}(V) = \langle X, Y \rangle$

Aber: $\langle X^2, Y^2 \rangle \subsetneq \langle X, Y \rangle$, denn: $X \in \langle X, Y \rangle$, aber $X \notin \langle X^2, Y^2 \rangle$,

denn: Ist $f \in \langle X^2, Y^2 \rangle$, also $f = h_1 X^2 + h_2 Y^2$ mit $h_1, h_2 \in K[X, Y]$,

dann hat jeder Term in f mindestens Totalgrad 2.

Also: $\langle X^2, Y^2 \rangle \subsetneq \mathcal{J}(V(X^2, Y^2))$

Anm.: Auch wenn im allg. keine Gleichheit zwischen $\langle f_1, \dots, f_s \rangle$ und $\mathcal{J}(V(f_1, \dots, f_s))$ herrscht, gibt es doch im Fall $K = \mathbb{C}$ eine interessante Beziehung zwischen den Idealen (Hilbertscher Nullstellensatz)

Bem. 3.14: K Körper, $V, W \subset K^n$ affine Varietäten. Dann gilt,

(a) $V \subset W \Leftrightarrow \mathcal{J}(V) \supset \mathcal{J}(W)$

(b) $V = W \Leftrightarrow \mathcal{J}(V) = \mathcal{J}(W)$,

d.h. durch das Ideal einer Varietät ist diese eindeutig bestimmt.

Bew.: (a) „$\Rightarrow$" Sei $V \subset W, f \in \mathcal{J}(W) \Rightarrow f(a) = 0 \ \forall a \in W \Rightarrow f(a) = 0 \ \forall a \in V$

$\Rightarrow f \in \mathcal{J}(V)$

„$\Leftarrow$" Sei $\mathcal{J}(W) \subset \mathcal{J}(V)$, $W = V(g_1, \dots, g_t)$ mit $g_1, \dots, g_t \in K[X_1, \dots, X_n]$

$\underset{3.12}{\Rightarrow} \langle g_1, \dots, g_t \rangle \subset \mathcal{J}(V(g_1, \dots, g_t)) = \mathcal{J}(W) \subset \mathcal{J}(V)$, d.h. alle g_i verschw. auf V. Da $W = V(g_1, \dots, g_t)$, folgt $V \subset W$.

(b) aus (a). □

Fragen: • Ist jedes Ideal $I \subset K[X_1, \dots, X_n]$ endlich erzeugt?
(dh. kann es in der Form $I = \langle f_1, \dots f_s \rangle$ mit $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ geschrieben werden)

• Idealmitgliedschaft: Gegeben seien $f_1, \dots f_s \in K[X_1, \dots, X_n]$. Gibt es einen Algorithmus, der entscheidet, ob ein vorgegebenes $f \in K[X_1, \dots, X_n]$ in $\langle f_1, \dots f_s \rangle$ liegt?

• Nullstellensatz: Was ist der Zusammenhang zwischen $\langle f_1, \dots f_s \rangle$ und $I(V(f_1, \dots f_s))$?

§4. Polynome in einer Variablen

Def. 4.1: K Körper, $f = a_m X^m + a_{m-1} X^{m-1} + \dots + a_0 \in K[X]$, $a_m \neq 0$

$LT(f) := a_m X^m$ heißt Leitterm (oder führender Term) von f.

$LC(f) := a_m$ heißt Leitkoeffizient von f

f heißt normiert $\overset{\text{Def}}{\Leftrightarrow} LC(f) = 1$

Bem. 4.2: K Körper, $f, g \in K[X]$, $f, g \neq 0$. Dann gilt:

(a) $LT(fg) = LT(f)\,LT(g)$

(b) $\deg(fg) = \deg(f) + \deg(g)$

Bew.: klar.

Bsp. 4.3: $f = 5X^4 - 3X^2 + 7 \in \mathbb{Q}[X] \Rightarrow LT(f) = 5X^4$, $LC(f) = 5$

Bem. + Alg. 4.4: K Körper, $f, g \in K[X]$, $g \neq 0$. Dann gilt:
Es existieren eindeutig bestimmte $q, r \in K[X]$ mit

$$f = qg + r, \quad \deg(r) < \deg(g) \text{ oder } r = 0$$

Diese können mit folgendem Algorithmus bestimmt werden:

Eingabe: f, g

Algorithmus:

$q := 0$

$r := f$

WHILE $r \neq 0$ AND $\deg(g) \leq \deg(r)$ DO

$q := q + \frac{LT(r)}{LT(g)}$

$r := r - \frac{LT(r)}{LT(g)} g$

Ausgabe: $quot(f,g) = q$, $rest(f,g) = r$

Bew.: ① Wir zeigen zunächst, daß der Algorithmus terminiert.

Zu zeigen ist also, daß der Ausdruck $r \neq 0$ AND $\deg(g) \leq \deg(r)$ nach hinreichend vielen Schleifendurchläufen falsch wird.

Es sei $r \neq 0$ und $\deg(g) \leq \deg(r)$, etwa

$r = a_m X^m + \ldots + a_0$, $g = b_k X^k + \ldots + b_0$ mit $a_m, b_k \neq 0$, $m \geq k$

$$\Rightarrow r - \frac{LT(r)}{LT(g)} g = a_m X^m + \ldots + a_0 - \frac{a_m X^m}{b_k X^k} (b_k X^k + \ldots + b_0)$$

$$\Rightarrow \deg\left(r - \frac{LT(r)}{LT(g)} g\right) < \deg(r) \quad \text{oder} \quad r - \frac{LT(r)}{LT(g)} g = 0$$

Nach endlich vielen Schritten ist also $\deg(r) < \deg(g)$ oder $r = 0$.

② Der Algorithmus gibt q, r mit den gewünschten Eigenschaften aus ($\Rightarrow$ Existenz)

Setzt man $q := 0$, $r := f$, dann gilt $f = qg + r$

Ändert man q, r wie in obiger WHILE - DO - Schleife, so gilt

$$\left(q + \frac{LT(r)}{LT(g)}\right) g + \left(r - \frac{LT(r)}{LT(g)} g\right) = qg + r,$$

d.h. das Polynom $qg + r$ bleibt nach jedem Schleifendurchlauf erhalten.

Vor Ausführung der Schleife ist $qg + r = f$, d.h. nach Terminierung der Schleife gilt $f = qg + r$.

Wegen ① gilt nach Terminierung der Schleife ebenfalls $\deg(r) < \deg(g)$ oder $r = 0$.

③ Eindeutigkeit:

Seien $\tilde{q}, \tilde{r} \in K[X]$ mit $f = qg + r = \tilde{q}g + \tilde{r}$, $\deg(r) < \deg(g)$ oder $r=0$,

$\deg(\tilde{r}) < \deg(g)$ oder $\tilde{r}=0$

$\Rightarrow (q-\tilde{q})g = \tilde{r} - r$

Falls $\tilde{r} = r$, dann ist $(q-\tilde{q})g = 0$, also $q = \tilde{q}$.

Andernfalls: $\deg(q-\tilde{q}) + \deg(g) \overset{4.3}{=} \deg(\tilde{r}-r)$.

Nach Vor. ist aber $\deg(\tilde{r}-r) < \deg(g)$ ↯ □

Bsp. 4.5: (vor dem Beweis von 4.3) ↗ Vorlesungsmaterialien (pdf)

Folgerung 4.6: K Körper, $f \in K[X]$, $a \in K$ mit $f(a) = 0$. Dann gilt:

$$(X-a) \mid f$$

Bew.: Wg. 4.4 ex. $q, r \in K[X]$ mit

$f = q(X-a) + r$ und $\deg(r) < \deg(X-a) = 1$ (d.h. r ist Konstantenpol.) oder $r = 0$

Es ist $0 = f(a) = q(a)(a-a) + r(a) \Rightarrow r(a) = 0$

$\Rightarrow r = 0$

$\Rightarrow f = q(X-a)$ □

Folgerung 4.7: K Körper, $f \in K[X]$, $f \neq 0$. Dann gilt:

f hat höchstens $\deg(f)$ Nullstellen in K

Bew.: Bew. per Induktion nach $\deg(f)$

$\deg(f) = 0 \Rightarrow f$ konstant $\overset{f \neq 0}{\Rightarrow} f$ hat keine Nullstelle

Sei $f \in K[X]$ Polynom von Grad m, $a \in K$ mit $f(a) = 0$

$\overset{4.6}{\Rightarrow}$ Es ex. $g \in K[X]$ mit $f = (X-a)g$

Ist $b \in K$, $b \neq a$ mit $f(b) = 0$, dann ist $0 = f(b) = (b-a)g(b)$, also $g(b) = 0$

Es ist $\deg(g) = m-1$, nach IV hat g höchsten $m-1$ NS

$\Rightarrow f$ hat höchstens m NS. □

Folgerung 4.8: K Körper, $J \subset K[X]$ Ideal. Dann gilt:

(a) Es existiert ein $f \in K[X]$, sd. $J = \langle f \rangle$

(b) Falls $f \neq 0$: f ist eindeutig bis auf Multiplikation mit einem von Null verschiedenen Konstanten Polynom

Bew.: Falls $J = \{0\}$, dann ist $J = \langle 0 \rangle$.

Sei also im folgenden $J \neq 0$. Sei $f \neq 0$ ein Polynom von minimalem Grad aus J.

Beh.: $J = \langle f \rangle$

Bew.: „$\supset$" Wegen $f \in J$ folgt $\langle f \rangle \subset J$

„$\subset$" Sei $g \in J$. Dann ex. $q, r \in K[X]$ mit $g = qf + r$ und $\deg(r) < \deg(g)$ oder $r = 0$

J ist ein Ideal $\overset{f \in J}{\Rightarrow} qf \in J \Rightarrow g - qf = r \in J$

Falls $r \neq 0$, dann $\deg(r) < \deg(g)$ $\lightning$ zur Minimalität von f

Also $r = 0$, d.h. $g = qf \in \langle f \rangle$.

(b) Sei $\langle f \rangle = \langle g \rangle$, $f, g \neq 0$

Wegen $f \in \langle g \rangle$ folgt $f = hg$ für ein $h \in K[X]$, $h \neq 0$

$\Rightarrow \deg(f) = \deg(h) + \deg(g) \Rightarrow \deg(f) \geq \deg(g)$

Selbes Argument mit f, g vertauscht liefert $\deg(g) \geq \deg(f)$

Also $\deg(f) = \deg(g) \Rightarrow \deg(h) = 0 \Rightarrow h$ ist konstant

Anm: Ein Ideal d. Form $\langle f \rangle$ nennt man auch ein Hauptideal.

Jedes Ideal in $K[X]$ ist wg. 4.7 ein Hauptideal. Man sagt: $K[X]$ ist ein Hauptidealring

Bsp. 4.9: Sei $J = \langle X^3 - X + 1, X^2 + 1 \rangle \subset K[X]$

Dann ex. nach 4.8 ein $f \in K[X]$ mit $J = \langle f \rangle$. Wie findet man dieses?

Def. 4.10: K Körper, $f, g \in K[X]$. $h \in K[X]$ heißt ein <u>größter gemeinsamer Teiler</u> von f, g wenn gilt:

(a) $h \mid f$, $h \mid g$

(b) Ist $p \in K[X]$ mit $p \mid f$, $p \mid g$, dann gilt $p \mid h$.

Anm.: Obige Def. sagt nichts darüber aus, ob ein größter gemeinsamer Teiler tatsächlich existiert.

Bem.+Alg. 4.11: K Körper, $f,g \in K[X]$. Dann gilt:

(a) Es existiert ein größter gemeinsamer Teiler von f,g. Falls $(f,g) \neq (0,0)$, dann ist dieser eindeutig bestimmt bis auf Multiplikation mit einem Element $\neq 0$ aus K. Insbesondere gibt es genau einen größten gemeinsamen Teiler von f,g, der normiert ist. Dieser wird mit $ggT(f,g)$ bezeichnet. $ggT(0,0) := 0$.

(b) Ist h ein größter gemeinsamer Teiler von f,g, dann gilt:

$$\langle f,g \rangle = \langle h \rangle, \text{ insbesondere } \langle f,g \rangle = \langle ggT(f,g) \rangle.$$

Insbesondere existieren $A, B \in K[X]$, so daß

$$ggT(f,g) = Af + Bg.$$

(c) $ggT(f,g)$ kann mit dem Euklidischen Algorithmus bestimmt werden:

Eingabe: f,g

Algorithmus:

$h := f$
$s := g$
WHILE $s \neq 0$ DO
  $r := rest(h,s)$
  $h := s$
  $s := r$
IF $h \neq 0$ THEN $h := \frac{h}{LC(h)}$

Ausgabe: $ggT(f,g) = h$

Bew.: (a) Sei $J = \langle f,g \rangle$. Wegen 4.8 ein $h \in K[X]$ mit $\langle f,g \rangle = J = \langle h \rangle$

Beh.: h ist ein größter gemeinsamer Teiler von f,g

Bew.: (1) Wegen $f \in \langle h \rangle$ ex. $q \in K[X]$ mit $f = qh$, also $h \mid f$

Analog: $h \mid g$

② Sei $p \in K[X]$ mit $p \mid f, p \mid g$. Dann ex. $C, D \in K[X]$ mit $f = Cp$, $g = Dp$

Wegen $h \in \langle f, g \rangle$ ex. $A, B \in K[X]$ mit $Af + Bg = h$

$\Rightarrow h = Af + Bg = ACp + BDp = (AC + BD)p$

$\Rightarrow p \mid h$

$\Rightarrow$ Beh, sowie (b). Eindeutigkeit aus 4.8(b)

(c) Algorithmus terminiert: In jeder Schleifendurchführung nimmt der Grad von s ab, dh. s wird nach hinr. vielen Schleifendurchläufen 0.

Beh.: Ist $f = qg + r$ [illegible], dann ist

$$ggT(f, g) = ggT(f - qg, g) = ggT(r, g)$$

Bew.: Aufgrund von (b) genügt zz.: $\langle f, g \rangle = \langle f - qg, g \rangle$

Wegen $f = (f - qg) + qg, g \in \langle f - qg, g \rangle$ folgt $\langle f, g \rangle \subset \langle f - qg, g \rangle$

wegen $f - qg, g \in \langle f, g \rangle$ folgt „⊃"

Insbes. gilt nach jedem Schleifendurchlauf $ggT(f, g) = ggT(h, s)$

Nach Absolvierung der Schleife ist $s = 0$ und $ggT(h, 0) = \frac{h}{LC(h)}$ (falls $h \neq 0$) bzw. $= 0$, falls $h = 0$.

Bsp. 4.12: (vor dem Beweis von 4.11) ↗ Vorlesungsmaterialien (pdf)

Def. 4.13: K Körper, $f_1, \dots, f_s \in K[X]$,

$h \in K[X]$ heißt ein größter gemeinsamer Teiler von $f_1, \dots, f_s$, wenn gilt:

(a) $h \mid f_1, \dots, h \mid f_s$

(b) Ist $p \in K[X]$ mit $p \mid f_1, \dots, p \mid f_s$, dann gilt $p \mid h$.

Bem. 4.14: K Körper, $f_1, \dots, f_s \in K[X]$. Dann gilt:

(a) Es existiert ein größter gemeinsamer Teiler von $f_1, \dots, f_s$. Falls $(f_1, \dots, f_s) \neq (0, \dots, 0)$, dann ist dieser eindeutig bestimmt bis auf Multiplikation mit einem Element $\neq 0$ aus K

Insbesondere gibt es genau einen normierten größten gemeinsamen Teiler von $f_1, \dots, f_s$. Dieser wird mit $ggT(f_1, \dots, f_s)$ bezeichnet.

(b) Ist h ein größter gemeinsamer Teiler von $f_1,\dots,f_s$, dann gilt

$$\langle f_1,\dots,f_s\rangle = \langle h\rangle$$

Insbesondere ist also $\langle f_1,\dots,f_s\rangle = \langle ggT(f_1,\dots,f_s)\rangle$

(c) Für $s \geq 3$ gilt

$$ggT(f_1,\dots,f_s) = ggT(f_1, ggT(f_2,\dots,f_s))$$

Dies liefert auch den Algorithmus zur Bestimmung von $ggT(f_1,\dots,f_s)$

Bew.: (a),(b) analog zu 4.11 (a),(b)

(c) Sei $h = ggT(f_2,\dots,f_s)$

① Beh.: $\langle f_1, h\rangle = \langle f_1, f_2,\dots,f_s\rangle$

Bew.: „$\subset$" Es ist $f_1 \in \langle f_1,\dots,f_s\rangle$, $h = ggT(f_2,\dots,f_s) \in \langle f_2,\dots,f_s\rangle$

„$\supset$" Es ist $f_1 \in \langle f_1, h\rangle$

Sei $i \in \{2,\dots,n\}$. Dann ist $f_i \in \langle f_2,\dots,f_s\rangle = \langle h\rangle \subset \langle f_1, h\rangle$

② Wegen ① und (b) ist $\langle ggT(f_1,h)\rangle = \langle ggT(f_1,\dots,f_s)\rangle$

$\overset{4.8(b)}{\Rightarrow}$ $ggT(f_1,h) = ggT(f_1,\dots,f_s)$ (da beide normiert)

Bem. 4.15: Sei $J = \langle X^3-3X+2, X^4-1, X^6-1\rangle \subset \mathbb{Q}[X]$

Es ist $ggT(X^3-3X+2, X^4-1, X^6-1) = ggT(X^3-3X+2, ggT(X^4-1, X^6-1))$

$= ggT(X^3-3X+2, X^2-1) = X-1$

Also: $\langle X^3-3X+2, X^4-1, X^6-1\rangle = \langle X-1\rangle$

Ist $X^3+4X^2+3X-7 \in J$?

Das ist nach obigem äquivalent zu $X^3+4X^2+3X-7 \in \langle X-1\rangle$

Es ist $X^3+4X^2+3X-7 = (X^2+5X+8)(X-1)+1$

Also: $X^3+4X^2+3X-7 \notin J$

Algorithmus 4.16: (Idealmitgliedschaft in $K[X]$)

Eingabe: $f_1,\dots,f_s \in K[X]$, $g \in K[X]$

Algorithmus: $h := ggT(f_1,\dots,f_s)$

$r := rest(g,h)$

IF $r=0$ RETURN(WAHR) ELSE RETURN(FALSCH)

Ausgabe: WAHR, wenn $g \in \langle f_1,\dots,f_s\rangle$, FALSCH, wenn $g \notin \langle f_1,\dots,f_s\rangle$

Kapitel II. Gröbnerbasen

§5. Monomordnungen auf $K[X_1,\dots,X_n]$

Anm.: Der Divisionsalgorithmus in $K[X]$ beruht darauf, daß man den Begriff des „Leitterms" eines Polynoms hat.
Man kann die Monome eines Polynoms in einer Variablen nach ihrem Grad anordnen:

$$\dots > X^{m+1} > X^m > \dots > X^2 > X > 1$$

Will man diesen Divisionsalgorithmus auf $K[X_1,\dots,X_n]$ verallgemeinern, ist es zweckmäßig, eine Ordnungsrelation auf der Menge der Monome in $K[X_1,\dots,X_n]$ einzuführen.

Die Menge der Monome in $K[X_1,\dots,X_n]$ kann über die Abbildung $X_1^{\alpha_1}\cdots X_n^{\alpha_n} \mapsto (\alpha_1,\dots,\alpha_n)$ bijektiv auf die Menge $\mathbb{N}_0^n$ abgebildet werden. Wir werden im folgenden „Monomordnungen" auf $\mathbb{N}_0^n$ studieren. Diese sind verträglich mit der algebraischen Struktur des Polynomrings $K[X_1,\dots,X_n]$.

Def.5.1: Eine Monomordnung auf $K[X_1,\dots,X_n]$ ist eine Relation „$\geq$" auf $\mathbb{N}_0^n$ mit folgenden Eigenschaften:

(a) „$\geq$" ist eine Totalordnung, d.h.
- „$\geq$" ist reflexiv: $\forall \alpha\in\mathbb{N}_0^n : \alpha\geq\alpha$
- „$\geq$" ist antisymmetrisch: $\forall \alpha,\beta\in\mathbb{N}_0^n : (\alpha\geq\beta \text{ und } \beta\geq\alpha) \Rightarrow \alpha=\beta$
- „$\geq$" ist transitiv: $\forall \alpha,\beta,\gamma\in\mathbb{N}_0^n : \alpha\geq\beta \wedge \beta\geq\gamma \Rightarrow \alpha\geq\gamma$
- „$\geq$" ist konnex: $\forall \alpha,\beta\in\mathbb{N}_0^n : \alpha\geq\beta$ oder $\beta\geq\alpha$

(b) Falls $\alpha,\beta,\gamma\in\mathbb{N}_0^n$ mit $\alpha\geq\beta$, dann ist $\alpha+\gamma\geq\beta+\gamma$

(c) „$\geq$" ist eine Wohlordnung auf $\mathbb{N}_0^n$, d.h.
Ist $\alpha_1\geq\alpha_2\geq\dots\geq\alpha_m\geq\dots$ eine Folge in $\mathbb{N}_0^n$, dann existiert ein $N\in\mathbb{N}$ mit $\alpha_m=\alpha_N\ \forall m\geq N$, d.h. die Folge wird stationär.

Im folgenden schreiben wir $\alpha > \beta \overset{\text{Def}}{\Leftrightarrow} \alpha \geq \beta$ und $\alpha \neq \beta$.

Anm.: - Dies kann man auch in die Sprechweise der Monome übersetzen.

(b) lautet dann etwa: $\underline{X}^{\alpha} \geq \underline{X}^{\beta} \Rightarrow \underbrace{\underline{X}^{\alpha}\underline{X}^{\gamma}}_{(=\underline{X}^{\alpha+\gamma})} \geq \underbrace{\underline{X}^{\beta}\underline{X}^{\gamma}}_{(=\underline{X}^{\beta+\gamma})}$.

(c) kann man auch so formulieren:

Jede strikt fallende Folge aus $\mathbb{N}_0^n$ $\quad \alpha_1 > \alpha_2 > \dots$ bricht ab.

Bsp. 5.2: Die übliche „$\geq$"-Relation auf $\mathbb{N}_0$ ist eine Monomordnung.

Bem. 5.3: „$\geq$" Totalordnung auf $\mathbb{N}_0^n$. Dann sind äquivalent:

(i) „$\geq$" ist eine Wohlordnung

(ii) Zu jeder nichtleeren Teilmenge M von $\mathbb{N}_0^n$ existiert ein Element $x \in M$ mit $x \leq y \ \forall y \in M$. Dieses ist eindeutig bestimmt

(d.h. jede Teilmenge $M \subset \mathbb{N}_0^n$, $M \neq \emptyset$, besitzt ein eindeutig bestimmtes kleinstes Element bzgl. „$\leq$")

Bew.: (i)$\Rightarrow$(ii) Ann.: Es ex. eine Teilmenge $M \subset \mathbb{N}_0^n$, $M \neq \emptyset$, die kein kleinstes Element bzgl. „$\geq$" hat.

Sei $\alpha_1 \in M$. Dann ex. ein $\alpha_2 \in M$ mit $\alpha_1 > \alpha_2$.

Induktiv erhält man eine unendliche strikt fallende Folge

$$\alpha_1 > \alpha_2 > \dots$$

$\Rightarrow$ (i) ist verletzt

(ii)$\Rightarrow$(i) Ann.: Es ex. eine unendliche strikt fallende Folge

$$\alpha_1 > \alpha_2 > \dots$$

in $\mathbb{N}_0^n$. Dann ist $\{\alpha_1, \alpha_2, \dots\}$ eine Teilmenge von $\mathbb{N}_0^n$, die kein kleinstes Element besitzt.

*Eindeutigkeit eines kleinsten El. (falls existent): klar wg. Antisymmetrie von „$\geq$". □

Def. 5.4: (Lexikographische Ordnung) $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$

$\alpha \underset{lex}{\geq} \beta \overset{\text{Def}}{\Leftrightarrow}$ $\alpha = \beta$ oder $\alpha_i > \beta_i$ für das kleinste i mit $\alpha_i \neq \beta_i$

Wir schreiben $\underline{X}^{\alpha} \underset{lex}{\geq} \underline{X}^{\beta} \overset{\text{Def}}{\Leftrightarrow} \alpha \underset{lex}{\geq} \beta$.

Bsp. 5.5: • $(3,5,1) \underset{lex}{>} (2,1,0)$

• $(3,5,1) \underset{lex}{<} (3,6,2)$

• $(1,0,\dots,0) \underset{lex}{>} (0,1,0,\dots,0) \underset{lex}{>} \dots \underset{lex}{>} (0,0,\dots,1)$

d.h. $X_1 \underset{lex}{>} X_2 \underset{lex}{>} \dots \underset{lex}{>} X_n$

• Arbeitet man mit Polynom in 2 oder 3 Variablen X, Y, Z, verwendet man i.d.R. die Identifikation $X_1 = X$, $X_2 = Y$, $X_3 = Z$ und somit $X > Y > Z$.

Anm.: Die lexikographische Ordnung ist analog zur Anordnung von Wörtern im Wörterbuch.

Bem. 5.6: Die lexikographische Ordnung auf $\mathbb{N}_0^n$ ist eine Monomordnung.

Bew.: ① „$\underset{lex}{\geq}$" ist eine Totalordnung:

• Reflexivität: klar nach Def.

• Antisymmetrie: Seien $\alpha, \beta \in \mathbb{N}_0^n$ mit $\alpha \underset{lex}{\geq} \beta$ und $\beta \underset{lex}{\geq} \alpha$

Falls $\alpha \neq \beta$, dann wäre $\alpha_i > \beta_i$ für das kleinste i mit $\alpha_i \neq \beta_i$,

ebenso $\beta_i > \alpha_i$ ↯ Also $\alpha = \beta$.

• Transitivität: Sei $\alpha \underset{lex}{\geq} \beta$ und $\beta \underset{lex}{\geq} \gamma$

Falls $\alpha = \beta$ oder $\beta = \gamma$, dann ist offenbar $\alpha \underset{lex}{\geq} \gamma$.

Sei also im folgenden $\alpha \underset{lex}{>} \beta$, $\beta \underset{lex}{>} \gamma$.

Sei i minimal mit $\alpha_i > \beta_i$ und j minimal mit $\beta_j > \gamma_j$.

Dann ist $\alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$,

$\beta_1 = \gamma_1, \dots, \beta_{j-1} = \gamma_{j-1}, \beta_j > \gamma_j$.

Insbes. ist $\alpha_k = \gamma_k$ für alle k mit $1 \leq k < \min\{i,j\} =: m$

1. Fall: $m = i \neq j$. Dann ist $\alpha_m > \beta_m \neq \gamma_m$

2. Fall: $m = j \neq i$. Dann ist $\alpha_m \neq \beta_m > \gamma_m$

3. Fall: $m = i = j$. Dann ist $\alpha_m > \beta_m > \gamma_m$

• Konnexität: Klar nach Def.

② Seien $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ mit $\alpha \geq_{lex} \beta$,

Falls $\alpha = \beta$, dann ist $\alpha + \gamma = \beta + \gamma$.

Falls $\alpha \neq \beta$, sei i minimal mit $\alpha_i > \beta_i$

Dann ist $\alpha_1 + \gamma_1 = \beta_1 + \gamma_1$, ..., $\alpha_{i-1} + \gamma_{i-1} = \beta_{i-1} + \gamma_{i-1}$, $\alpha_i + \gamma_i > \beta_i + \gamma_i$

$\Rightarrow \alpha + \gamma \geq_{lex} \beta + \gamma$.

③ zz.: „$\geq_{lex}$" ist eine Wohlordnung

Sei $\eta_1, \eta_2, \ldots$ eine Folge in $\mathbb{N}_0^n$ mit

$$\eta_1 \geq_{lex} \eta_2 \geq_{lex} \eta_3 \geq_{lex} \ldots$$

Dann bilden die Komponenten $\eta_{1,1}, \eta_{2,1}, \ldots$ eine Folge mit d. Eig.

$$\eta_{1,1} \geq \eta_{2,1} \geq \ldots$$

Da $\mathbb{N}_0$ bzgl. „$\geq$" wohlgeordnet ist, wird diese Folge stationär,

d.h. $\exists k_1 \in \mathbb{N}$: $\eta_{i,1} = \eta_{k_1,1}$ $\forall i \geq k_1$.

Nach Def. d. lexikograph. Ordnung folgt

$$\eta_{i,2} \geq \eta_{i+1,2} \geq \ldots \qquad \forall i \geq k_1$$

und mit demselben Argument wie eben: $\exists k_2 \in \mathbb{N}$: $\eta_{i,1} = \eta_{k_2,1}$ $\forall i \geq k_2$

$\eta_{i,2} \geq \eta_{k_2,2}$

Induktiv erhält man schließlich ein $k_n \in \mathbb{N}$ mit $\eta_i = \eta_{k_n}$ $\forall i \geq k_n$,

d.h. obige Folge wird stationär.

<u>Def. 5.7:</u> (Graduiert lexikographische Ordnung) $\alpha, \beta \in \mathbb{N}_0^n$

$$\alpha \geq_{grlex} \beta \overset{Def}{\Leftrightarrow} \alpha = \beta \text{ oder } \begin{cases} |\alpha| > |\beta| \text{ oder} \\ |\alpha| = |\beta| \text{ und } \alpha >_{lex} \beta \end{cases}$$

(Zur Erinnerung: Für $i \in \mathbb{N}_0^n$ ist $|i| = i_1 + \ldots + i_n$)

<u>Bsp. 5.8:</u> • $(4,1,2) >_{grlex} (1,3,0)$ wg. $|(4,1,2)| = 7 > |(1,3,0)| = 4$

• $(4,1,2) >_{grlex} (3,3,1)$ wg. $|(4,1,2)| = 7 = |(3,3,1)|$ und $(4,1,2) \geq_{lex} (3,3,1)$

- $X_1 >_{grlex} X_2 > \dots >_{grlex} X_n$
- Es ist $X >_{lex} Y^2Z^3$, aber $X <_{grlex} Y^2Z^3$.

Bem. 5.9: „$\geq_{grlex}$" ist eine Monomordnung.

Bew.: ÜA

Def. 5.10: (Graduiert revers lexikographische Ordnung) $\alpha, \beta \in \mathbb{N}_0^n$

$$\alpha \geq_{grevlex} \beta \overset{Def}{\Leftrightarrow} \alpha = \beta \text{ oder}$$
$$|\alpha| > |\beta| \text{ oder}$$
$$|\alpha| = |\beta| \text{ und } \alpha_i < \beta_i \text{ für das größte } i \text{ mit } \alpha_i \neq \beta_i$$

Bsp. 5.11:
- $(4,1,2) >_{grevlex} (1,3,0)$ wg. $|(4,1,2)| = 7 \geq |(1,3,0)| = 4$
- $(4,1,2) <_{grevlex} (3,3,1)$ wg. $|(4,1,2)| = |(3,3,1)|$ und $2 > 1$.
- $(1,0,\dots,0) >_{grevlex} (0,1,0,\dots,0) >_{grevlex} \dots >_{grevlex} (0,0,\dots,0,1)$

(d.h. $X_1 >_{grevlex} X_2 >_{grevlex} \dots >_{grevlex} X_n$)

Bem. 5.12: „$\geq_{grevlex}$" ist eine Monomordnung.

Anm.: Ist eine Monomordnung auf $K[X_1, \dots, X_n]$ fixiert, können die Monome eines Polynoms angeordnet werden.

Bsp. 5.13: $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in \mathbb{Q}[X,Y,Z]$

- bzgl. „$\geq_{lex}$": $f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$
- bzgl. „$\geq_{grlex}$": $f = 7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2$
- bzgl. „$\geq_{grevlex}$" $f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2$

Def. 5.14: K Körper, $f = \sum_{\underline{i} \in \mathbb{N}_0^n} a_{\underline{i}} \underline{X}^{\underline{i}} \in K[X_1, \dots, X_n]$, $f \neq 0$, „$\geq$" Monomordnung auf $K[X_1, \dots, X_n]$

$$multideg(f) := \max_{(bzgl. \text{„}\geq\text{"})} \{ \underline{i} \in \mathbb{N}_0^n \mid a_{\underline{i}} \neq 0 \}$$ heißt Multigrad von f

$LC(f) := a_{multideg(f)} \in K$ heißt Leitkoeffizient von f

$LM(f) := X^{multideg(f)}$ heißt Leitmonom von f

$LT(f) := LC(f) \cdot LM(f)$ heißt Leitterm von f

Bsp. 5.15: $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in \mathbb{Q}[X,Y,Z]$ bzgl. $\geq_{lex}$:

$multideg(f) = (3,0,0)$, $LC(f) = -5$, $LM(f) = X^3$, $LT(f) = -5X^3$

(vgl. Bsp. 5.12)

Bem. 5.16: K Körper, $f,g \in K[X_1,\dots,X_n]$, $f,g \neq 0$. Dann gilt:

(a) $multideg(fg) = multideg(f) + multideg(g)$

(b) Falls $f+g \neq 0$, dann gilt:

$multideg(f+g) \leq \max\{multideg(f), multideg(g)\}$

Ist $multideg(f) \neq multideg(g)$, gilt sogar „$=$".

Bew.: ÜA.

§6. Divisionsalgorithmus in $K[X_1,\dots,X_n]$

Satz (Abg.) 6.1: (Divisionsalg. in $K[X_1,\dots,X_n]$) K Körper, „$\geq$" Monomordnung auf $\mathbb{N}_0^n$,

$F = (f_1,\dots,f_s) \in K[X_1,\dots,X_n]^s$, $f \in K[X_1,\dots,X_n]$.

Dann gilt:

Es existieren $a_1,\dots,a_s, r \in K[X_1,\dots,X_n]$, s.d. gilt:

- $f = a_1f_1 + \dots + a_sf_s + r$
- $r = 0$ oder r ist eine K-Linearkombination von Monomen, von denen keines durch $LT(f_1),\dots,LT(f_s)$ teilbar ist.

r heißt ein Rest von f bei Division durch F.

Falls $a_if_i \neq 0$ (sei $i \in \{1,\dots,s\}$), dann gilt: $multideg(f) \geq multideg(a_if_i)$

$a_1,\dots,a_s, r$ können mit folgendem Algorithmus bestimmt werden:

Eingabe: $(f_1, \dots, f_s), f$

Algorithmus:

$a_1 := 0, \dots, a_s := 0, r := 0$

$p := f$

WHILE $p \neq 0$ DO

  $i := 1$

  dividiert := FALSCH

  WHILE $i \leq s$ AND dividiert = FALSCH DO

Divisionsschritt (I):

    IF $LT(f_i) \mid LT(p)$ THEN

      $a_i := a_i + \frac{LT(p)}{LT(f_i)}$

      $p := p - \left(\frac{LT(p)}{LT(f_i)}\right) f_i$

      dividiert := WAHR

    ELSE

      $i := i+1$

  END WHILE

Restschritt (II):

  IF dividiert = FALSCH THEN

    $r := r + LT(p)$

    $p := p - LT(p)$

  END IF

END WHILE

Ausgabe: $f = r, a_1, \dots, a_s$

Bsp. 6.2: ↗ Vorlesungsmaterialien (pdf)

Bsp. 6.3: ↗ Vorlesungsmaterialien (pdf)

Bew. von Satz 6.1: (1) Der Algorithmus terminiert.

Beh.: Bei jeder Ausführung von (I), (II) sinkt der Multigrad von p oder p wird 0.

Bew.: (I) Setze $p' := p - \frac{LT(p)}{LT(f_i)} f_i$

$\rightarrow LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) \underset{\text{Übung}}{=} \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$

Falls $p' \neq 0$, dann ist $\text{multideg}(p') < \text{multideg}(p)$

(II) Setze $p' := p - LT(p)$

Falls $p' \neq 0$, dann ist $\text{multideg}(p') < \text{multideg}(p)$.

Falls p niemals 0 wird der Alg. nicht terminieren würde, erhielten wir eine unendliche strikt fallende Folge (der Multigrade multideg(p)) in $\mathbb{N}_0$"

↯ zur Wohlordnungseig. von „$\mathbb{Z}$".

Also $p=0$ nach endlich vielen Schritten, dh. der Alg. terminiert.

② Am Anfang sowie nach Ausführung des Divisions- bzw. Restschrittes gilt stets:

$$f = a_1 f_1 + \ldots + a_s f_s + p + r$$

Anfang: $a_1 = \ldots = a_s = 0$, $p = f$, $r = 0$ ✓

Es gelte $f = a_1 f_1 + \ldots + a_s f_s + p + r$.

Divisionsschritt: Es gelte $LT(f_i) \mid LT(p)$ für ein $i \in \{1, \ldots, n\}$

Setze $a_i' := a_i + \frac{LT(p)}{LT(f_i)}$, $p' := p - \frac{LT(p)}{LT(f_i)} f_i$

$$\Rightarrow a_i' f_i + p' = \left(a_i + \frac{LT(p)}{LT(f_i)}\right) f_i + p - \frac{LT(p)}{LT(f_i)} f_i = a_i f_i + p$$

Alle anderen Variablen bleiben gleich $\Rightarrow$ Beh.
Nach Konstruktion hat r die gewünschten Eigenschaften.

③ $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$, falls $a_i \neq 0$:

Jeder Term in a_i ist von d. Form $\frac{LT(p)}{LT(f_i)}$ für einen Wert von p, der im Laufe des Algorithmus angenommen wurde.

Der Algorithmus startet mit $p = f$, der Multigrad von p fällt bei jeder Ausführung von Divisions- bzw. Restschritt.

$\Rightarrow \text{multideg}(p) \leq \text{multideg}(f)$.

Es ist also $a_i = \frac{LT(p_1)}{LT(f_i)} + \ldots + \frac{LT(p_m)}{LT(f_i)}$ mit $\text{multideg}(p_i) \leq \text{multideg}(f)$ für $i = 1, \ldots, m$

$$\Rightarrow a_i f_i = \frac{LT(p_1)}{LT(f_i)} f_i + \ldots + \frac{LT(p_m)}{LT(f_i)} f_i$$

Es ist $LT\left(\frac{LT(p_k)}{LT(f_i)} f_i\right) = \frac{LT(p_k)}{LT(f_i)} LT(f_i) = LT(p_k)$ für $k = 1, \ldots, m$

$\Rightarrow \text{multideg}(a_i f_i) \leq \text{multideg}(f)$. □

Bsp. 6.4: Es ist (vgl. 6.3)

$$X^2Y + XY^2 + Y^2 = (X+Y)(XY-1) + 1\cdot(Y^2-1) + X + Y + 1$$ (berechnet via $F = (XY-1, Y^2-1)$)

ebenfalls ist

$$X^2Y + XY^2 + Y^2 = X(XY-1) + (X+1)(Y^2-1) + 2X + 1$$ (berechnet via $F = (Y^2-1, XY-1)$)

Dies zeigt daß in Alg. 6.1 die Elemente $a_{1,1}, \dots, a_{s,t}$ nicht eindeutig bestimmt sind.

Bsp. 6.5: Sei $f = XY^2 - X$, $f_1 = XY+1$, $f_2 = Y^2-1 \in K[X,Y]$, bzgl. „$\geq_{lex}$".

Wir erhalten (mit $F = (f_1, f_2)$):

$$f = XY^2 - X = Y(XY+1) + 0\cdot(Y^2-1) + (-X-Y),$$

mit $F = (f_2, f_1)$:

$$f = XY^2 - X = X(Y^2-1) + 0(XY+1) + 0$$

Insbesondere ist $f \in \langle f_1, f_2\rangle$, und trotzdem ist der Rest im Divisionsalg. bzgl. (f_1, f_2) ungleich Null.

Alg. 6.1 läßt sich in dieser Form also nicht benutzen, um Idealzugehörigkeit zu überprüfen.

Anm.: Wir werden in §8 „gute" Idealbasen kennenlernen, an denen man mit Hilfe des Divisionsalgorithmus über die Idealzugehörigkeit entscheiden kann.

§7. Monomideale und Dicksons Lemma

Def. 7.1: Ein Ideal $I \subset K[X_1, \dots, X_n]$ heißt Monomideal $\overset{\text{Def}}{\iff}$

$$\exists\, A \subset \mathbb{N}_0^n, \text{ sd. } I = \Big\{ \sum_{\alpha \in A} h_\alpha \underline{X}^\alpha \;\Big|\; h_\alpha \in K[\underline{X}],\ h_\alpha = 0 \text{ für fast alle } \alpha \in A \Big\}$$

Schreibweise: $I = \langle \underline{X}^\alpha \mid \alpha \in A\rangle$

Anm.: A kann auch unendlich sein.

Bsp. 7.2: $I = \langle X^2Y, XY^2, X^5Y^7\rangle (\subset K[X,Y])$ Sei

$$= \{ h_1 X^2Y + h_2 XY^2 + h_3 X^5Y^7 \}.\ A = \{(2,1), (1,2), (5,7)\}$$

Wg. $X^5Y^7 = (X^2Y)\cdot(X^3Y^6)$ kann X^3Y^6 als Erzeuger weggelassen werden.

Bem. 7.3: K Körper, $A \subset \mathbb{N}_0^n$, $J = \langle \underline{X}^\alpha \mid \alpha \in A \rangle \subset K[\underline{X}]$ Monomideal, $\beta \in \mathbb{N}_0^n$

Dann sind äquivalent:

(i) $\underline{X}^\beta \in J$

(ii) $\exists\, \alpha \in A: \underline{X}^\alpha \mid \underline{X}^\beta$

(iii) $\exists^{\alpha \in A,}\, \gamma \in \mathbb{N}_0^n: \beta = \alpha + \gamma$

Bew: (i) $\Rightarrow$ (ii) Sei $\underline{X}^\beta \in J \Rightarrow \underline{X}^\beta = \sum_{i=1}^{s} h_i \underline{X}^{\alpha_i}$ mit $h_1, \dots, h_s \in K[\underline{X}]$, $\alpha_i \in A$.

$\Rightarrow$ Jeder Term auf der rechten Seite ist durch ein Monom der Form $\underline{X}^{\alpha_i}$ teilbar

$\Rightarrow$ $\quad -\!\!-\quad$ linken $\quad -\!\!-$

$\Rightarrow \exists \alpha \in A: \underline{X}^\alpha \mid \underline{X}^\beta$

(ii) $\Rightarrow$ (i) $\underline{X}^\alpha \mid \underline{X}^\beta \Rightarrow \underline{X}^\beta \in \langle \underline{X}^\alpha \rangle \subset J$

(ii) $\Rightarrow$ (iii) Sei $\alpha \in A$ mit $\underline{X}^\alpha \mid \underline{X}^\beta$. Dann ex. ein $f \in K[\underline{X}]$ mit $\underline{X}^\beta = f \underline{X}^\alpha$. Offenbar kann f nur aus einem einzigen Term bestehen, und es ist $LC(f) = 1$, d.h. f ist ein Monom $\underline{X}^\gamma$ für ein $\gamma \in \mathbb{N}_0^n$.

$\Rightarrow \underline{X}^\beta = \underline{X}^\alpha \underline{X}^\gamma = \underline{X}^{\alpha+\gamma} \Rightarrow$ Beh. □

(iii) $\Rightarrow$ (ii) klar.

Bem. 7.4: K Körper, $J = \langle \underline{X}^\alpha \mid \alpha \in A \rangle \subset K[\underline{X}]$ Monomideal, $f \in K[\underline{X}]$.

Dann sind äquivalent:

(i) $f \in J$

(ii) Jeder Term von f liegt in J

(iii) f ist eine K-Linearkombination von Monomen aus J, d.h.

$\exists\, c_1, \dots, c_s \in K: f = c_1 \underline{X}^{\beta_1} + \dots + c_s \underline{X}^{\beta_s}$ mit $\underline{X}^{\beta_1}, \dots, \underline{X}^{\beta_s} \in J$

Bew: (iii) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (i) klar, da J Ideal.

(i) $\Rightarrow$ (iii) Sei $f \in J = \langle \underline{X}^\alpha \mid \alpha \in A \rangle \Rightarrow f = \sum_{i=1}^{r} h_i \underline{X}^{\alpha_i}$ mit $h_1, \dots, h_r \in K[\underline{X}]$, $\alpha_1, \dots, \alpha_r \in A$

$\Rightarrow$ Jeder Term von f ist von der Form $c\underline{X}^\beta$ mit $\underline{X}^{\alpha_i} \mid \underline{X}^\beta$ für ein $i \in \{1, \dots, r\}$, d.h. wegen 7.3: $\underline{X}^\beta \in J \Rightarrow$ Beh.

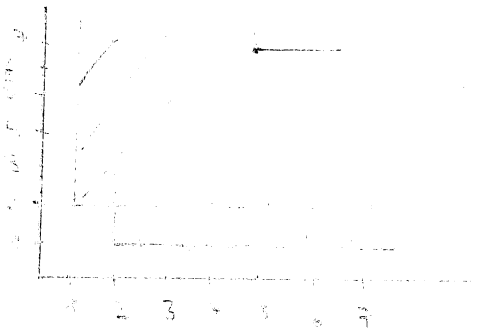
Bsp. 7.5: ~~[illegible]~~ vgl. 7.2: $J = \langle X^2Y, XY^2, X^5Y^7 \rangle \subset K[X,Y] = K[\underline{X}]$

Nach 7.4 ist $f \in J \Leftrightarrow f = c_1 \underline{X}^{\beta_1} + \ldots + c_s \underline{X}^{\beta_s}$ mit $c_1, \ldots, c_s \in K$ und $\beta_1, \ldots, \beta_s \in M$, wobei

$M = \{ (2,1) + \mathbb{N}_0^2 \} \cup \{ (1,2) + \mathbb{N}_0^2 \} \cup \{ (5,7) + \mathbb{N}_0^2 \}$

(denn nach 7.3 ist $\underline{X}^\beta \in J \Leftrightarrow \exists \gamma \in \mathbb{N}_0^2, \alpha \in A: \beta = \alpha + \gamma$ ✓)

Skizze von M:



Satz 7.6: (Dicksons Lemma) K Körper, $A \subset \mathbb{N}_0^n$, $J = \langle \underline{X}^\alpha \mid \alpha \in A \rangle \subset K[\underline{X}]$ Monomideal

Dann gilt:

$\exists \alpha_1, \ldots, \alpha_s \in A: J = \langle \underline{X}^{\alpha_1}, \ldots, \underline{X}^{\alpha_s} \rangle$

Insbesondere ist J endlich erzeugt.

Bew.: ① Wir zeigen per Induktion nach n, daß J endlich erzeugt ist.

$n=1$: $J = \langle \underline{X}^\alpha \mid \alpha \in A \rangle$, $A \subset \mathbb{N}_0$

Sei $\beta = \min A$. Dann gilt: $\underline{X}^\beta \mid \underline{X}^\alpha$ für alle $\alpha \in A$

$\Rightarrow J = \langle \underline{X}^\beta \rangle$

$n-1 \Rightarrow n$: Sei die Beh. für $n-1$ wahr.

Wir schreiben die n Variablen als $X_1, \ldots, X_{n-1}, Y$

Monome in $K[X_1, \ldots, X_{n-1}, Y]$ sind von der Form $\underline{X}^\alpha Y^m$ mit $\alpha \in \mathbb{N}_0^{n-1}$, $\beta \in \mathbb{N}_0$.

Sei $J \subset K[X_1, \ldots, X_{n-1}, Y]$ Monomideal.

Setze $J := \langle \underline{X}^\alpha \mid \alpha \in \mathbb{N}_0^{n-1}, \exists l \in \mathbb{N}_0: \underline{X}^\alpha Y^l \in J \rangle \subset K[X_1, \ldots, X_{n-1}]$

Nach Ind.ann. ex. $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0^{n-1}$: $J = \langle \underline{X}^{\alpha_1}, \ldots, \underline{X}^{\alpha_s} \rangle$

Für $i = 1, \ldots, s$ ex. $l_i \in \mathbb{N}_0$ mit $\underline{X}^{\alpha_i} Y^{l_i} \in J$.

Setze $m := \max_{i=1,\dots,s} l_i$.

Für $k = 0, \dots, m-1$ setze $\mathfrak{J}_k := \langle \underline{X}^\beta \mid \beta \in \mathbb{N}_0^{n-1}, \underline{X}^\beta Y^k \in \mathfrak{J} \rangle_{ck[X_1,\dots,X_{n-1}]}$

Es ist $\mathfrak{J}_0 \subset \mathfrak{J}_1 \subset \dots \subset \mathfrak{J}_{m-1}$.

Nach Ind.ann. ist $\mathfrak{J}_k = \langle \underline{X}^{\alpha_{k,1}}, \dots, \underline{X}^{\alpha_{k,s_k}} \rangle$ für $k = 0, \dots, m-1$,

und geeigneten $\alpha_{i,j} \in \mathbb{N}_0^{n-1}$.

Setze

$$\tilde{\mathfrak{J}} := \langle \underbrace{\underline{X}^{\alpha_1} Y^m}_{\in \mathfrak{J}}, \dots, \underbrace{\underline{X}^{\alpha_s} Y^m}_{\in \mathfrak{J}}, \quad \text{(vgl. Def. } \mathfrak{J}\text{)}$$

$$\underline{X}^{\alpha_{0,1}}, \dots, \underline{X}^{\alpha_{0,s_0}}, \quad \text{(vgl. } \mathfrak{J}_0\text{)}$$

$$\underline{X}^{\alpha_{1,1}} Y, \dots, \underline{X}^{\alpha_{1,s_1}} Y, \quad \text{(vgl. } \mathfrak{J}_1\text{)}$$

$$\vdots$$

$$\underbrace{\underline{X}^{\alpha_{m-1,1}} Y^{m-1}}_{\in \mathfrak{J}}, \dots, \underbrace{\underline{X}^{\alpha_{m-1,s_{m-1}}} Y^{m-1}}_{\in \mathfrak{J}} \rangle \quad \text{(vgl. } \mathfrak{J}_{m-1}\text{)}$$

Beh.: $\tilde{\mathfrak{J}} = \mathfrak{J}$

„$\subset$" nach Konstruktion (alle Erzeuger liegen in $\mathfrak{J}$)

„$\supset$" Jedes Monom aus $\mathfrak{J}$ ist durch eines der obigen Monome teilbar.

denn: Sei $\underline{X}^\alpha Y^p \in \mathfrak{J}$ mit $\alpha \in \mathbb{N}_0^{n-1}$, $p \in \mathbb{N}_0$

1. Fall: $p \geq m$.

Es ist $\underline{X}^\alpha \in \mathfrak{J} = \langle \underline{X}^{\alpha_1}, \dots, \underline{X}^{\alpha_s} \rangle \Rightarrow \exists i \in \{1,\dots,s\} : \underline{X}^{\alpha_i} \mid \underline{X}^\alpha$

$\Rightarrow \underline{X}^{\alpha_i} Y^p \mid \underline{X}^\alpha Y^p$

Wegen $p \geq m$ folgt $\underline{X}^{\alpha_i} Y^m \mid \underline{X}^{\alpha_i} Y^p$

2. Fall: $p \leq m-1$

Wegen $\underline{X}^\alpha Y^p \in \mathfrak{J}$ ist $\underline{X}^\alpha \in \mathfrak{J}_p = \langle \underline{X}^{\alpha_{p,1}}, \dots, \underline{X}^{\alpha_{p,s_p}} \rangle$

$\Rightarrow \exists i \in \{1,\dots,s_p\} : \underline{X}^{\alpha_{p,i}} \mid \underline{X}^\alpha$

$\Rightarrow \underline{X}^{\alpha_{p,i}} Y^p \mid \underline{X}^\alpha Y^p$

$\Rightarrow$ Jedes Monom aus $\mathfrak{J}$ liegt in $\tilde{\mathfrak{J}}$.

$\overset{7.4}{\Rightarrow} J \subset \tilde{J}$ (denn jedes $f \in J$ ist K-Linearkombination von Monomen aus J und somit aus $\tilde{J}$)

Also: $J = \tilde{J}$, damit ist J endlich erzeugt.

② Nach Schritt ① ist $J = \langle \underline{X}^{\alpha} \mid \alpha \in A \rangle \subset K[\underline{X}]$ endlich erzeugt.

noch zB.: Die Erzeuger können von der Form $\underline{X}^{\alpha_1}, \dots, \underline{X}^{\alpha_s}$ mit $\alpha_1, \dots, \alpha_s \in A$ gewählt werden: $J = \langle \underline{X}^{\alpha_1}, \dots, \underline{X}^{\alpha_s} \mid \alpha_1, \dots, \alpha_s \in A \rangle$

Bew.: Nach ① ist $J = \langle \underline{X}^{\beta_1}, \dots, \underline{X}^{\beta_s} \rangle$ mit $\underline{X}^{\beta_1}, \dots, \underline{X}^{\beta_s} \in J$.

$\overset{7.3}{\Rightarrow} \forall i \in \{1, \dots, s\} \; \exists \alpha_i \in A: \underline{X}^{\alpha_i} \mid \underline{X}^{\beta_i}$, d

Setze $\tilde{J} := \langle \underline{X}^{\alpha_1}, \dots, \underline{X}^{\alpha_s} \rangle$.

Dann ist $\tilde{J} \subset J$ wg. $\underline{X}^{\alpha_i} \in J$ für alle $i \in \{1, \dots, s\}$

Andererseits ist $\underline{X}^{\beta_i} \in \langle \underline{X}^{\alpha_i} \rangle \subset \tilde{J}$ für $i = 1, \dots, s$

$\Rightarrow J = \langle \underline{X}^{\beta_1}, \dots, \underline{X}^{\beta_s} \rangle \subset \tilde{J}$

Also $J = \tilde{J} = \langle \underline{X}^{\alpha_1}, \dots, \underline{X}^{\alpha_s} \rangle$. □

Bsp. 7.7: In Bsp. 7.2 sieht die Konstruktion aus obigem Beweis wie folgt aus:

$J = \langle X^2Y, XY^2, X^5Y^7 \rangle \subset K[X,Y]$

$J = \langle X \rangle$ (denn $XY^2 \in J$)

$m = 2$

$J_0 = \langle X^{\beta} \mid \beta \in \mathbb{N}_0, X^{\beta} \in J \rangle = \{0\}$

$J_1 = \langle X^{\beta} \mid \beta \in \mathbb{N}_0, X^{\beta}Y \in J \rangle = \langle X^2 \rangle$

$\tilde{J} = \langle XY^2, 0, X^2Y \rangle$

$X^5Y^7 \in \tilde{J}$, denn: $X^5 \in J = \langle X \rangle \Rightarrow XY^7 \mid X^5Y^7 \Rightarrow XY^2 \mid X^5Y^7$.

Folgerung 7.8: Sei „$\geq$" eine Relation auf $\mathbb{N}_0^n$ mit

- „$\geq$" ist eine Totalordnung
- Falls $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ mit $\alpha \geq \beta$, dann ist $\alpha + \gamma \geq \beta + \gamma$

Dann sind äquivalent:

(i) „$\geq$" ist eine Wohlordnung

(ii) $\alpha \geq 0 \quad \forall \alpha \in \mathbb{N}_0^n$

Bew.: (i)$\Rightarrow$(ii) Sei „$\geq$" Wohlordnung. Sei α_0 das kleinste Element von $\mathbb{N}_0^n$ bzgl. „$\geq$".

Ann.: $\alpha_0 < 0$

$\Rightarrow m\alpha_0 > (m+1)\alpha_0 \quad \forall m \in \mathbb{N}_0$

$\Rightarrow 0 > \alpha_0 > 2\alpha_0 > \ldots > m\alpha_0 > (m+1)\alpha_0 > \ldots$

Wir erhalten eine unendliche strikt fallende Folge in $\mathbb{N}_0^n$ bzgl. „$\geq$" ↯
Also: $\alpha_0 \geq 0$, damit $\alpha \geq 0 \ \forall \alpha \in \mathbb{N}_0^n$.

(ii)$\Rightarrow$(i) Sei $\alpha \geq 0 \ \forall \alpha \in \mathbb{N}_0^n$. Sei $A \subset \mathbb{N}_0^n$ nichtleer.

zz.: A hat ein kleinstes Element

Sei $J = \langle \underline{X}^\alpha \mid \alpha \in A \rangle$

$\overset{\text{7.6 Dickson}}{\Rightarrow} \exists \alpha_1, \ldots, \alpha_s \in A: J = \langle \underline{X}^{\alpha_1}, \ldots, \underline{X}^{\alpha_s} \rangle$, o.E. $\alpha_1 < \ldots < \alpha_s$

Beh.: α_1 ist das kleinste Element von A

Bew.: Sei $\alpha \in A \Rightarrow \underline{X}^\alpha \in J = \langle \underline{X}^{\alpha_1}, \ldots, \underline{X}^{\alpha_s} \rangle$

$\Rightarrow \exists i \in \{1, \ldots, s\}: \underline{X}^{\alpha_i} \mid \underline{X}^\alpha$

$\Rightarrow \exists \gamma \in \mathbb{N}_0^n: \alpha = \alpha_i + \gamma$

$\overset{\gamma \geq 0}{\Rightarrow} \alpha = \alpha_i + \gamma \geq \alpha_i + 0 \geq \alpha_1$

$\Rightarrow \alpha_1$ ist das kleinste El. von A.

Anm.: Diese Folgerung aus Dicksons Lemma vereinfacht die Überprüfung, ob es sich bei einer gegebenen Ordnung auf $\mathbb{N}_0^n$ mit den Eig. wie bei 7.8 um eine Monomordnung handelt, signifikant.

5.11.08

§8. Der Hilbertsche Basissatz und Gröbnerbasen

Ab jetzt sei auf dem Polynomring $K[X]$ eine Monomordnung fixiert.

Def. 8.1: K Körper, $J \subset K[X]$ Ideal, $J \neq \{0\}$.

$LT(J) := \{ LT(f) \mid f \in J \setminus \{0\} \} \subset K[X]$

$LT(0) := \emptyset$

$\langle LT(J) \rangle$ heißt das Leitideal von J.

Bsp. 8.2: Sei $J = \langle f_1, f_2 \rangle \subset K[X,Y]$ mit „$\succ_{grlex}$", $f_1 = X^3 - 2XY$,
$f_2 = X^2Y - 2Y^2 + X$

Es ist $X^2 = X(X^2Y - 2Y^2 + X) - Y(X^3 - 2XY) \Rightarrow X^2 \in J$

$\Rightarrow X^2 = LT(X^2) \in LT(J) \subset \langle LT(J) \rangle = L_J(J)$

Aber: $\langle LT(f_1), LT(f_2) \rangle = \langle X^3, X^2Y \rangle \Rightarrow X^2 \notin \langle LT(f_1), LT(f_2) \rangle$

Anm.: Ist $J = \langle f_1, \dots, f_s \rangle$, dann ist $LT(f_i) \in \langle LT(J) \rangle$ für $i = 1, \dots, s$,
insbes. ist $\langle LT(f_1), \dots, LT(f_s) \rangle \subset L_J(J)$.

Bsp. 8.2 zeigt, daß im allg. keine Gleichheit besteht.

Bem. 8.3: K Körper, $J \subset K[X]$ Ideal. Dann gilt:

(a) $L_J(J) = \langle LT(J) \rangle$ ist ein Monomideal

(b) $\exists\, g_1, \dots, g_t \in J$: $L_J(J) = \langle LT(g_1), \dots, LT(g_t) \rangle$

Bew.: (a) Es ist $L_J(J) = \langle LT(f) \mid f \in J \setminus \{0\} \rangle = \langle LM(f) \mid f \in J \setminus \{0\} \rangle$
(↑ unterscheiden sich nur um Elemente aus K.)

(b) $L_J(J) \overset{(a)}{=} \langle LM(g) \mid g \in J \setminus \{0\} \rangle$

$\overset{7.6}{\Rightarrow}$ (Lemma v. Dickson) $\exists\, g_1, \dots, g_t \in J \setminus \{0\}$: $L_J(J) = \langle LM(g_1), \dots, LM(g_t) \rangle$
$= \langle LT(g_1), \dots, LT(g_s) \rangle$

Satz 8.4: (Hilbertscher Basissatz) K Körper, $J \subset K[X]$. Dann gilt:

J ist endlich erzeugt, d.h. es ex. $g_1, \dots, g_t \in J$: $J = \langle g_1, \dots, g_t \rangle$

Bew.: Falls $J = \{0\}$, dann $J = \langle 0 \rangle$, fertig.

Sei also im folgenden $J \neq \{0\}$.

Wg. 8.3 (Lemma v. Dickson) ex. $g_1, \dots, g_t \in J$: $LT(J) = \langle LT(g_1), \dots, LT(g_t) \rangle$

Beh.: $J = \langle g_1, \dots, g_t \rangle$

Bew.: „$\supseteq$" klar, da $g_1, \dots, g_t \in J$

„$\subseteq$" Sei $f \in J$

$\overset{6.1}{\Rightarrow} \exists\, a_1, \dots, a_t \in K[X_1, \dots, X_n],\ r \in K[X_1, \dots, X_n]$:

$f = a_1 g_1 + \dots + a_t g_t + r$

sd. $r = 0$ oder r ist eine K-Linearkomb. von Monomen von denen keines durch $LT(g_1), \dots, LT(g_t)$ teilbar ist.

Beh.: $r = 0$

denn: $r = f - a_1 g_1 - \dots - a_t g_t \in J$

Falls $r \neq 0 \Rightarrow LT(r) \in LT(J) = \langle LT(g_1), \dots, LT(g_t) \rangle$

$\overset{7.3}{\Rightarrow} \exists i \in \{1, \dots, t\}$: $LT(g_i) \mid LT(r)$ ↯

Also: $r = 0 \Rightarrow f = a_1 g_1 + \dots + a_t g_t \in \langle g_1, \dots, g_t \rangle$

$\Rightarrow$ „$\subseteq$".

□

Def. 8.5: K Körper, $J \subset K[X]$ Ideal, „$\geq$" Monomordnung auf $K[X]$

$G = \{g_1, \dots, g_t\} \subset J$ ($g_1, \dots, g_t \neq 0$, $\{0\}$) heißt Gröbnerbasis (bzgl. „$\geq$") von J, wenn

$$LT(J) = \langle LT(g_1), \dots, LT(g_t) \rangle$$

Folgerung 8.6: K Körper, $J \subset K[X]$. Dann gilt:

(a) J besitzt eine Gröbnerbasis

(b) Ist $G \subset J$ eine Gröbnerbasis von J, dann ist J eine Basis von J

Bew.: siehe Bew. von 8.4

□

Bem. 8.7: K Körper, $J \subset K[X]$ Ideal, $G = \{g_1, \dots, g_t\} \subset J$.

Dann sind äquivalent:

(i) G ist eine Gröbnerbasis von J

(ii) Für alle $f \in J \setminus \{0\}$ ex. ein $i \in \{1, \dots, t\}$ sd. $LT(g_i) \mid LT(f)$

Bew.: aus Def. 8.5 und 7.3

Bsp. 8.8: Sei $J = \langle f_1, f_2 \rangle \subset K[X,Y]$, $f_1 = X^3 - 2XY$, $f_2 = X^2Y - 2Y^2 + X$

bzgl. „$\leq_{grlex}$" (siehe Bsp. 8.2)

Dann ist $\{f_1, f_2\}$ keine Gröbnerbasis von J, denn $\langle LT(f_1), LT(f_2) \rangle \subsetneq \langle LT(f) \rangle$

Bsp. 8.9: Sei $J = \langle g_1, g_2 \rangle \subset \mathbb{R}[X,Y,Z]$, $g_1 = X + Z$, $g_2 = Y - Z$

Beh.: $\{g_1, g_2\}$ ist eine Gröbnerbasis von J bzgl. „$\geq_{lex}$".

zz. ist wg. 8.7: Ist $f \in J \setminus \{0\}$, dann gilt: $\underset{LT(g_1)}{X} \mid LT(f)$ oder $LT(g_2) = Y \mid LT(f)$

Sei $f = Ag_1 + Bg_2 \in J$, $f \neq 0$, mit $A, B \in \mathbb{R}[X,Y,Z]$

Ann.: $X \nmid LT(f)$ und $Y \nmid LT(f) \Rightarrow f \in \mathbb{R}[Z]$

Setze $V := V(X+Z, Y-Z)$. Wegen $f = A(X+Z) + B(Y-Z)$ ist $f|_V = 0$

Offenbar ist $V = \{t(-1,1,1) \mid t \in \mathbb{R}\}$

$\overset{4.6}{\Rightarrow} f = 0$ ↯.

Satz 8.10: (Aufsteigende Kettenbedingung) K Körper.

Sei $J_1 \subset J_2 \subset J_3 \subset \dots$ eine aufsteigende Kette von Idealen in $K[X]$. Dann ex. ein $N \geq 1$, sd.

$$J_N = J_{N+1} = \dots$$

Bew.: Setze $J := \bigcup_{k=1}^{\infty} J_k$

① J ist ein Ideal in $K[X]$, denn:

- $0 \in J$, denn $0 \in J_k$ für alle $k \in \mathbb{N}$

· Es seien $f, g \in J \Rightarrow \exists i,j \in \mathbb{N}: f \in J_i, g \in J_j$

Es ist $J_i \subset J_j$ oder $J_j \subset J_i$, o.E. $J_i \subset J_j$. $\Rightarrow f, g \in J_j$

$\Rightarrow f+g \in J_j \subset J$

· Es sei $f \in J$, $h \in K[X]$. Dann ex. ein $j \in \mathbb{N}$ mit $f \in J_j \Rightarrow hf \in J_j \subset J$.

② Wg. Hilbertsch. Basissatz ex. $f_1, \dots, f_s \in J$, sd. $J = \langle f_1, \dots, f_s \rangle$

Für $k = 1, \dots, s$ ex. $j_k \in \mathbb{N}$ mit $f_k \in J_{j_k}$.

Setze $m := \max_{k=1,\dots,s} j_k$. Dann gilt: $f_1, \dots, f_s \in J_m$

$\Rightarrow J = \langle f_1, \dots, f_s \rangle \subset J_m \subset J$

$\Rightarrow J = J_m = J_{m+1} = \dots$ □

Anm.: Ein Ring, der die obige Bedingung für absteigende Ketten von Idealen erfüllt, heißt ein Noetherscher Ring. Der Polynomring $K[X]$ ist also ein Noetherscher Ring.

Def. 8.11: K Körper, $J \subset K[X]$ Ideal.

$V(J) := \{ a \in K^n \mid f(a) = 0 \text{ für alle } f \in J \}$ heißt die Varietät von J.

Bem. 8.12: K Körper, $J \subset K[X]$ Ideal. Dann gilt:

(a) $V(J)$ ist eine affine Varietät

(b) Ist $J = \langle f_1, \dots, f_s \rangle$, dann ist $V(J) = V(f_1, \dots, f_s)$

Bew.: Nach Hilbertschem Basissatz ex. $f_1, \dots, f_s \in J$, sd. $J = \langle f_1, \dots, f_s \rangle$.

Beh.: $V(J) = V(f_1, \dots, f_s)$ $(\Rightarrow (a), (b))$

„$\subset$" Sei $a \in V(J) \Rightarrow f(a) = 0 \ \forall f \in J \Rightarrow f_1(a) = \dots = f_s(a) = 0$

$\Rightarrow a \in V(f_1, \dots, f_s)$

„$\supset$" Sei $a \in V(f_1, \dots, f_s) \Rightarrow f_1(a) = \dots = f_s(a) = 0$

Sei $f \in J \Rightarrow \exists h_1, \dots, h_s \in K[X]: f = \sum_{i=1}^{s} h_i f_i \Rightarrow f(a) = \sum_{i=1}^{s} h_i(a) \underbrace{f_i(a)}_{=0} = 0$

$\Rightarrow a \in V(J)$.

Anm.: 8.12 liefert auch einen neuen Bew. von 3.7: $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$

$\Rightarrow V(f_1, \dots, f_s) = V(g_1, \dots, g_t)$.

§9. Eigenschaften von Gröbnerbasen

Im folgenden sei stets eine Monomordnung fixiert, wenn wir von einer Gröbnerbasis sprechen.

Bem. 9.1: K Körper, $J \subset K[X]$ Ideal, $G = \{g_1, \dots, g_t\}$ Gröbnerbasis von J, $f \in K[X]$. Dann gilt:

Es existiert genau ein $r \in K[X]$ mit den folgenden Eigenschaften:

(a) Kein Term von r ist durch einen der Terme $LT(g_1), \dots, LT(g_t)$ teilbar

(b) Es ex. ein $g \in J$ mit $f = g + r$ (oder $r = 0$)

Insbesondere ist der Rest der Division von f durch G eindeutig bestimmt (egal wie G angeordnet wird) und stimmt mit r überein.

Beweis: ① Existenz: Nach 6.1 (Div.alg. in $K[X]$) existieren stets $a_1, \dots, a_t, r \in K[X]$

mit $f = a_1 g_1 + \dots + a_t g_t + r$,

und r erfüllt (a)

Setze $g := a_1 g_1 + \dots + a_t g_t$, dann ist $g \in J = \langle g_1, \dots, g_t \rangle$

② Eindeutigkeit:

Sei $f = g_1 + r_1 = g_2 + r_2$ mit g_1, g_2, r_1, r_2 wie oben

$\Rightarrow r_2 - r_1 = g_1 - g_2 \in J$

Falls $r_1 \neq r_2 \Rightarrow LT(r_1 - r_2) \in LT(J) \overset{G \text{ Gröbner basis}}{=} \langle LT(g_1), \dots, LT(g_t) \rangle$

$\Rightarrow \exists i \in \{1, \dots, t\}: LT(g_i) \mid LT(r_2 - r_1)$ ↯ da kein Term von r_1, r_2 durch einen der Terme $LT(g_1), \dots, LT(g_t)$ teilbar.

Also: $r_2 - r_1 = 0 \Rightarrow$ Beh.

Der Zusatz folgt aus der Eindeutigkeit von r. □

Anm.: In der Situation von 9.1 macht es also Sinn $\bar{f}^{\{g_1, \dots, g_n\}}$ statt $\bar{f}^{(g_1, \dots, g_n)}$ zu schreiben und die Ordnung auf $(g_1, \dots, g_n)$ zu vergessen.

Folgerung 9.2: K Körper, $J \subset K[X]$ Ideal, $G = \{g_1, \dots, g_t\}$ Gröbnerbasis von J.

Dann sind äquivalent:

(i) $f \in J$

(ii) $\bar{f}^G = 0$

Bew.: (i)$\Rightarrow$(ii) $f = \overset{\in J}{f} + 0$, $r = 0$ erfüllt (a), (b) aus 9.1

$\overset{9.1}{\Rightarrow} \bar{f}^G = 0$.

(ii)$\Rightarrow$(i) $\bar{f}^G = 0 \Rightarrow f \in \langle g_1, \dots, g_t \rangle = J$. □

Anm.: Ein Hindernis für $\{f_1, \dots, f_s\}$ eine Gröbnerbasis von $\langle f_1, \dots, f_s \rangle$ zu sein, ist die Existenz von $f \in J$ mit $LT(f) \notin \langle LT(f_1), \dots, LT(f_s) \rangle$

So etwas kann auftreten bei einem Polynom d. Form

$$a X^{\alpha} f_i - b X^{\beta} f_j ,$$

wo sich die Leitterme wegheben. Diese Möglichkeit werden wir nun studieren.

Def. 9.3: K Körper, $f, g \in K[X]$ ($K[X_1, \dots, X_n]$), $f, g \neq 0$, $\alpha = \text{multideg}(f)$, $\beta = \text{multideg}(g)$

Sei $\gamma = (\gamma_1, \dots, \gamma_n)$ mit $\gamma_i = \max(\alpha_i, \beta_i)$ für $i = 1, \dots, n$

$kgV(LM(f), LM(g)) := X^{\gamma}$ heißt kleinstes gem. Vielfaches von $LM(f), LM(g)$

($LM(f) = X^{\alpha}$, $LM(g) = X^{\beta}$)

$$S(f,g) := \frac{X^{\gamma}}{LT(f)} f - \frac{X^{\gamma}}{LT(g)} g$$ heißt S-Polynom von f, g.

Bsp. 9.4: $f = X^3Y^2 - X^2Y^3$, $g = 3X^4Y + Y^2 \in \mathbb{R}[X,Y]$ bzgl. $\leq_{grlex}$.

$\text{multideg}(f) = (3,2)$, $\text{multideg}(g) = (4,1)$

$kgV(X^3Y^2, X^4Y) = X^4Y^2$

$$S(f,g) = \frac{X^4Y^2}{X^3Y^2} f - \frac{X^4Y^2}{3X^4Y} g = Xf - \frac{1}{3} Y g = X(X^3Y^2 - Y^2X^3) - \frac{1}{3} Y(3X^4Y + Y^2)$$

$$= -X^3Y^3 + X^2 - \frac{1}{3} Y^3$$

Bem. 9.5: K Körper, $f = \sum_{i=1}^{t} c_i \underline{X}^{\alpha_i} g_i \in K[\underline{X}]$ mit $c_i \in K$, $\alpha_i \in \mathbb{N}_0^n$, $g_i \in K[\underline{X}]$, $\delta \in \mathbb{N}_0^n$, so daß

$$\alpha_i + \text{multideg}(g_i) = \delta \quad \text{für alle } i \in \{1, \dots, t\}$$

Dann gilt:

Ist $\text{multideg}(f) < \delta$, dann existieren $c_{jk} \in K$, $\gamma_{jk} \in \mathbb{N}_0^n$, $k, j = 1, \dots, t$ mit

$$f = \sum_{j,k} c_{jk} \underline{X}^{\delta - \gamma_{jk}} S(g_j, g_k)$$

Hierbei ist γ_{jk} gegeben durch

$$\underline{X}^{\gamma_{jk}} = kgV(LM(g_j), LM(g_k))$$

Es gilt ferner: $\text{multideg}(\underline{X}^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta$ für $k, j = 1, \dots, t$. $k \neq j$.

Bew.: Setze $d_i := LC(g_i)$ für $i = 1, \dots, t$.

$\Rightarrow LC(c_i \underline{X}^{\alpha_i} g_i) = c_i d_i$ -"-

Wegen $\text{multideg}(c_i \underline{X}^{\alpha_i} g_i) = \delta$ für $i = 1, \dots, t$ und $\text{multideg}(f) < \delta$ folgt:

$$\sum_{i=1}^{t} c_i d_i = 0.$$

Setze $p_i := \frac{\underline{X}^{\alpha_i} g_i}{d_i}$ für $i = 1, \dots, t$ (dann ist insb. $LC(p_i) = 1$, $\text{multideg}(p_i) = \delta$)

Wir erhalten

$$f = \sum_{i=1}^{t} c_i \underline{X}^{\alpha_i} g_i = \sum_{i=1}^{t} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3)$$
$$+ \dots + (c_1 d_1 + \dots + c_{t-1} d_{t-1})(p_{t-1} - p_t)$$
$$+ (\underbrace{c_1 d_1 + \dots + c_t d_t}_{=0}) p_t$$

~~Bem. $i = 1, \dots, t$ existieren $\beta_i \in \mathbb{N}_0^n$ mit $LT(g_i) = d_i \underline{X}^{\beta_i}$.~~

Setze $\beta_i := \text{multideg}(g_i)$ für $i = 1, \dots, t$.

Insbes. gilt dann $\alpha_i + \beta_i = \delta$ für $i = 1, \dots, t$.

$\Rightarrow LM(g_i) = \underline{X}^{\beta_i} \mid \underline{X}^{\delta}$

$\Rightarrow \underline{X}^{\gamma_{jk}} = kgV(LM(g_j), LM(g_k)) \mid \underline{X}^{\delta} \Rightarrow \underline{X}^{\delta-\gamma_{jk}}$ ist wohldef

für $j,k = 1,\dots,t$

Es ist für $j,k = 1,\dots,t$

$$\underline{X}^{\delta-\gamma_{jk}} S(g_j,g_k) = \underline{X}^{\delta-\gamma_{jk}} \left(\frac{\underline{X}^{\gamma_{jk}}}{LT(g_j)} g_j - \frac{\underline{X}^{\gamma_{jk}}}{LT(g_k)} g_k \right)$$

$$= \frac{\underline{X}^{\delta}}{d_j \underline{X}^{\beta_j}} g_j - \frac{\underline{X}^{\delta}}{d_k \underline{X}^{\beta_k}} g_k$$

$$= \frac{\underline{X}^{\alpha_j}}{d_j} g_j - \frac{\underline{X}^{\alpha_k}}{d_k} g_k = p_j - p_k$$

$$\Rightarrow f = c_1 d_1 \underline{X}^{\delta-\gamma_{12}} S(g_1,g_2) + (c_1 d_1 + c_2 d_2) \underline{X}^{\delta-\gamma_{23}} S(g_2,g_3)$$

$$+ \dots + (c_1 d_1 + \dots + c_{t-1} d_{t-1}) \underline{X}^{\delta-\gamma_{t-1,t}} S(g_{t-1},g_t)$$

Definiere $c_{jk} := \sum_{i=1}^{j} c_i d_i$, falls $k = j+1$, sonst $c_{jk} = 0$.

Es ist multideg $(p_j) = \delta$, $LC(p_j) = 1$ für $j = 1,\dots,t$

$\Rightarrow$ multideg $(\underline{X}^{\delta-\gamma_{jk}} S(g_j,g_k)) = $ multideg $(p_j - p_k) < \delta$ für $k,j = 1,\dots,t$, $k \neq j$. □

Satz 9.6: K Körper, $J \subset K[\underline{X}]$ Ideal, $G = \{g_1,\dots,g_t\} \subset J$ Basis von J.

Dann sind äquivalent:

(i) G ist eine Gröbnerbasis von J

(ii) Für alle $i,j \in \{1,\dots,t\}$, $i \neq j$, ist $\overline{S(g_i,g_j)}^{G} = 0$ (hierbei ist G mit einer beliebigen Anordnung versehen).

Bew.: (i) $\Rightarrow$ (ii) Es ist $S(g_i,g_j) \in \langle g_i, g_j \rangle \subset J \overset{9.2}{\Rightarrow} \overline{S(g_i,g_j)}^{G} = 0$.

(ii) $\Rightarrow$ (i) Sei $f \in J$, $f \neq 0$.

zz.: $LT(f) \in \langle LT(g_1),\dots,LT(g_t) \rangle$

Es ex. $h_1,\dots,h_t \in K[\underline{X}]$ mit $f = \sum_{i=1}^{t} h_i g_i$.

Setze $m_i := \text{multideg}(h_i g_i)$, $\delta := \max_{i=1,\dots,t} m_i$

Wg. 5.14 ist $\text{multideg}(f) \leq \delta$.

Wir wählen $h_1,\dots,h_t$ so, daß δ minimal ist. Das geht weil unsere Monomordnung eine Wohlordnung ist.

Beh.: Dann ist $\text{multideg}(f) = \delta$

(Insbes. ist dann $\text{multideg}(f) = \text{multideg}(h_{i_0} g_{i_0})$ für ein $i_0 \in \{1,\dots,t\}$

$\Rightarrow LT(g_{i_0}) \mid LT(f) \Rightarrow LT(f) \in \langle LT(g_1),\dots,LT(g_t)\rangle \Rightarrow$ Beh. fertig)

Bew. d. Beh.: Ann.: $\text{multideg}(f) < \delta$

Wir schreiben

$$f = \sum_{m_i=\delta} h_i g_i + \sum_{m_i<\delta} h_i g_i = \sum_{m_i=\delta} LT(h_i) g_i + \sum_{m_i=\delta} \underbrace{(h_i - LT(h_i)) g_i + \sum_{m_i<\delta} h_i g_i}_{\text{Terme von multideg} < \delta}$$

$\overset{\text{multideg}(f)<\delta}{\Rightarrow}$ $\text{multideg}\left(\sum_{m_i=\delta} LT(h_i) g_i\right) < \delta$

Sei $LT(h_i) = c_i \underline{X}^{\alpha_i}$ mit $c_i \in K$, $\alpha \in \mathbb{N}_0^n$

$$\Rightarrow \sum_{m_i=\delta} LT(h_i) g_i = \sum_{m_i=\delta} c_i \underline{X}^{\alpha_i} g_i \overset{9.5}{=} \sum_{j,k} c_{jk} \underline{X}^{\delta-\gamma_{jk}} S(g_j,g_k)$$ mit geeigneten $c_{jk} \in K$,

$\underline{X}^{\gamma_{jk}} = kgV(LM(g_j), LM(g_k))$

Nach Vor. ist $\overline{S(g_j,g_k)}^{G} = 0$ für alle $j,k \in \{1,\dots,t\}$, d.h.

$$S(g_j,g_k) = \sum_{i=1}^{t} q_{ijk} g_i \quad \text{mit } q_{ijk} \in K[\underline{X}],$$

4. $\text{multideg}(q_{ijk} g_i) \leq \text{multideg}(S(g_j,g_k))$ für alle $i,j,k \in \{1,\dots,t\}$, $j \neq k$.

Es ist dann

$$\underline{X}^{\delta-\gamma_{jk}} S(g_j,g_k) = \sum_{i=1}^{t} b_{ijk} g_i \quad \text{mit geeigneten } b_{ijk} \in K[\underline{X}]$$

und $\text{multideg}(b_{ijk} g_i) \leq \text{multideg}(\underline{X}^{\delta-\gamma_{jk}} S(g_j,g_k)) \overset{9.5}{<} \delta$ für alle $i,j,k \in \{1,\dots,t\}$, $j \neq k$

$$\Rightarrow \sum_{m_i=\delta} LT(h_i)\,g_i = \sum_{jik} c_{jk} \sum_{i=1}^{t} b_{ijk}\,g_i = \sum_{i=1}^{t}\Big(\sum_{jik} c_{jk} b_{ijk}\Big) g_i = \sum_{i=1}^{t} \tilde{h}_i\, g_i$$

mit $\tilde{h}_i := \sum_{jik} c_{jk} b_{ijk}$

Wegen $multideg(b_{ijk}\,g_i) < \delta$ folgt $multideg\Big(\sum_{jik} c_{jk} b_{ijk}\Big) g_i < \delta$,

also $multideg(\tilde{h}_i\, g_i) < \delta$

$$\Rightarrow f = \sum_{m_i=\delta} LT(h_i)\,g_i + \sum_{m_i=\delta} (h_i - LT(h_i))\,g_i + \sum_{m_i<\delta} h_i g_i$$

$$= \sum_{i=1}^{t} \underbrace{\tilde{h}_i\, g_i}_{multideg<\delta} + \sum_{m_i=\delta} \underbrace{(h_i - LT(h_i))\,g_i}_{multideg<\delta} + \sum_{m_i<\delta} \underbrace{h_i g_i}_{multideg<\delta}$$

↯ zur Minimalität von δ

Bsp. 9.7: $J = \langle Y - X^2, Z - X^3 \rangle \subset \mathbb{R}[X, Y, Z]$

Beh.: $G = \{Y - X^2, Z - X^3\}$ ist eine Gröbnerbasis von J bzgl. „$\geq_{lex}$"

mit $Y > Z > X$

denn: $S(Y - X^2, Z - X^3) = \frac{YZ}{Y}(Y - X^2) - \frac{YZ}{Z}(Z - X^3) =$

$$= -ZX^2 + YX^3$$

$$= X^3(Y - X^2) + (-X^2)(Z - X^3)$$

$$\Rightarrow \overline{S(Y - X^2, Z - X^3)}^{G} = 0$$

Bezüglich „$\geq_{lex}$" mit $X > Y > Z$ ist G aber keine Gröbnerbasis von J.

In diesem Fall ist nämlich $LT(Y - X^2) = -X^2$, $LT(Z - X^3) = X^3$, also

$$\langle LT(Y - X^2), LT(Z - X^3) \rangle = \langle -X^2, X^3 \rangle = \langle X^2 \rangle$$

Aber: $-X(Y - X^2) + 1\cdot(Z - X^3) = -XY + Z \in \langle Y - X^2, Z - X^3 \rangle$,

$$LT(-XY + Z) = -XY \notin \langle X^2 \rangle = \langle LT(Y - X^2), LT(Z - X^3) \rangle.$$

Man prüft in diesem Falle auch nach: $\overline{S(Y - X^2, Z - X^3)}^{G} \neq 0$.

§10. Der Buchberger-Algorithmus

Satz + Alg. 10.1: (Buchberger-Algorithmus) K Körper, $f_1,\dots,f_s \in K[X]$, $J = \langle f_1,\dots,f_s\rangle$.

Dann gilt: Der folgende Algorithmus liefert eine Gröbnerbasis für J.

Eingabe: $F = \{f_1,\dots,f_s\}$

Algorithmus: $G := F$

REPEAT

$G' := G$

FOR $p,q \in G', p \neq q$ DO

$S := \overline{S(p,q)}^{G'}$

IF $S \neq 0$ THEN $G := G \cup \{S\}$

UNTIL $G = G'$

Ausgabe: Gröbnerbasis$(F) := G$

Bsp. 10.2: Sei $J = \langle f_1, f_2\rangle \subset \mathbb{R}[X,Y]$ mit $f_1 := X^3 - 2XY$, $f_2 := X^2Y - 2Y^2 + X$,

Monomordnung sei „$\geq_{grlex}$". (vgl. Bsp. 8.2)

Es ist $S(f_1,f_2) = -X^2$, $\overline{S(f_1,f_2)}^{(f_1,f_2)} = -X^2 \neq 0$

$\Rightarrow G := \{f_1, f_2\}$ ist keine Gröbnerbasis von J

Füge zu G das Polynom $f_3 := \overline{S(f_1,f_2)}^{(f_1,f_2)}$ hinzu: $G := \{f_1,f_2,f_3\}$.

Erhalte folgende S-Polynome für G: $S(f_1,f_2) = f_3$, d.h. $\overline{S(f_1,f_2)}^{G} = 0$

$S(f_1,f_3) = -2XY$, $\overline{S(f_1,f_3)}^{G} = -2XY \neq 0$

Füge zu G das Polynom $f_4 := \overline{S(f_1,f_3)}^{G} = -2XY$ hinzu: $G := \{f_1,f_2,f_3,f_4\}$.

Erhalte folgende S-Polynome für G:

$\overline{S(f_1,f_2)}^{G} = \overline{S(f_1,f_3)}^{G} = 0$ (nach Konstruktion)

$\overline{S(f_1,f_4)}^{G} = 0$ (ausrechnen)

$S(f_2,f_3) = -2Y^2 + X$, $\overline{S(f_2,f_3)}^{G} = -2Y^2 + X \neq 0$

Füge zu G das Polynom $f_5 := -2Y^2 + X$ hinzu: $G = \{f_1, f_2, f_3, f_4, f_5\}$.

Man rechnet nun nach: $\overline{S(f_i, f_j)}^{G} = 0$ für $1 \le i < j \le 5$.

$\Rightarrow G = \{f_1, f_2, f_3, f_4, f_5\}$ ist eine Gröbnerbasis von J.

Bew. von Satz 10.1: ① Algorithmus terminiert:

Nach jedem Durchlauf der REPEAT-UNTIL-Schleife gilt jeweils

$$G = G' \cup \{ \overline{S(p,q)}^{G'} \mid p, q \in G', \overline{S(p,q)}^{G'} \neq 0 \}$$

Beh.: Falls $G' \subsetneq G$, dann ist $\langle LT(G') \rangle \subsetneq \langle LT(G) \rangle$

Bew.: Seien $p, q \in G'$, $p \neq q$ mit $r := \overline{S(p,q)}^{G'} \neq 0$.

$\Rightarrow LT(r)$ ist durch kein $LT(g)$, $g \in G'$, teilbar

$\Rightarrow LT(r) \notin \langle LT(G') \rangle$, aber $LT(r) \in \langle LT(G) \rangle$

Die Ideale $\langle LT(G) \rangle$ aus den sukzessiven Iterationen der REPEAT-UNTIL-Schleife bilden eine aufsteigende Kette. Nach Satz 8.10 stabilisiert diese Kette, d.h. nach endlich vielen Schleifendurchläufen ist $\langle LT(G') \rangle = \langle LT(G) \rangle$. Wegen obiger Behauptung ist dann $G' = G$, d.h. obiger Algorithmus terminiert

② Algorithmus liefert eine Gröbnerbasis

Beh.: $G \subset J$ an jeder Stelle im Algorithmus

Bew.: · Am Anfang ist $G = F \subset J$

· Für $p, q \in G \subset J$ ist $S(p,q) \in J$ und somit auch $S := \overline{S(p,q)}^{G} \in J$

(denn: $S(p,q) = \sum_{g \in G} h_g g + S$, $S(p,q) \in J$, $\sum_{g \in G} h_g g \in J$)

$\Rightarrow G \cup \{S\} \subset J$

Wegen $G \supset \{f_1, \dots, f_5\}$ ist G eine Basis von J.

Nach Terminierung des Algorithmus ist $\overline{S(p,q)}^{G} = 0$ für alle $p, q \in G$, $p \neq q$

$\overset{9.6}{\Rightarrow}$ G ist Gröbnerbasis von J. □

Anm.: Der Algorithmus aus 10.1 kann noch deutlich verbessert werden (vgl. evtl. Übung)

Bem. 10.3: K Körper, $J \subset K[\underline{X}]$ Ideal, G Gröbnerbasis von J, $p \in G$ mit $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$.

Dann gilt: $G \setminus \{p\}$ ist eine Gröbnerbasis von J.

Bew.: Es ist $LT(J) = \langle LT(G) \rangle$

Wegen $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$ ist $LT(J) = \langle LT(G) \rangle = \langle LT(G \setminus \{p\}) \rangle$

$\Rightarrow G \setminus \{p\}$ ist eine Gröbnerbasis von J. □

Def. 10.4: K Körper, $J \subset K[\underline{X}]$ Ideal, G Gröbnerbasis von J

G heißt minimale Gröbnerbasis von J, wenn die folgenden Bedingungen erfüllt sind:

(a) $LC(p) = 1$ für alle $p \in G$

(b) $LT(p) \notin \langle LT(G \setminus \{p\}) \rangle$ für alle $p \in G$.

Bsp 10.5: (vgl. Bsp 10.2) $J = \langle f_1, f_2, f_3, f_4, f_5 \rangle \subset \mathbb{R}[X,Y]$,

$f_1 = X^3 - 2XY$, $f_2 = X^2Y - 2Y^2 + X$, $f_3 = -X^2$, $f_4 = -2XY$, $f_5 = -2Y^2 + X \in \mathbb{R}[X,Y]$

(bzgl. „$\geq_{grlex}$"), $\{f_1, \dots, f_5\}$ ist Gröbnerbasis von J.

Es ist $LT(f_1) = X^3 = -X\,LT(f_3) \in \langle LT(f_2), LT(f_3), LT(f_4), LT(f_5) \rangle$

$\overset{10.3}{\Rightarrow}$ f_1 kann als Erzeuger weggelassen werden

$LT(f_2) = X^2Y = -Y\,LT(f_3) \in \langle LT(f_3), LT(f_4), LT(f_5) \rangle$

$\overset{10.3}{\Rightarrow}$ f_2 kann als Erzeuger weggelassen werden.

Weitere f_i können nicht weggelassen werden (wg. $LT(f_3) = -X^2$, $LT(f_4) = -2XY$, $LT(f_5) = -2Y^2$)

Setze $\tilde{f}_3 := X^2$, $\tilde{f}_4 := XY$, $\tilde{f}_5 := Y^2 - \frac{1}{2}X$

$\Rightarrow \{\tilde{f}_3, \tilde{f}_4, \tilde{f}_5\}$ ist eine minimale Gröbnerbasis von J.

Ist $a \in \mathbb{R}$, dann ist auch $\{\hat{f}_3, \hat{f}_4, \hat{f}_5\}$ mit $\hat{f}_3 := X^2 + aXY$, $\hat{f}_4 := XY$, $\hat{f}_5 := Y^2 - \frac{1}{2}X$ eine minimale Gröbnerbasis von J.

Denn: Offenbar ist $J = \langle \hat{f}_3, \hat{f}_4, \hat{f}_5 \rangle = \langle \tilde{f}_3, \tilde{f}_4, \tilde{f}_5 \rangle$, und

$$LT(J) = \langle LT(\tilde{f}_3), LT(\tilde{f}_4), LT(\tilde{f}_5) \rangle = \langle LT(\hat{f}_3), LT(\hat{f}_4), LT(\hat{f}_5) \rangle.$$

Insbesondere hat J unendlich viele minimale Gröbnerbasen.

Algorithmus 10.6: K Körper, $f_1, \dots, f_s \in K[X]$, $J = \langle f_1, \dots, f_s \rangle$

Dann gilt: „J besitzt eine minimale Gröbnerbasis." Der folgende Algorithmus liefert eine minimale Gröbnerbasis von J

Eingabe: $F = \{f_1, \dots, f_s\}$

Algorithmus: $G := \text{Gröbnerbasis}(F)$

$H := G$

FOR g in H DO

IF $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$ THEN $G := G \setminus \{g\}$

END FOR

FOR g in G DO $g := g/LC(g)$ END FOR

Ausgabe: Minimale Gröbner Basis $(F) := G$

Bew.: klar.

Bem. 10.7: K Körper, $J \subset K[X]$ Ideal, $G, \tilde{G}$ minimale Gröbnerbasen von J.

Dann gilt:

(a) $LT(G) = LT(\tilde{G})$

(b) $G, \tilde{G}$ haben dieselbe Elementanzahl.

Bew.: Sei $G = \{g_1, \dots, g_s\}$, $\tilde{G} = \{\tilde{g}_1, \dots, \tilde{g}_t\}$, o.E. $s \leq t$.

Für alle $i \in \{1, \dots, s\}$ ist dann $LT(g_i) \in \langle LT(G) \rangle = LT(J) = \langle LT(\tilde{G}) \rangle$

$\Rightarrow \forall i \in \{1, \dots, s\}\ \exists j_i \in \{1, \dots, t\} : LT(\tilde{g}_{j_i}) \mid LT(g_i)$

$\Rightarrow LT(J) = \langle LT(g_1), \dots, LT(g_s) \rangle \subset \langle LT(\tilde{g}_{j_1}), \dots, LT(\tilde{g}_{j_r}) \rangle$

$\subset \langle LT(\tilde{g}_1), \dots, LT(\tilde{g}_t) \rangle = LT(J)$

$\Rightarrow \langle LT(\tilde{g}_{j_1}), \dots, LT(\tilde{g}_{j_s}) \rangle = \langle LT(\tilde{g}_1), \dots, LT(\tilde{g}_t) \rangle$

Da $\tilde{G}$ minimale Gröbnerbasis von J ist, folgt $\{j_1,\dots,j_s\} = \{1,\dots,t\}$

(insb. $s=t$ ($\Rightarrow$(b))

Es ist also $\tilde{G} = \{\tilde{g}_1,\dots,\tilde{g}_s\}$, und nach Umnummerieren von $\tilde{G}$ können wir annehmen: $LT(\tilde{g}_i) \mid LT(g_i)$ für $i=1,\dots,s$.

Aus Symmetriegründen ex. für jedes $i\in\{1,\dots,s\}$ ein $k_i\in\{1,\dots,s\}$ mit $LT(g_{k_i}) \mid LT(\tilde{g}_i)$

$\Rightarrow LT(g_{k_i}) \mid LT(\tilde{g}_i) \mid LT(g_i)$

Da G minimale Gröbnerbasis von J ist, folgt $LT(g_{k_i}) = LT(g_i)$

$\Rightarrow LT(g_i) \mid LT(\tilde{g}_i) \mid LT(g_i)$ ✱

$\Rightarrow LT(g_i) = LT(\tilde{g}_i)$ für alle $i\in\{1,\dots,s\}$

$\Rightarrow LT(G) = LT(\tilde{G})$. □

Def. 10.8: K Körper, $J\subset K[X]$ Ideal, G Gröbnerbasis von J

G heißt reduzierte Gröbnerbasis von J, wenn die folgenden Bedingungen erfüllt sind:

(a) $LC(p) = 1$ für alle $p\in G$

(b) Für alle $p\in G$ liegt kein Monom von p in $\langle LT(G\setminus\{p\})\rangle$

Anm.: Insbesondere ist eine reduzierte Gröbnerbasis stets eine minimale Gröbnerbasis.

Bsp. 10.9: (vgl. Bsp. 10.5)

$\{X^2, XY, Y^2 - \frac{1}{2}X\}$ ist eine reduzierte Gröbnerbasis von J aus Bsp. 10.5,

$\{X^2+XY, XY, Y^2-\frac{1}{2}X\}$ ist keine reduzierte Gröbnerbasis von J

Satz 10.10: K Körper, $J\subset K[X]$ Ideal, „$\leq$" Monomordnung auf $K[X]$.

Dann gilt: J besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Bew.: Existenz: Sei G eine minimale Gröbnerbasis von J.

Wir nennen $g \in G$ reduziert bzgl. G, wenn kein Monom von g in $\langle LT(G \setminus \{g\}) \rangle$ liegt.

Ziel: G so modifizieren, daß alle Elemente von G reduziert bzgl. G sind

① $g \in G$ reduziert bzgl. $G \Rightarrow g$ ist reduziert bzgl. jeder anderen Gröbnerbasis von J, welche g enthält und dieselbe Menge an Leitkoeffizienten hat (klar)

② Für $g \in G$ setze $g' := \bar{g}^{G \setminus \{g\}}$, $G' := (G \setminus \{g\}) \cup \{g'\}$

Beh.: G' ist eine minimale Gröbnerbasis von J, g' ist reduziert bzgl. G'

Bew.: Sei $G = \{g, g_1, \ldots, g_s\}$. Da G eine minimale Gröbnerbasis von J ist, ist $LT(g)$ durch keinen der Terme $LT(g_1), \ldots, LT(g_s)$ teilbar.

$\Rightarrow$ Im Algorithmus 6.1 zur Bestimmung von $\bar{g}^{\{g_1, \ldots, g_s\}}$ wird als erstes ein Restschritt ausgeführt; $LT(g)$ geht in den Rest der Division. Im weiteren Verlauf des Divisionsalgorithmus kommen nur noch Terme von kleinerem Multigrad dazu.

$\Rightarrow LT(g') = LT(g)$

$\Rightarrow \langle LT(G) \rangle = \langle LT(G') \rangle$

Es ist $g' \in J$ wg. $G \subset J \Rightarrow G' \subset J$

$\Rightarrow G'$ ist Gröbnerbasis von J mit $|G| = |G'| \Rightarrow G'$ ist minimale Gröbnerbasis von J

Nach Konstruktion liegt kein Monom von $g' = \bar{g}^{G \setminus \{g\}}$ in $LT(G \setminus \{g\}) = LT(G' \setminus \{g'\})$

$\Rightarrow g'$ reduziert bzgl. G'

③ Wende obigen Prozeß nacheinander auf die Elemente von G an, bis alle reduziert sind.

Dabei kann sich die Gröbnerbasis ändern; die Leitterme der Gröbnerbasis bleiben jedoch erhalten. Wegen ④ bleibt jedes reduzierte Element bei Abänderung der Gröbnerbasis reduziert.

Obiger Prozeß liefert also nach endlich vielen Schritten eine reduzierte Gröbnerbasis von J.

Eindeutigkeit: Seien $G, \tilde{G}$ reduzierte Gröbnerbasen von J

$\Rightarrow G, \tilde{G}$ sind minimale Gröbnerbasen von J

$\overset{10.7}{\Rightarrow} LT(G) = LT(\tilde{G})$

Sei $g \in G \Rightarrow$ Es ex. ein eind. best. $\tilde{g} \in \tilde{G}$ mit $LT(g) = LT(\tilde{g})$

Beh.: $g = \tilde{g}$ ($\Rightarrow G \subset \tilde{G}$; aus Symmetriegr. folgt $G = \tilde{G}$)

Bew.: Es ist $g - \tilde{g} \in J \overset{\substack{G \text{ Gröbner-} \\ \text{basis von } J \\ (9.2)}}{\Rightarrow} \overline{g - \tilde{g}}^{G} = 0$

Kein Monom von g ist durch einen der Terme aus $LT(G \setminus \{g\})$ teilbar,

-11- $\tilde{g}$ -11- $LT(\tilde{G} \setminus \{\tilde{g}\})$ -11-

Wegen $LT(g) = LT(\tilde{g})$ heben sich diese Leitterme in $g - \tilde{g}$ auf

$\Rightarrow$ Kein Monom von $g - \tilde{g}$ ist durch einen der Terme aus $LT(G) = LT(\tilde{G})$ teilbar.

$\Rightarrow \overline{g - \tilde{g}}^{G} = g - \tilde{g} \Rightarrow g - \tilde{g} = 0 \Rightarrow g = \tilde{g}$. □

Algorithmus 10.11: K Körper, $f_1, \dots, f_s \in K[X]$, $J = \langle f_1, \dots, f_s \rangle$.
Dann gilt: Der folgende Algorithmus liefert eine reduzierte Gröbnerbasis von J.

Eingabe: $F = \{f_1, \dots, f_s\}$

Algorithmus: $G :=$ Minimale Gröbnerbasis (F)

$H := G$

FOR $g \in H$ DO

$g' := \bar{g}^{G \setminus \{g\}}$

$G := (G \setminus \{g\}) \cup \{g'\}$

END FOR

Ausgabe: ReduzierteGröbnerbasis$(F) := G$

Bew.: aus dem Bew. von 10.10. □

Bsp. 10.12: $f_1 = XZ - Y^2$, $f_2 = X^3 - Z^2 \in \mathbb{C}[X,Y,Z]$, $J = \langle f_1, f_2 \rangle$, „$\geq$"$_{grlex}$ als Monomordnung

Algorithmus 10.11 liefert folgendes.

Setze $f_3 := X^2Y^2 - Z^3$, $f_4 := XY^4 - Z^4$, $f_5 := Y^6 - Z^5$, dann ist

$G = \{f_1, f_2, f_3, f_4, f_5\}$ eine reduzierte Gröbnerbasis von J.

Diese kann z.B. benutzt werden, um über Idealmitgliedschaft zu entscheiden:

- Ist $f = -4X^2Y^2Z^2 + Y^6 + 3Z^5$, dann ist $f = -4Z^2 f_3 + f_5 \in J$
- Ist $f = XY - 5Z^2 + X$, dann ist $XY = LT(f) \notin \langle LT(f_1), \dots, LT(f_5) \rangle = \langle XZ, X^3, X^2Y^2, XY^4, Y^6 \rangle = LT(J)$

$\Rightarrow f \notin J$.

Folgerung 10.13: K Körper, $f_1, \dots, f_s \in K[\underline{X}]$, $J = \langle f_1, \dots, f_s \rangle$, $J = \langle g_1, \dots, g_t \rangle$, „$\geq$" Monomordnung auf $K[\underline{X}]$.

Dann sind äquivalent:

(i) $J = J$

(ii) J, J haben dieselbe reduzierte Gröbnerbasis bzgl. „$\geq$"

Bew.: folgt sofort aus Satz 10.11. □

Kapitel III. Eliminationstheorie

§11. Eliminations- und Fortsetzungssatz

Bsp. 11.1: Sei $f_1 = X^2+Y+Z-1, f_2 = X+Y^2+Z-1, f_3 = X+Y+Z^2-1 \in \mathbb{C}[X,Y,Z]$, $J = \langle f_1, f_2, f_3\rangle$. Wir möchten die Varietät

$$V(f_1,f_2,f_3) = \{(x,y,z)\in\mathbb{C}^3 \mid x^2+y+z=1,\ x+y^2+z=1,\ x+y+z^2=1\}$$

explizit bestimmen, d.h. das algebraische Gleichungssystem $f_1=0, f_2=0, f_3=0$ lösen.

Bezüglich „$\geq_{lex}$" ist eine Gröbnerbasis von J gegeben durch $G=\{g_1,g_2,g_3,g_4\}$ mit $g_1 = X+Y+Z^2-1$, $g_2 = Y^2-Y-Z^2+Z$, $g_3 = 2YZ^2+Z^4-Z^2$, $g_4 = Z^6-4Z^4+4Z^3-Z^2$.

Es ist $V(f_1,f_2,f_3) = V(g_1,g_2,g_3,g_4)$. Wegen $g_4 = Z^2(Z-1)^2(Z^2+2Z-1)$ sind für Elemente $(x,y,z)\in V(f_1,f_2,f_3)$ die einzig möglichen Werte für z gegeben durch $0, 1, -1\pm\sqrt{2}$. Substitution dieser Werte in $g_2=0, g_3=0$ liefert die möglichen Werte für y, Substitution in $g_1=0$ liefert schließlich die Werte für x.

Wir erhalten

$$V(f_1,f_2,f_3) = \{(1,0,0),(0,1,0),(0,0,1),(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}),(-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2})\}$$

Die Lösung des obigen Gleichungssystemes erfolgte in zwei Schritten:

- Eliminationsschritt: Wir haben eine Konsequenz der Ausgangsgleichungen gefunden, die nur die Variable Z involviert: $g_4 \in J\cap\mathbb{C}[Z]$
- Fortsetzungsschritt: Nach Lösung der Gleichung $g_4=0$ konnten die so gefundenen Lösungen für z zu Lösungen der Ausgangsgleichung fortgesetzt werden.

In diesem Kapitel werden wir zeigen, daß diese Schritte in größerer Allgemeinheit funktionieren.

Def.+Bem. 11.2: K Körper, $f_1,\dots,f_s \in K[X_1,\dots,X_n]$, $J = \langle f_1,\dots,f_s\rangle$, $m \in \{0,1,\dots,n-1\}$, „$\geq$" Monomordnung auf $K[X_1,\dots,X_n]$, $i_1,\dots,i_n \in \{1,\dots,n\}$ sd. $X_{i_1} > X_{i_2} > \dots > X_{i_n}$.

Dann gilt:

$$J_m := J \cap K[X_{i_{m+1}},\dots,X_{i_n}]$$

ist ein Ideal in $K[X_{i_{m+1}},\dots,X_{i_n}]$. J_m heißt das <u>m-te Eliminationsideal</u> von J.

<u>Anm.:</u> In J_m sind die höchsten m Variablen eliminiert.

<u>Bew. von Bem. 11.2:</u> ① $0 \in J_m$: klar

② Seien $f,g \in J_m \Rightarrow f,g \in J$ und $f,g \in K[X_{i_{m+1}},\dots,X_{i_n}]$
$\overset{J \text{ Ideal}}{\Rightarrow} f+g \in J$ und $f+g \in K[X_{i_{m+1}},\dots,X_{i_n}]$
$\Rightarrow f+g \in J_m$

③ Seien $f \in J_m$, $h \in K[X_{i_{m+1}},\dots,X_{i_n}] \Rightarrow f \in J$ und $f,h \in K[X_{i_{m+1}},\dots,X_{i_n}]$
$\overset{J \text{ Ideal}}{\Rightarrow} hf \in J$ und $hf \in K[X_{i_{m+1}},\dots,X_{i_n}]$
$\Rightarrow hf \in J_m$. □

Bem. 11.3: K Körper, $J \subset K[X_1,\dots,X_n]$ Ideal, $m \in \{0,\dots,n-2\}$. Dann gilt:

$$J_{m+1} = (J_m)_1$$

<u>Bew.:</u> Seien $i_1,\dots,i_n \in \{1,\dots,n\}$ mit $X_{i_1} > X_{i_2} > \dots > X_{i_n}$.

Dann ist

$$J_{m+1} = J \cap K[X_{i_{m+2}},\dots,X_{i_n}] = (\underbrace{J \cap K[X_{i_{m+1}},\dots,X_{i_n}]}_{\subset K[X_{i_{m+1}},\dots,X_{i_n}] \text{ (Variablen: } X_{i_{m+1}} > \dots > X_{i_n})}) \cap K[X_{i_{m+2}},\dots,X_{i_n}]$$
$$= (J_m)_1.$$ □

Satz 11.4: (Eliminationssatz) K Körper, $J \subset K[X_1,\dots,X_n]$ Ideal, G Gröbnerbasis von J bzgl. „$\geq_{lex}$" (mit $X_1 >_{lex} X_2 >_{lex} \dots >_{lex} X_n$), $m \in \{0,\dots,n-1\}$. Dann gilt:

$$G_m := G \cap K[X_{m+1},\dots,X_n]$$

ist eine Gröbnerbasis des m-ten Eliminationsideals $J_m = J \cap K[X_{m+1},\dots,X_n]$.

Bew.: Offenbar ist $G_m = G \cap K[X_{m+1}, \dots, X_n] \subset J \cap K[X_{m+1}, \dots, X_n] = J_m$.

Es genügt also zz.: $LT(J_m) = \langle LT(G_m) \rangle$

„$\supseteq$" ist trivial,

„$\subseteq$": Sei $f \in J_m$. Wir müssen zeigen: Es ex. ein $g \in G_m$ mit $LT(g) \mid LT(f)$.

Bew.:
Wegen $f \in J_m \subset J$ ex. ein $g \in G$ mit $LT(g) \mid LT(f)$, da G Gröbnerbasis von J.

$f \in J_m \Rightarrow LT(g)$ involviert nur die Variablen $X_{m+1}, \dots, X_n$.

Da wir „$>_{lex}$" (mit $X_1 >_{lex} X_2 >_{lex} \dots >_{lex} X_n$) verwenden, folgt: $g \in K[X_{m+1}, \dots, X_n]$

$\Rightarrow g \in G_m$. □

Bsp. 11.5: (vgl. Bsp. 11.1) $J = \langle X^2+Y+Z-1, X+Y^2+Z-1, X+Y+Z^2-1 \rangle \subset \mathbb{C}[X,Y,Z]$

Gröbnerbasis $G = \{g_1, g_2, g_3, g_4\}$ bzgl. „$>_{lex}$" wie in Bsp. 11.1

Nach dem Eliminationssatz ist

$$J_1 = J \cap \mathbb{C}[Y,Z] = \langle G \cap \mathbb{C}[Y,Z] \rangle = \langle g_2, g_3, g_4 \rangle$$

$$J_2 = J \cap \mathbb{C}[Z] = \langle G \cap \mathbb{C}[Z] \rangle = \langle g_4 \rangle \; (= \langle Z^6 - 4Z^4 + 4Z^3 - Z^2 \rangle)$$

Insbes. ist jedes andere Polynom aus J, in dem X, Y eliminiert sind, ein Vielfaches von g_4.

Def. 11.6: K Körper, $f_1, \dots, f_s \in K[X_1, \dots, X_n]$, $J = \langle f_1, \dots, f_s \rangle$, $m \in \{0, \dots, n-1\}$

$(a_{m+1}, \dots, a_n) \in V(J_m) \subset K^{n-m}$

heißt partielle Lösung der Stufe $n-m$ bzgl. J (oder auch: partielle Lösung der Stufe m des Gleichungssystems $f_1 = \dots = f_s = 0$).

Eine partielle Lösung der Stufe n heißt vollständige Lösung.

Anm.: Wir wollen partielle Lösungen $(a_{m+1}, \dots, a_n) \in V(J_m)$ durch sukzessives Hinzufügen jeweils einer weiteren Koordinate fortsetzen zu vollständigen Lösungen.

Wir müssen also zunächst $a_m \in K$ bestimmen, so daß $(a_m, a_{m+1}, \dots, a_n) \in V(J_{m-1})$

Ist $J_{m-1} = \langle h_1, \dots, h_r \rangle \subset K[X_m, \dots, X_n]$, müssen wir dazu

die Lösungen der Gleichungen

$$h_1(X_m, a_{m+1}, \dots, a_n) = \dots = h_r(X_m, a_{m+1}, \dots, a_n)$$

bestimmen.

Problem: Die $h_i(X_m, a_{m+1}, \dots, a_n)$ haben u.U. gar keine gemeinsame Nullstelle m.a.W.: nicht jede partielle Lösung wird sich zu einer vollständigen Lösung ausdehnen lassen.

Bsp. 11.7: Sei $f_1 = XY-1$, $f_2 = XZ-1 \in \mathbb{R}[X,Y,Z]$, $J = \langle f_1, f_2 \rangle$

Eine Gröbnerbasis von J bzgl. $\geq_{lex}$ ist gegeben durch $G = \{XZ-1, Y-Z\}$.

Insbes. ist $J_1 = J \cap \mathbb{R}[Y,Z] = \langle Y-Z \rangle$

Die Menge der partiellen Lösungen der Stufe 2 bzgl. J ergibt sich zu

$$V(J_1) = \{(y,z) \in \mathbb{R}^2 \mid y = z\} = \{(a,a) \in \mathbb{R}^2 \mid a \in \mathbb{R}\}$$

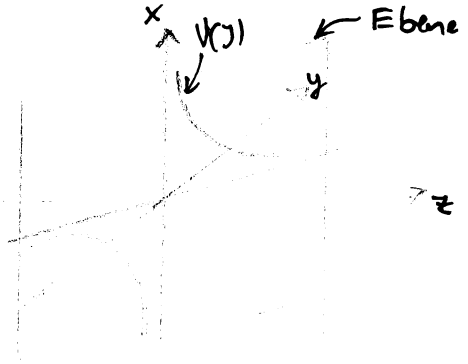
Es ist $J_0 = J = \langle XZ-1, Y-Z \rangle$. Ist $(x,a,a) \in \mathbb{R}^3$ eine vollständige Lösung bzgl. J, dann ist x Nullstelle des Polynoms

$$Xa-1 \in \mathbb{R}[X].$$

Offenbar setzt sich jede partielle Lösung (a,a) mit $a \neq 0$ zu einer vollständigen Lösung $(\frac{1}{a}, a, a)$ fort, die partielle Lösung $(0,0)$ setzt sich nicht fort.

geometrische Sicht: $V(J_1) = V(Y-Z)$ def. eine Ebene im $\mathbb{R}^3$

$V(J) = V(XZ-1, Y-Z) = V(XZ-1) \cap V(Y-Z)$ ist eine Hyperbel in dieser Ebene:



$V(J)$ hat keine Punkte über $(0,0)$.

Satz 11.8: (Fortsetzungssatz) $f_1,\dots,f_s \in \mathbb{C}[X_1,\dots,X_n]$, $J = \langle f_1,\dots,f_s\rangle$,
schreibe für alle $i\in\{1,\dots,s\}$ f_i in der Form

$$f_i = g_i(X_2,\dots,X_n)X_1^{N_i} + \text{Terme von } X_1\text{-Grad} < N_i$$

mit $N_i \geq 0$, $g_i \in \mathbb{C}[X_2,\dots,X_n]$, $g_i \neq 0$ (Falls $f_i = 0$, setze $g_i := 0$).
Dann gilt:
Ist $(a_2,\dots,a_n) \in V(J_1)$ eine partielle Lösung der Stufe $n-1$ bzgl J
mit $(a_2,\dots,a_n) \notin V(g_1,\dots,g_s)$, dann ex. ein $a_1 \in \mathbb{C}$, sd. $(a_1,\dots,a_n) \in V(J)$,
(d.h. $(a_2,\dots,a_n)$ kann zu einer vollständigen Lösung fortgesetzt werden).

Bew.: später.

Bsp. 11.9: vgl. Bsp. 11.7: $f_1 = XY-1$, $f_2 = XZ-1 \in \mathbb{C}[X,Y,Z]$
Es ist $f_1 = Y\cdot X - 1$, d.h. $g_1 = Y$,
$f_2 = Z\cdot X - 1$, d.h. $g_2 = Z$
Alle partiellen Lösungen (a,a), $a\in\mathbb{C}$ der Stufe 2 bzgl. $J = \langle f_1,f_2\rangle$ (vgl. 11.7)
mit $(a,a) \notin V(Y,Z) = \{(0,0)\}$ setzen sich nach 11.8 fort zu vollst. Lösungen.

Anm.: $V(g_1,\dots,g_s)$ in 11.8 hängt von der Wahl von $f_1,\dots,f_s$ ab.

Bsp. 11.10: Es sei $f_1 = X^2 - Y$, $f_2 = X^2 - Z \in \mathbb{C}[X,Y,Z]$, $J = \langle f_1,f_2\rangle$
Es ist $J_1 = \langle Y-Z\rangle$. Partielle Lösungen der Stufe 2 bzgl. J sind somit
von d. Form (a,a), $a\in\mathbb{C}$.
Es ist $f_1 = 1\cdot X^2 - Y$, $f_2 = 1\cdot X^2 - Z$, also $g_1 = 1$, $g_2 = 1$, insb. $V(g_1,g_2) = \emptyset$
Damit setzt sich nach 11.8 jede partielle Lösung $(a,a),a\in\mathbb{C}$ zu einer vollständigen Lösung fort.
(nämlich zu $(\pm\sqrt{a},a,a)$)
Über $\mathbb{R}$ ist das falsch: Hier setzen sich nur partielle Lösungen (a,a)
mit $a \geq 0$ zu vollständigen Lösungen fort, denn $X^2 - a = 0$ hat genau
dann Lösungen, wenn $a \geq 0$.
Also: Die Voraussetzung $K = \mathbb{C}$ ist essentiell in Satz 11.8

Bsp. 11.11: Es sei $f_1 = X^2+Y^2+Z^2-1$, $f_2 = XYZ-1 \in \mathbb{C}[X,Y,Z]$, $J = \langle f_1, f_2, f_3 \rangle$.

Eine Gröbnerbasis von J bzgl. „$\overrightarrow{lex}$" ist gegeben durch $G = \{h_1, h_2\}$ mit

$$h_1 = Y^4Z^2 + Y^2Z^4 - Y^2Z^2 + 1, \quad h_2 = X + Y^3Z + YZ^3 - YZ$$

Mit dem Eliminationssatz erhalten wir

$$J_1 = J \cap \mathbb{C}[Y,Z] = \langle h_1 \rangle$$

$$J_2 = J \cap \mathbb{C}[Z] = \{0\}$$

Welche partiellen Lösungen $c \in V(J_2) = \mathbb{C}$ erster Stufe bzgl. J setzen sich zu vollständigen Lösungen $(a,b,c) \in V(J)$ fort?

Wir werden dazu den Fortsetzungssatz zweimal anwenden.

1. Schritt: von J_2 nach $J_1 = \langle h_1 \rangle$

$h_1 = Z^2 \cdot Y^4 +$ Terme von kleinerem Y-Grad

$\Rightarrow$ Jede partielle Lösung $c \in V(J_2) = \mathbb{C}$ mit $c \notin V(Z^2) = \{0\}$ setzt sich fort zu einer vollständigen Lösung $(b,c) \in V(J_1)$ bzgl. J_1. (= partielle Lösung zweiter Stufe bzgl. J).

$h_1(Y,0)$ besitzt keine Nullstelle, d.h. $0 \in V(J_2)$ setzt sich nicht zu einer wollst. Lösung bzgl. J_1 fort.

2. Schritt: von J_1 nach $J_0 = J$

Sei $(b,c) \in V(J_1)$, $c \neq 0$

Es ist $f_1 = 1 \cdot X^2 +$ Terme ohne X, $f_2 = YZ \cdot X - 1$

$\Rightarrow$ Jede partielle Lösung $(b,c) \in V(J_1)$ zweiter Stufe bzgl. J mit $(b,c) \notin V(1, YZ) = \emptyset$ setzt sich fort zu einer vollständigen Lösung $(a,b,c) \in V(J)$.

Wir erhalten insgesamt: Jede partielle Lösung $c \in V(J_2) = \mathbb{C}$, $c \neq 0$, bzgl. J setzt sich fort zu einer vollständigen Lösung $(a,b,c) \in V(J)$.

Folgerung 11.12: $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$, $J = \langle f_1, \dots, f_s \rangle$.

Es existiere ein $i \in \{1, \dots, s\}$, sd. f_i von der Form

$$f_i = c X_1^N + \text{Terme von kleinerem } X_1\text{-Grad}$$

mit $c \in \mathbb{C}$, $c \neq 0$. Dann gilt:

Ist $(a_2, \dots, a_n) \in V(J_1)$ eine partielle Lösung a. Stufe $n-1$ bzgl. J, dann ex. ein $a_1 \in \mathbb{C}$ mit $(a_1, a_2, \dots, a_n) \in V(J)$.

Bew.: folgt aus dem Fortsetzungssatz: In der Notation von 11.8 ist

$$g_i = c, \text{ und } V(g_1, \dots, c, \dots, g_s) = \emptyset, \text{ d.h. } a_2 \notin V(g_1, \dots, g_s). \qquad \square$$

Bsp. 11.13: $f_1 = XY - 4$, $f_2 = Y^2 - X^3 + 1 \in \mathbb{C}[X, Y]$

Eine Gröbnerbasis von $\langle f_1, f_2 \rangle$ bzgl. $\succ_{lex}$ ist gegeben durch $G = \{g_1, g_2\}$ mit $g_1 = 16X - Y^2 - Y^4$, $g_2 = Y^5 + Y^3 - 64$

D.h. $J_1 = \langle g_2 \rangle$, $V(g_2) = \{y \in \mathbb{C} \mid y^5 + y^3 - 64 = 0\}$ kann nur numerisch bestimmt werden, $V(J)$ entsprechend auch.

§12. Die Geometrie der Elimination

Bem 12.1: K Körper, $f_1, \dots, f_s \in K[X_1, \dots, X_n]$, $J = \langle f_1, \dots, f_s \rangle$, $V := V(J) \subset K^n$, $m \in \{0, \dots, n-1\}$, $\pi_m : K^n \longrightarrow K^{n-m}$ sei die Projektionsabb. auf die letzten $n-m$ Komponenten: $\pi_m(a_1, \dots, a_n) = (a_{m+1}, \dots, a_n)$, $J_m = J \cap K[X_{m+1}, \dots, X_n]$.

Dann gilt: $\pi_m(V) \subset V(J_m)$.

Bew.: Sei $f \in J_m$, $(a_1, \dots, a_n) \in V \overset{f \in J_m \subset J}{\Longrightarrow} f(a_1, \dots, a_n) = 0$

Wegen $f \in J_m$ können wir f auch als Polynom in den Variablen $X_{m+1}, \dots, X_n$ auffassen und erhalten

$$f(a_{m+1}, \dots, a_n) = f(\pi(a_1, \dots, a_n)) = 0$$

$\Rightarrow \pi(a_1, \dots, a_n) \in V(J_m)$. $\square$

Anm: Es ist $\pi_m(V) = \{(a_{m+1}, \dots, a_n) \in V(J_m) \mid$ Es ex. $a_1, \dots, a_m \in K$ mit $(a_1, \dots, a_m, a_{m+1}, \dots, a_n) \in V\}$,

d.h. $\pi_m(V)$ ist genau die Menge der partiellen Lösungen $(n-m)$-ter Stufe bzgl. J, die sich zu vollständigen Lösungen bzgl. J fortsetzen lassen.

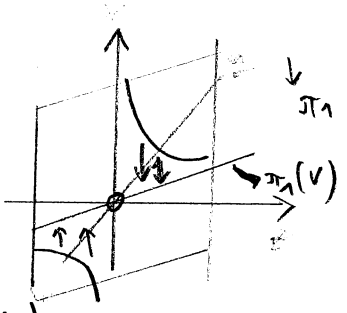
Bsp. 12.2: vgl. Bsp. 11.7, 11.9: $f_1 = XY - 1$, $f_2 = XZ - 1 \in \mathbb{C}[X, Y, Z]$ bzgl. $\geq_{lex}$.

$J = \langle f_1, f_2 \rangle$, $V = V(J)$.

Es ist $J_1 = \langle Y - Z \rangle$, $V(J_1) = \{(a, a) \mid a \in \mathbb{C}\}$,

$V = V(J) = \{(\frac{1}{a}, a, a) \mid a \in \mathbb{C}, a \neq 0\}$

$\Rightarrow \pi_1(V) = \{(a, a) \in \mathbb{C}^2 \mid a \neq 0\}$



Insb. ist $\pi_1(V)$ keine affine Varietät (Nullpunkt fehlt.)

Satz 12.3: (Fortsetzungssatz, Geometrische Formulierung) $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$, $J = \langle f_1, \dots, f_s \rangle$. Schreibe für alle $i \in \{1, \dots, s\}$ f_i in der Form

$$f_i = g_i(X_2, \dots, X_n) X_1^{N_i} + \text{Terme von } X_1\text{-Grad} < N_i$$

mit $N_i \geq 0$, $g_i \in \mathbb{C}[X_2, \dots, X_n]$, $g_i \neq 0$ (Falls $f_i = 0$, setze $g_i = 0$).

Es sei ferner $\pi_1 : \mathbb{C}^n \longrightarrow \mathbb{C}^{n-1}$, $(a_1, \dots, a_n) \mapsto (a_2, \dots, a_n)$.

Dann gilt:

$$V(J_1) = \pi_1(V) \cup (V(g_1, \dots, g_s) \cap V(J_1)).$$

Bew.: „$\supset$" $\pi_1(V) \subset V(J_1)$ nach Bem. 12.1, $V(g_1, \dots, g_s) \cap V(J_1) \subset V(J_1)$ klar.

„$\subset$" Sei $(a_2, \dots, a_n) \in V(J_1)$, dh. $(a_2, \dots, a_n)$ ist eine partielle Lösung d. Stufe $n-1$ bzgl. J. Falls $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s) \cap V(J_1)$, dann kann $(a_2, \dots, a_n)$ nach dem Fortsetzungssatz (11.8) zu einer vollst. Lösung bzgl. J fortgesetzt werden, dh. $(a_2, \dots, a_n) \in \pi_1(V)$ (vgl. Anm. nach 12.1) $\Rightarrow$ Beh. $\square$

Folgerung 12.4: $f_1,\dots,f_s \in \mathbb{C}[X_1,\dots,X_n]$, $J = \langle f_1,\dots,f_s\rangle$. ~~Schreibe für alle $i \in \{1,\dots,s\}$~~

Es existiere ein $i \in \{1,\dots,s\}$, sd.

$$f_i = c X_1^N + \text{Terme von kleinerem } X_1\text{-Grad}$$

mit $c \in \mathbb{C}\setminus\{0\}, N > 0$.

Dann gilt: $\pi_1(V) = V(J_1)$.

Bew.: In d. Not. von 12.3 ist $g_i = c \Rightarrow V(g_1,\dots,\overset{c}{g_i},\dots,g_n) = \emptyset$

$\overset{12.3}{\Rightarrow} V(J_1) = \pi_1(V)$. □

Bsp. 12.5: Sei $f_1 = (Y-Z)X^2 + XY - 1$, $f_2 = (Y-Z)X^2 + XZ - 1 \in J \subset \mathbb{C}[X,Y,Z]$, $J := \langle f_1, f_2\rangle$

Man kann zeigen: $J = \langle XY-1, XZ-1\rangle$ (vgl. Bsp. 11.7, 11.9),

insbes. ist $J_1 = \langle Y-Z\rangle$.

In d. Not. von 12.3 ist $g_1 = g_2 = Y-Z$, d.h. $V(g_1,g_2) = V(J_1)$

Die Aussage von 12.3 ist in diesem Fall $V(J_1) = \pi_1(V) \cup V(J_1)$,

d.h. man kann nichts über $\pi_1(V)$ folgern.

Satz 12.6: (Satz vom Abschluß) $f_1,\dots,f_s \in \mathbb{C}[X_1,\dots,X_n]$, $J := \langle f_1,\dots,f_s\rangle$, $m \in \{0,\dots,n-1\}$,

$V := V(J)$, $J_m := J \cap \mathbb{C}[X_{m+1},\dots,X_n]$. Dann gilt:

(a) $V(J_m)$ ist die kleinste aff. Varietät in $\mathbb{C}^{n-m}$, die $\pi_m(V)$ enthält, d.h.

- $\pi_m(V) \subset V(J_m)$
- Ist $Z \subset \mathbb{C}^{n-m}$ eine affine Varietät mit $Z \supset \pi_m(V)$, dann ist $V(J_m) \subset Z$

(b) Falls $V \neq \emptyset$, dann ex. eine affine Varietät $W \subsetneq V(J_m)$, sd.

$V(J_m) \setminus W \subset \pi_m(V)$.

Anm.: anschauliche Interpretation: $V(J_m)$ wird im wesentl. durch $\pi_m(V)$ ausgefüllt – bis auf Punkte, die auf einer echt kleineren affinen Varietät als $V(J_m)$ liegen.

Bew.: (a) später

(b) hier nur für $m=1$:

Nach 12.3 ist

$$V(J_1) = \pi_1(V) \cup \left(V(g_{11\cdots}, g_s) \cap V(J_1) \right)$$

mit $g_{11\cdots}, g_s$ wie in 12.3

Setze $W := V(g_{11\cdots}, g_s) \cap V(J_1)$; W ist affine Varietät wg. 2.8(a)

$\Rightarrow V(J_1) \setminus W \subset \pi_1(V)$

1.Fall: $W \neq V(J_1)$, dann fertig.

2.Fall: $W = V(J_1)$ (d.h. insbes. $V(g_{11\cdots}, g_s) \supset V(J_1)$)

① Beh: $V = V(f_{11\cdots}, f_s, g_{11\cdots}, g_s)$

Bew.: „$\supset$" Offenbar ist $V(f_{11\cdots}, f_s, g_{11\cdots}, g_s) \subset V(f_{11\cdots}, f_s) = V$

„$\subset$" Sei $(a_{11\cdots}, a_n) \in V \Rightarrow f_1(a_{11\cdots}, a_n) = \ldots = f_s(a_{11\cdots}, a_n) = 0$,

$(a_{2\cdots}, a_n) \in \pi_1(V) \overset{12.1}{\subset} V(J_1) = W \subset V(g_{11\cdots}, g_s)$

$\Rightarrow (a_{11\cdots}, a_n) \in V(f_{11\cdots}, f_s, g_{11\cdots}, g_s)$

② Setze $\tilde{J} := \langle f_{11\cdots}, f_s, g_{11\cdots}, g_s \rangle$.

Nach ① ist $V = V(J) = V(\tilde{J}) \overset{(a)}{\Rightarrow} V(J_1)$ und $V(\tilde{J}_1)$ ist jew. die kleinste aff-Varietäten in $\mathbb{C}^{n-m}$, die $\pi_1(V)$ enthält

$\Rightarrow V(J_1) = V(\tilde{J}_1)$.

Setze $\tilde{f}_i := f_i - g_i X_1^{N_i}$, $i = 1, \ldots, s$.

Nach Def. von g_i ist $\tilde{f}_i = 0$ oder $\tilde{f}_i$ hat kleineren Grad in X_1 als f_i.

Offenbar ist $\tilde{J} = \langle f_{11\cdots}, f_s, g_{11\cdots}, g_s \rangle \supset \langle \tilde{f}_{11\cdots}, \tilde{f}_s, g_{11\cdots}, g_s \rangle$,

umgekehrt ist $f_i = \tilde{f}_i + g_i X_1^{N_i} \in \langle \tilde{f}_{11\cdots}, \tilde{f}_s, g_{11\cdots}, g_s \rangle$, d.h.

$\tilde{J} \subset \langle \tilde{f}_{11\cdots}, \tilde{f}_s, g_{11\cdots}, g_s \rangle$

$\Rightarrow \tilde{J} = \langle \tilde{f}_{11\cdots}, \tilde{f}_s, g_{11\cdots}, g_s \rangle$

$\Rightarrow V(J_1) = V(\tilde{J}_1) \overset{12.3}{=} \pi_1(V) \cup \tilde{W}$

mit $\tilde{W} = V(h_1, \dots, h_s, g_1, \dots, g_s) \cap V(\tilde{J}_1) = V(h_1, \dots, h_s, g_1, \dots, g_s) \cap V(J_1)$,

wobei $f_i = h_i(X_2, \dots, X_n) X_1^{N_i} +$ Terme von kleinerem X_1-Grad, $i = 1, \dots, s$

($g_i = g_i(X_2, \dots, X_n) \cdot X_1^0$ für $i = 1, \dots, s$)

Falls $\tilde{W} \subsetneq V(J_1)$, dann fertig.

Dieser Prozeß wird iteriert. Falls irgendwann $\tilde{W} \subsetneq V(J_1)$, dann fertig.

③ Was passiert, wenn wir immer $W = V(J_1)$ erhalten?

Bei jedem Schritt in obiger Iteration sinken die X_1-Grade der Erzeuger von $\tilde{J}$ (oder bleiben Null).

Nach hinreichend vielen Iterationen erhalten wir

$V = V(\hat{f}_1, \dots, \hat{f}_t)$ *

mit $\hat{f}_1, \dots, \hat{f}_t \in \mathbb{C}[X_2, \dots, X_n]$.

Damit: Ist $(a_2, \dots, a_n)$ eine partielle Lsg. bzgl. J_1, dann ist

$(a_1, a_2, \dots, a_n) \in V$ für jedes $a_1 \in \mathbb{C}$

$\Rightarrow$ Jede partielle Lsg. setzt sich fort

$\Rightarrow \pi_1(V) = V(J_1)$

$V \neq \emptyset \Rightarrow W = \emptyset$ erfüllt die Beh. aus dem Satz. □

Bsp. 12.7: (vgl. Bsp. 12.5) $f_1 = (Y-Z)X^2 + XY - 1$, $f_2 = (Y-Z)X^2 + XZ - 1 \in \mathbb{C}[X,Y,Z]$

$J := \langle f_1, f_2 \rangle$, $V := V(f_1, f_2)$.

Es ist $J_1 = \langle Y-Z \rangle$, $g_1 = g_2 = Y-Z \Rightarrow W = V(g_1, g_2) \cap V(J_1) = V(J_1)$

Wie im Bew. von 12.5 erhalten wir

$\tilde{J} = \langle f_1, f_2, g_1, g_2 \rangle = \langle \tilde{f}_1, \tilde{f}_2, g_1, g_2 \rangle$ mit $\tilde{f}_1 = XY-1$, $\tilde{f}_2 = XZ-1$

$\Rightarrow \tilde{J} = \langle XY-1, XZ-1, Y-Z \rangle$.

Es ist $h_1 = Y$, $h_2 = Z \Rightarrow \tilde{W} = V(Y, Z, Y-Z) = \{(0,0)\} \subsetneq V(J_1)$.

Anm: • Man kann das folgende genauere Resultat zeigen:

Es gibt affine Varietäten $Z_i \subset W_i \subset \mathbb{C}^{n-m}$, s.d.

$$\pi_m(V) = \bigcup_{i=1}^{m} (W_i \setminus Z_i)$$

Man sagt dann auch, daß $\pi_m(V)$ konstruierbar ist.

• Der Satz vom Abschluß gilt über jedem algebraisch abgeschlossenen Körper K.

(Ein Körper K heißt algebraisch abgeschlossen, wenn jeder nichtkonstante Polynom aus $K[X]$ eine Nullstelle in K besitzt.)

§13. Implizitisierung

Anm: Gegeben seien Polynome $f_1, \dots, f_n \in K[t_1, \dots, t_m]$, $F: K^m \to K^n$ sei def. durch

$$F(a_1, \dots, a_m) := (f_1(a_1, \dots, a_m), \dots, f_n(a_1, \dots, a_m)).$$

Gesucht ist die kleinste affine Varietät in K^n, die $F(K^m)$ enthält.

Bsp. 13.1: In Bsp. 2.14 ist $f_1 = 1+t$, $f_2 = 1+t^2 \in \mathbb{C}[t]$. Wie oben sei

$F: \mathbb{C} \to \mathbb{C}^2$, $F(a) = (f_1(a), f_2(a)) = (1+a, 1+a^2)$.

Wir haben in 12.4 nachgerechnet: $F(\mathbb{C}) = V(Y - X^2 + 2X - 2) \subset \mathbb{C}^2$.

Wie geht das algorithmisch?

Satz 13.2: (Polynomiale Implizitisierung) $K \subset \mathbb{C}$ Körper, $f_1, \dots, f_n \in K[t_1, \dots, t_m]$,

$F: K^m \to K^n$, $F(a_1, \dots, a_m) := (f_1(a_1, \dots, a_m), \dots, f_n(a_1, \dots, a_m))$

Setze

$$J := \langle X_1 - f_1, \dots, X_n - f_n \rangle \subset K[t_1, \dots, t_m, X_1, \dots, X_n],$$

$J_m := J \cap K[X_1, \dots, X_m]$ (m-tes Eliminationsideal von J bzgl. $\succcurlyeq_{lex}$ auf $K[t_1, \dots, t_m, X_1, \dots, X_n]$ mit $t_1 > t_2 > \dots > t_m > X_1 > \dots > X_n$)

Dann gilt: $V(J_m)$ ist die kleinste Varietät in K^m, die $F(K^m)$ enthält.

Bsp. 13.3: (vgl. 13.1) $f_1 = 1+t, f_2 = 1+t^2 \in \mathbb{C}[t]$, F wie in 13.1

Setze $J := \langle X-(1+t), Y-(1+t^2)\rangle \subset \mathbb{C}[t,X,Y]$

Eine Gröbnerbasis von J (bzgl. „$\geq_{lex}$" mit $t > X > Y$) ist gegeben durch

$G = \{t - X + 1, X^2 - 2X - Y + 2\}$

Insbes. ist $J_1 = \langle X^2 - 2X - Y + 2\rangle \subset \mathbb{C}[X,Y]$.

$\overset{13.2}{\Rightarrow}$ $V(J_1) = V(X^2-2X-Y+2)$ ist die kleinste Varietät in $\mathbb{C}^2$, die $F(\mathbb{C})$ enthält. Ist $F(\mathbb{C}) = V(J_1)$?

M.a.W.: Gibt es zu $(x,y) \in V(J_1)$ stets ein $t \in \mathbb{C}$, sd. $F(t) = (x,y)$, d.h. $f_1(t) = x$, $f_2(t) = y$ ($\Leftrightarrow (t,x,y) \in V(J)$)

Äquivalent: Setzt sich jede partielle Lösung $(x,y) \in V(J_1)$ bzgl. J zu einer vollst. Lösung bzgl. J fort?

Es ist $J = \langle X-(1+t), Y-(1+t^2)\rangle = \langle \underbrace{(-1)}_{\in \mathbb{C}\setminus\{0\}}\cdot t + X - 1, \underbrace{(-1)}_{\in \mathbb{C}\setminus\{0\}} t^2 + (Y-1)\rangle$

$\overset{11.12}{\Rightarrow}$ Jede partielle Lösung setzt sich fort.

Also: $F(\mathbb{C}) = V(J_1) = V(X^2-2X-Y+2)$.

Bew. von Satz 13.2: (1) Definiere $i: K^m \longrightarrow K^{n+m}$,

$i(a_1,\dots,a_m) := (a_1,\dots,a_m, f_1(a_1,\dots,a_m),\dots,f_n(a_1,\dots,a_m))$,

$\pi_m: K^{n+m} \longrightarrow K^n$, $\pi_m(a_1,\dots,a_m,b_1,\dots,b_n) := (b_1,\dots,b_n)$

Setze $V := V(J) = V(X_1 - f_1,\dots,X_n - f_n)$

$= \{(a_1,\dots,a_m,b_1,\dots,b_n) \in K^{n+m} \mid b_1 = f_1(a_1,\dots,a_m),\dots,b_n = f_n(a_1,\dots,a_m)\}$

$= \{(a_1,\dots,a_m,f_1(a_1,\dots,a_m),\dots,f_n(a_1,\dots,a_m) \mid (a_1,\dots,a_m) \in K^m\}$

$= i(K^m)$

Wir erhalten

$$F(K^m) = \pi_m(i(K^m)) = \pi_m(V) = \pi_m(V(J)).$$

② Fallunterscheidung

1. Fall: $K = \mathbb{C}$

Nach dem Satz vom Abschluß (12.6) ist $V(J_m)$ die kleinste Varietät in $\mathbb{C}^n$, die $\pi_m(V) \overset{s.o.}{=} F(\mathbb{C}^m)$ enthält.

2. Fall: $K \subsetneq \mathbb{C}$

Wegen $1 \in K$ ist dann auch $\underbrace{1+\ldots+1}_{n\text{-mal}} = n \in K$ für alle $n \in \mathbb{N}$, insbes. ist K unendlich.

Nach obigem ist

$$F(K^m) = \pi_m(V) \overset{12.1}{\subset} V(J_m)$$

Sei $Z := V(g_1, \ldots, g_s) \subset K^n$ eine affine Varietät in K^n mit $F(K^m) \subset Z$, $g_1, \ldots, g_s \in K[$

zz.: $V(J_m) \subset Z$

Bew.: Offenbar verschwinden die Polynome $g_1, \ldots, g_s$ auf $F(K^m) \subset Z$.

$\Rightarrow$ Die Abbildungen $g_i \circ F$, $i = 1, \ldots, s$ sind jeweils die Nullabb. $K^m \to K$

~~$g_i \circ F \in K[x_1, \ldots, x_m]$~~. Explizit ist $g_i \circ F$ gegeben durch

$$g_i \circ F : K^m \to K, \quad (a_1, \ldots, a_m) \mapsto (g_i(f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m)) = h_i(a_1, \ldots, a_m)$$

mit $h_i \in K[t_1, \ldots, t_m]$

Also: Die Polynome $h_1, \ldots, h_s$ verschwinden auf K^m

$\overset{K \text{ unendl.}}{\Rightarrow} h_1 = \ldots = h_s = 0$

$\Rightarrow$ Die Abbildungen $g_i \circ F : \mathbb{C}^m \to \mathbb{C}$ sind jew. die Nullabb.

$\Rightarrow$ Die Polynome $g_1, \ldots, g_s$ verschwinden auf $F(\mathbb{C}^m)$

$\Rightarrow Z_{\mathbb{C}} := V_{\mathbb{C}}(g_1, \ldots, g_s) := \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid g_1(a_1, \ldots, a_n) = \ldots = g_s(a_1, \ldots, a_n) = 0\}$

ist eine affine Varietät in $\mathbb{C}^n$ mit $Z_{\mathbb{C}} \supset F(\mathbb{C}^m)$.

Setze $J_{\mathbb{C}} := \langle X_1 - f_1, \ldots, X_n - f_n \rangle \subset \mathbb{C}[t_1, \ldots, t_m, X_1, \ldots, X_n]$

Nach Fall 1 ist $V((J_{\mathbb{C}})_m)$ die kleinste Varietät in $\mathbb{C}^n$, die $F(\mathbb{C}^m)$ enthält.

$\Rightarrow V((J_{\mathbb{C}})_m) \subset Z_{\mathbb{C}}$

Sei $\{p_1, \ldots, p_r\} \subset K[X_1, \ldots, X_n]$ die reduzierte Gröbnerbasis von J_m. Der Algorithmus zur Bestimmung von $(J_{\mathbb{C}})_m$ liefert dieselbe reduzierte Gröbnerbasis für $(J_{\mathbb{C}})_m$

Also: $V((J_{\mathbb{C}})_m) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid p_1(a_1, \ldots, a_n) = \ldots = p_r(a_1, \ldots, a_n) = 0\}$

$\subset \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid g_1(a_1, \ldots, a_n) = \ldots = g_s(a_1, \ldots, a_n) = 0\}$

$= Z_{\mathbb{C}}$

$\Rightarrow \{(a_1, \ldots, a_n) \in K^n \mid p_1(a_1, \ldots, a_n) = \ldots = p_r(a_1, \ldots, a_n) = 0\}$

$\subset \{(a_1, \ldots, a_n) \in K^n \mid g_1(a_1, \ldots, a_n) = \ldots = g_s(a_1, \ldots, a_n) = 0\}$

$\Rightarrow V(J_m) \subset Z$. □

Algorithmus

Folgerung 13.4: (Implizitisierungssatz für polynomiale Parametrisierungen)

$K \subset \mathbb{C}$ Körper.

Eingabe: $(f_1, \ldots, f_n) \in (K[t_1, \ldots, t_m])^n$

Algorithmus: (1) Setze $J := \langle X_1 - f_1, \ldots, X_n - f_n \rangle \subset K[t_1, \ldots, t_m, X_1, \ldots, X_n]$

(2) Berechne Gröbnerbasis G von J bzgl. $\geq_{lex}$ mit $t_1 > \ldots > t_m > X_1 > \ldots > X_n$

(3) $G_m := G \cap K[X_1, \ldots, X_n]$ ist eine Gröbnerbasis von J_m.

Ausgabe: $V(G_m)$ ist die kleinste Varietät in K^n, die $F(K^m)$ enthält, wobei $F: K^m \to K^n, (a_1, \ldots, a_m) \mapsto (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$.

Bew.: klar nach 13.2. □

Satz 13.5: (Rationale Implizitisierung) $K \subset \mathbb{C}$ Körper, $f_1, \dots, f_n, g_1, \dots, g_n \in K[t_1, \dots, t_m]$ ($\in$?), $g_1, \dots, g_n \neq 0$, $W := V(g_1, \dots, g_n)$, $F: K^m \setminus W \to K^n$,

$$F(a_1, \dots, a_m) := \left(\frac{f_1(a_1, \dots, a_m)}{g_1(a_1, \dots, a_m)}, \dots, \frac{f_n(a_1, \dots, a_m)}{g_n(a_1, \dots, a_m)} \right).$$

Setze

$$J := \langle g_1 X_1 - f_1, \dots, g_n X_n - f_n, 1 - gY \rangle \subset K[Y, t_1, \dots, t_m, X_1, \dots, X_n]$$

(hierbei ist $g := g_1 \cdot \dots \cdot g_m$).

$J_{m+1} := J \cap K[X_1, \dots, X_n]$ ($(m+1)$-tes Eliminationsideal von J bzgl. „$\geq_{lex}$" mit $Y > t_1 > \dots > t_m > X_1 > \dots > X_n$)

Dann gilt:

$V(J_{m+1})$ ist die kleinste Varietät in K^n, die $F(K^m \setminus W)$ enthält.

Anm.: Die Gleichungen, die J beschreiben, sind

$$g_1 X_1 = f_1, \dots, g_n X_n = f_n, \; g_1 \cdot \dots \cdot g_n Y = 1$$

Die ersten n Gleichungen entstehen durch Wegmultiplizieren der Nenner, die letzte Gleichung bewirkt, daß keiner der Nenner verschwinden kann.

Bsp. 13.6: Sei $f_1 = 1 - t^2$, $g_1 = 1 + t^2$, $f_2 = 2t$, $g_2 = 1 + t^2 \in \mathbb{R}[t]$, F wie in Not. u. 13.5,

Es ist $W = V(g_1, g_2) = V(1 + t^2) = \emptyset$,

$$J = \langle (1+t^2) X_1 - (1 - t^2), \; (1+t^2) X_2 - 2t, \; 1 - (1+t^2)^2 Y \rangle$$

Eine Gröbnerbasis von J ist gegeben durch

$$G = \{ Y - \tfrac{1}{2} X_1 + \tfrac{1}{4} X_2^2 - \tfrac{1}{2}, \; t X_1 + t - X_2, \; t X_2 + X_1 - 1, \; X_1^2 + X_2^2 - 1 \}$$

Insbes. ist $J_2 = \langle X_1^2 + X_2^2 - 1 \rangle$, nach 13.5 ist $V(X_1^2 + X_2^2 - 1)$ die kleinste affine Varietät in $\mathbb{R}^2$, die $F(\mathbb{R})$ enthält.

Bew. von 13.5: ① Definiere

$$j: K^m \setminus W \longrightarrow K^{n+m+1}, \quad j(a_1,\dots,a_m) := \left(\frac{1}{g(a_1,\dots,a_m)}, a_1,\dots,a_m, \frac{f_1(a_1,\dots,a_m)}{g_1(a_1,\dots,a_m)},\dots,\frac{f_n(a_1,\dots,a_m)}{g_n(a_1,\dots,a_m)} \right)$$

$$\pi_{m+1}: K^{n+m+1} \longrightarrow K^n, \quad \pi_{m+1}(y, a_1,\dots,a_m, b_1,\dots,b_n) := (b_1,\dots,b_n)$$

Setze $V := V(J) = V(g_1 X_1 - f_1, \dots, g_n X_n - f_n, 1 - g Y)$

Offenbar ist $F = \pi_{m+1} \circ j$

Beh.: $j(K^m \setminus W) = V(J) \subset K^{n+m+1}$

Bew.: „$\subset$" nach Konstr. von j

„$\supset$" Sei $(y, a_1,\dots,a_m, b_1,\dots,b_n) \in V(J) \Rightarrow g(a_1,\dots,a_m)\, y = 1$, sowie

$g_i(a_1,\dots,a_m)\, b_i = f_i(a_1,\dots,a_m)$ für $i = 1,\dots,n$

$\Rightarrow g_i(a_1,\dots,a_m) \neq 0$ für $i = 1,\dots,n$,

$$\rightarrow (y, a_1,\dots,a_m, b_1,\dots,b_n) = \left(\frac{1}{g_0(a_1,\dots,a_m)}, a_1,\dots,a_m, \frac{f_1(a_1,\dots,a_m)}{g_1(a_1,\dots,a_m)},\dots,\frac{f_n(a_1,\dots,a_m)}{g_n(a_1,\dots,a_m)} \right)$$

$$\in j(K^m \setminus W)$$

$$\Rightarrow F(K^m \setminus W) = \pi_{m+1}(j(K^m \setminus W)) = \pi_{m+1}(V(J))$$

② Fallunterscheidung:

1. Fall: $K = \mathbb{C}$

Nach dem Satz vom Abschluß ist $V(J_{m+1})$ die kleinste affine Varietät in $\mathbb{C}^n$, die $\pi_{m+1}(V(J)) \overset{s.o.}{=} F(K^m \setminus W)$ enthält.

2. Fall: $K \subsetneq \mathbb{C}$

Insbes. ist K unendlich.

Nach obigem ist

$$F(K^m \setminus W) = \pi_{m+1}(V(J)) \overset{12.1}{\subset} V(J_{m+1})$$

Sei $Z := V(h_1,\dots,h_s) \subset K^n$ eine affine Varietät mit $F(K^m \setminus W) \subset Z$.

zz.: $V(J_{m+1}) \subset Z$

Bew.: Die Polynome $h_{11\ldots}, h_s$ verschwinden auf $F(K^m \setminus W)$

Die Abb. $h_i \circ F: K^m \setminus W \to K$ ist die Nullabb. für $i = 1, \ldots, s$

Explizit ist $h_i \circ F$ gegeben durch

$$h_i \circ F: K^m \setminus W \to K, \quad (a_1, \ldots, a_m) \mapsto \tilde{h}_i(a_1, \ldots, a_m)$$

mit $\tilde{h}_i \in K(t_1, \ldots, t_m)$ (vgl. Bew. zu 13.2), $\tilde{h}_i = \frac{h_i'}{h_i''}$, $h_i', h_i'' \in K[t_1, \ldots, t_m]$

Also: Die Polynome $h_1''', \ldots, h_s'''$ verschwinden auf $K^m \setminus W = K^m \setminus V(g)$

$\Rightarrow h_1''' g, \ldots, h_s''' g$ verschwinden auf K^m

$\overset{K \text{ unendl.}}{\Rightarrow} h_1''' g = \ldots = h_s''' g = 0$

$\overset{g \neq 0}{\Rightarrow} h_1''' = \ldots = h_s''' = 0 \Rightarrow \tilde{h}_1 = \ldots = \tilde{h}_s = 0.$

$\Rightarrow h_i \circ F: \mathbb{C}^m \setminus V_{\mathbb{C}}(g) \to \mathbb{C}$, $i = 1, \ldots, s$

ist jeweils die Nullabb. ($V_{\mathbb{C}}(\ldots)$ sei jew. wie in Bew. von 13.2 def.)

$\Rightarrow h_1, \ldots, h_s$ verschwinden auf $F(\mathbb{C}^m \setminus V_{\mathbb{C}}(g))$

$\Rightarrow Z_{\mathbb{C}} := V_{\mathbb{C}}(h_1, \ldots, h_s)$ ist eine affine Var. in $\mathbb{C}^n$ mit $Z_{\mathbb{C}} \supset F(\mathbb{C}^m \setminus V_{\mathbb{C}}(g))$

Setze $J_{\mathbb{C}} := \langle g_1 X_1 - f_1, \ldots, g_n X_n - f_n, gY - 1 \rangle \subset \mathbb{C}[Y, t_1, \ldots, t_m, X_1, \ldots, X_n]$

$\overset{\text{Fall 1}}{\Rightarrow} V((J_{\mathbb{C}})_{m+1})$ ist die kleinste affine Var. in $\mathbb{C}^n$, die $F(\mathbb{C}^m \setminus V_{\mathbb{C}}(g))$ enthält.

$(J_{\mathbb{C}})_{m+1}$ und J_{m+1} haben dieselbe reduzierte Gröbnerbasis, etwa

$\{p_1, \ldots, p_r\}$ mit $p_1, \ldots, p_r \in K[X_1, \ldots, X_n]$

$V((J_{\mathbb{C}})_{m+1}) \subset Z_{\mathbb{C}}$ impliziert dann wie im Beweis von 13.2:

$V(J_{m+1}) \subset Z$. □

Algorithmus 13.7: (Implizitisierungsalgorithmus für rationale Parametrisierung)

$K \subset \mathbb{C}$ Körper

Eingabe: $(f_1,\dots,f_n) \in (K[t_1,\dots,t_m])^s$, $(g_1,\dots,g_n) \in (K[t_1,\dots,t_m])^s$ \{o.B.d.A.\}

Algorithmus: (1) Setze $g := g_1 \cdot \ldots \cdot g_n$

$J := \langle g_1 X_1 - f_1, \dots, g_n X_n - f_n, 1 - g Y \rangle \subset K[Y, t_1, \dots, t_m, X_1, \dots, X_n]$

(2) Berechne Gröbnerbasis G von J bzgl. „$\geq_{lex}$" mit $Y > t_1 > \dots > t_m > X_1 > \dots > X_n$

(3) $G_m := G \cap K[X_1,\dots,X_n]$ ist Gröbnerbasis von J_{m+1}

Ausgabe: $V(G_m)$ ist die kleinste affine Varietät in K^n, die $F(K^m \setminus W)$ enthält, wobei $W = V(g_1 \cdot \ldots \cdot g_n)$, $F: K^m \setminus W \to K^n$, $(a_1,\dots,a_m) \mapsto \left(\frac{f_1(a_1,\dots,a_m)}{g_1(a_1,\dots,a_m)}, \dots, \frac{f_n(a_1,\dots,a_m)}{g_n(a_1,\dots,a_m)} \right)$.

Anm.: Die Sätze 13.2, 13.5 gelten über Körpern K mit unendlich vielen Elementen (es muß also nicht unbedingt $K \subset \mathbb{C}$ vorausgesetzt werden.)

§14. Faktorisierung und Resultanten

Def. 14.1: K Körper, $f \in K[X_1,\dots,X_n]$ nichtkonstant

f heißt *irreduzibel* $\overset{\text{Def}}{\Leftrightarrow}$ Aus $f = gh$ mit $g,h \in K[X_1,\dots,X_n]$ folgt stets: g konstant oder h konstant.

Bsp. 14.2:
- $f = X^2 + 1 \in \mathbb{R}[X]$ ist irreduzibel
- $f = X^2 + 1 = (X+i)(X-i) \in \mathbb{C}[X]$ ist reduzibel

Bem. 14.3: K Körper, $f \in K[X_1,\dots,X_n]$ nichtkonstant. Dann gilt:

Es existieren irreduzible Polynome $h_1,\dots,h_t \in K[X_1,\dots,X_n]$, sd.

$$f = h_1 \cdot \ldots \cdot h_t$$

Bew.: (per Induktion nach dem Totalgrad $n := \deg(f)$)

$n = 1$: Sei $f = gh$ mit $g,h \in K[X]$, g,h nichtkonstant

$\Rightarrow 1 = \deg(f) = \deg(g) + \deg(h)$

$\Rightarrow \deg(g) = 0$ oder $\deg(h) = 0$

$\Rightarrow$ g oder h konstant

$\Rightarrow$ f irreduzibel

Induktionsschritt: 1. Fall: f irreduzibel. Dann fertig

2. Fall: f reduzibel $\Rightarrow$ Es ex. $g, h \in K[X_1, \dots, X_n]$ mit g, h nichtkonstant, sd. $f = gh$.

$\Rightarrow \deg(g) < \deg(f)$, $\deg(h) < \deg(f)$

$\overset{IV}{\Rightarrow}$ Es ex. irred. Polynome $g_1, \dots, g_t, h_1, \dots, h_s \in K[\underline{X}]$, sd.

$g = g_1 \cdot \dots \cdot g_t$, $h = h_1 \cdot \dots \cdot h_s$

$\Rightarrow f = g_1 \cdot \dots \cdot g_t h_1 \cdot \dots \cdot h_s$ □

<u>Satz 14.4:</u> K Körper, $f \in K[X_1, \dots, X_n]$ irreduzibel, $g, h \in K[X_1, \dots, X_n]$ mit $f \mid gh$. Dann gilt:

$f \mid g$ oder $f \mid h$.

<u>Bew.:</u> per Induktion nach n.

$n = 1$: Setze $p := ggT(f, g)$. Dann gilt insbes. $p \mid f$. Wegen f irred. ergeben sich die folgenden Fälle

1. Fall: p ist nichtkonstant

$\overset{f \text{ irred}}{\Rightarrow} f = cp$ mit $c \in K$

$\Rightarrow p = c^{-1} f \overset{p \mid g}{\Rightarrow} f \mid g$.

2. Fall: $p = 1$

$\overset{4.11(b)}{\Rightarrow} \exists A, B \in K[X_1] : Af + Bg = 1$

$\Rightarrow h = h(Af + Bg) = Ahf + Bgh$

$\overset{f \mid gh}{\Rightarrow} f \mid Ahf + Bgh = h$.

Ind. schritt:

(1) Wir betrachten zunächst einen Spezialfall.

Beh.: Ist $u \in K[X_2, \dots, X_n]$ irreduzibel, $g, h \in K[X_1, \dots, X_n]$ mit $u \mid gh$, dann gilt: $u \mid g$ oder $u \mid h$

Bew.: Sei $g = \sum_{i=0}^{l} a_i X_1^i$, $h = \sum_{i=0}^{m} b_i X_1^i$ mit $a_0, \dots, a_l, b_0, \dots, b_m \in K[X_2, \dots, X_n]$

1. Fall: $u \mid a_i$ für alle $i \in \{0, \dots, l\}$ oder $u \mid b_i$ für alle $i \in \{0, \dots, m\}$, dann fertig

2. Fall: Es ex. $i \in \{0, \dots, l\}$, $j \in \{0, \dots, m\}$ minimal mit $u \nmid a_i$, $u \nmid b_j$.

Wir schreiben $gh = \sum_{k=0}^{m+l} c_k X_1^k$

Insbes. ist $c_{i+j} = (a_0 b_{i+j} + \dots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \dots + a_{i+j} b_0)$

(hierbei ist $a_k := 0$ für $k \notin \{0, \dots, l\}$, $b_k := 0$ für $k \notin \{0, \dots, m\}$)

u teilt alle Terme in der linken sowie der rechten Klammer,

$u \nmid a_i$, $u \nmid b_j$

$\overset{\text{Ind. vor.}}{\Rightarrow}$ $u \nmid a_i b_j$

$\Rightarrow u \nmid c_{i+j}$

Aus $u \mid gh$ folgt aber $gh = uw$ mit $w = \sum_{k=0}^{m+l} w_k X_1^k$ mit

$w_k \in K[X_2, \dots, X_n] \Rightarrow gh = \sum_{k=0}^{m+l} \underbrace{(uw_k)}_{=c_k} X_1^k$, insbes. $u \mid c_{i+j}$. ↯

Allgem. Fall:

(2) Falls $f \in K[X_2, \dots, X_n]$, dann fertig nach (1).

Im folgenden involviere f die Variable X_1

Beh.: f ist irreduzibel in $K(X_2, \dots, X_n)[X_1]$, d.h. ist $f = AB$ mit $A, B \in K(X_2, \dots, X_n)[X_1]$, dann ist $A \in K(X_2, \dots, X_n)$ oder $B \in K(X_2, \dots, X_n)$

Bew.: Sei $f = AB$ mit A, B wie in Beh., sei $d \in K[X_2, \dots, X_n]$ das Produkt aller Nenner in A, B

$\Rightarrow \tilde{A} := dA$, $\tilde{B} := dB$ sind in $K[X_1, \dots, X_n]$

$\Rightarrow d^2 f = \tilde{A}\tilde{B} \in K[X_{1,\dots}, X_n]$

$d^2 \in K[X_{2,\dots}, X_n]$ läßt sich nach 14.3 als Produkt irred. Polynome aus $K[X_{2,\dots}, X_n]$ schreiben: $d^2 = d_1 \cdot \dots \cdot d_s$

Es gilt dann $d_1 \mid \tilde{A}\tilde{B}$, wg. ① folgt $d_1 \mid \tilde{A}$ oder $d_1 \mid \tilde{B}$, durch Kürzen erhalten wir also $\tilde{\tilde{A}}, \tilde{\tilde{B}} \in K[X_{1,\dots}, X_n]$ mit

$$d_2 \cdot \dots \cdot d_s f = \tilde{\tilde{A}}\,\tilde{\tilde{B}}$$

Dieses Argument mehrfach angewendet liefert

$$f = \hat{A}\,\hat{B} \quad \text{mit } \hat{A}, \hat{B} \in K[X_{1,\dots}, X_n]$$

f irred. in $K[X_{1,\dots}, X_n] \Rightarrow \hat{A}$ konstant oder $\hat{B}$ konstant

$\hat{A}, \hat{B}$ entstehen aus A, B durch Multiplikation mit bzw. Division durch Elemente aus $K[X_{2,\dots}, X_n]$

$\Rightarrow A \in K(X_{2,\dots}, X_n)$ oder $B \in K(X_{2,\dots}, X_n)$.

③ Nach ② ist f irreduzibel in $K(X_{2,\dots}, X_n)[X_1]$

$\overset{\text{Satz für } n=1}{\Rightarrow} f \mid g$ oder $f \mid h$ in $K(X_{2,\dots}, X_n)[X_1]$,

o.E. $g = Af$ mit $A \in K(X_{2,\dots}, X_n)[X_1]$.

Durch Wegmult. der Nenner erhalten wir

$$dg = \tilde{A} f$$

mit $\tilde{A} \in K[X_{1,\dots}, X_n]$, $d \in K[X_{2,\dots}, X_n]$

1. Fall: d konstant, dann folgt $f \mid g$, fertig

2. Fall: d nichtkonstant

Nach 14.3 ist $d = d_1 \cdot \dots \cdot d_s$ mit $d_{1 \le \nu \le s} \in K[X_{2,\dots}, X_n]$ irreduzibel

$\Rightarrow d_1 \cdot \dots \cdot d_s g = \tilde{A} f$

Wegen ① folgt $d_1 \mid \tilde{A}$ oder $d_1 \mid f$

Falls $d_1 \mid f$, folgt wg. f irreduzibel: $f = c d_1$ mit $c \in K$ ↯ zu X_1-Grad von f ist > 1

Also: $d_1 | A$

Kürzen liefert $d_2 \cdot \ldots \cdot d_s \, g = \tilde{\tilde{A}} f$ mit $\tilde{\tilde{A}} \in K[X_1, \ldots, X_n]$

Wiederholen dieses Prozesses liefert schließlich $g = \hat{A} f$ mit $\hat{A} \in K[X_1, \ldots, X_n]$, d.h. $f | g$. □

<u>Folgerung 14.5:</u> K Körper, $f, g \in K[X_1, \ldots, X_n]$ mit positivem Grad in X_1.
Dann sind äquivalent:

(i) f, g haben einen gemeinsamen Faktor in $K[X_1, \ldots, X_n]$ von positivem X_1-Grad

(ii) f, g haben einen gemeinsamen Faktor in $K(X_2, \ldots, X_n)[X_1]$ von positivem (X_1-) Grad.

<u>Bew.:</u> (i)$\Rightarrow$(ii) klar wg. $K[X_1, \ldots, X_n] \subset K(X_2, \ldots, X_n)[X_1]$.

(ii)$\Rightarrow$(i) Sei $\tilde{h} \in K(X_2, \ldots, X_n)[X_1]$ ein gem. Faktor von f, g von pos. Grad.

$\rightarrow$ $f = \tilde{h} \tilde{f}_1$ für ein $\tilde{f}_1 \in K(X_2, \ldots, X_n)[X_1]$

$g = \tilde{h} \tilde{g}_1$ für ein $\tilde{g}_1 \in K(X_2, \ldots, X_n)[X_1]$

Sei $d \in K[X_2, \ldots, X_n]$ das Produkt der Nenner von $\tilde{h}, \tilde{f}_1, \tilde{g}_1$

$\Rightarrow$ $h := d\tilde{h}$, $f_1 := d\tilde{f}_1$, $g_1 := d\tilde{g}_1 \in K[X_1, \ldots, X_n]$

Wir erhalten

$d^2 f = h f_1$, $d^2 g = h g_1$

Das Polynom h hat ebenso wie $\tilde{h}$ positiven Grad in X_1, insbes. ex. ein irred. Faktor $h_1 \in K[X_1, \ldots, X_n]$ von h von positivem X_1-Grad.

$\Rightarrow$ $h_1 | h f_1 = d^2 f \overset{14.4}{\Rightarrow} h_1 | d^2$ oder $h_1 | f$

1. Fall: $h_1 | d^2$ ↯ da $d^2 \in K[X_2, \ldots, X_n]$

Also: $h_1 | f$

Ein analoges Argument zeigt $h_1 | g$. □

Satz 14.6: K Körper, $f \in K[X_1, \dots, X_n]$ nichtkonstant. Dann gilt:

(a) f kann als Produkt von irreduziblen Polynomen $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ geschrieben werden: $f = f_1 \cdot \dots \cdot f_r$

(b) Sind $f = f_1 \cdot \dots \cdot f_r = g_1 \cdot \dots \cdot g_s$ zwei Darstellungen von f als Produkt irreduzibler Polynome, dann ist $r = s$, und nach Umnummerierung von $g_1, \dots, g_s$ kann man erreichen, daß $g_i = c_i f_i$ für $i = 1, \dots, r$ mit $c_i \in K \setminus \{0\}$

(d.h. die Darstellung von f als Produkt irreduzibler Polynome ist eindeutig bis auf Reihenfolge und Multiplikation mit Elementen aus $K \setminus \{0\}$.

Bew.: (a) = Bem. 14.4

(b) per Induktion nach $m := \deg(f)$

$m = 1$: Dann ist f irreduzibel, siehe Bew. von 14.3

Ind.schritt: Sei $f = f_1 \cdot \dots \cdot f_r = g_1 \cdot \dots \cdot g_s$ mit $f_1, \dots, f_r, g_1, \dots, g_s \in K[\underline{X}]$ irreduzibel

$\Rightarrow f_1 \mid g_1 \cdot \dots \cdot g_s$

$\overset{14.4}{\Rightarrow}$ f_1 teilt eines der Polynome $g_1, \dots, g_s$, o.E. $f_1 \mid g_1$

$\overset{\substack{g_1 \text{ irred} \\ f_1 \text{ irred}}}{\Rightarrow}$ $g_1 = c_1 f_1$ mit $c_1 \in K^{\times} \setminus \{0\}$

Durch Kürzen erhalten wir

$f_2 f_3 \cdot \dots \cdot f_r = (c_1 g_2) g_3 \cdot \dots \cdot g_s$

Es ist $\deg(f_2 \cdot \dots \cdot f_r) < m \Rightarrow$ Beh. aus Ind.vor.

Anm.: Man sagt auch: $K[X_1, \dots, X_n]$ ist ein Ring mit eindeutiger Primfaktorzerlegung (ZPE-Ring) oder faktorieller Ring.

Ziel: Im folgenden werden wir (für $K[X]$) studieren, wie man ablesen kann ob zwei Polynome einen gemeinsamen Faktor haben, ohne den ggT auszurechnen oder die Polynome zu faktorisieren.

Bem. 14.7: K Körper, $f, g \in K[X]$ mit $l := \deg(f) > 0$, $m := \deg(g) > 0$.

Dann sind äquivalent:

(i) f, g haben einen gemeinsamen nichtkonstanten Faktor in $K[X]$

(ii) Es ex. Polynome $A, B \in K[X]$ mit

(a) A, B sind nicht beide Null

(b) $\deg(A) \leq m-1$, $\deg(B) \leq l-1$

(c) $Af + Bg = 0$

Bew.: (i)$\Rightarrow$(ii) Sei $h \in K[X]$ nichtkonstant mit $f = hf_1$, $g = hg_1$ mit $f_1, g_1 \in K[X]$

$\Rightarrow \deg(f_1) \leq l-1$, $\deg(g_1) \leq m-1$, sowie

$\Rightarrow g_1 \cdot f + (-f_1 g) = g_1 h_1 f - f_1 h_1 g = 0$

Setze $A := g_1$, $B := -f_1$

(ii)$\Rightarrow$(i) Wegen (a) können wir oE annehmen: $B \neq 0$

Falls f, g keinen gemeinsamen nichtkonstanten Faktor haben, dann ist $\operatorname{ggT}(f, g) = 1$

$\overset{4.11(b)}{\Rightarrow} \exists \tilde{A}, \tilde{B} \in K[X] : \tilde{A}f + \tilde{B}g = 1$

$\Rightarrow B = (\tilde{A}f + \tilde{B}g)B = \tilde{A}Bf + \tilde{B}Bg \overset{(c)}{=} \tilde{A}Bf - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f$

$\Rightarrow \deg(B) \geq l$ ↯ zu (b)

Anm.: Um zu klären, ob A, B wie in (ii) existieren, kann man einen expliziten Ansatz machen und die Koeff. mit Hilfe eines LGS (Koeffvergl.) ausrechnen! Dies führt zur Def. der Resultante.

Def. 14.8: K Körper, $f, g \in K[X]$ nichtkonstant,

$f = a_0 X^l + \dots + a_l \quad a_0 \neq 0,$

$g = b_0 X^m + \dots + b_m, \quad b_0 \neq 0$

$$Syl(f,g) := \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & a_2 & & a_0 & \vdots & \ddots & & b_0 \\ a_l & \vdots & & a_1 & \vdots & & & b_1 \\ & a_l & & \vdots & b_m & \ddots & & \vdots \\ & & & a_l & & b_m & \cdots & b_m \end{pmatrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\\a\end{matrix}}\right\} l+m \text{ Zeilen}$$

m Spalten, l Spalten

$$\in M_{l+m, l+m}(K)$$

heißt die Sylvestermatrix von f, g.

$Res(f,g) := \det(Syl(f,g)) \in K$ heißt die Resultante von f und g.

Anm.: $Res(f,g)$ hängt offenbar in folgendem Sinne „ganz-polynomial" von den Koeffizienten von f, g ab: Es ex. ein Pol. $M \in \mathbb{Z}[s_0, \dots, s_l, t_0, \dots, t_m]$, sd. $Res(f,g) = M(a_0, \dots, a_l, b_0, \dots, b_m)$ ($\rightsquigarrow$ Leibnizformel)

Bsp. 14.9: (a) $f = 2X^2 + 3X + 1, \quad g = 7X^2 + X + 3 \in \mathbb{Q}[X]$

$$\Rightarrow Res(f,g) = \det \begin{pmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{pmatrix} = 153$$

(b) $f = X^2 + aX + b, \quad g = X + c \in \mathbb{Q}[X]$

$$\Rightarrow Res(f,g) = \det \begin{pmatrix} 1 & 1 & 0 \\ a & c & 1 \\ b & 0 & c \end{pmatrix} = c^2 - ac + b$$

Bem. 14.10: K Körper, $f, g \in K[X]$ nichtkonstant. Dann sind äquivalent:

(i) f, g haben einen gemeinsamen nichtkonstanten Faktor in $K[X]$

(ii) $Res(f,g) = 0$.

Bew.: Sei $f = a_0 X^l + \dots + a_l$, $g = b_0 X^m + \dots + b_m$, $a_0, b_0 \neq 0$

(ii) $\overset{14.7}{\Leftrightarrow}$ Es ex. $A, B \in K[X]$ mit $Af + Bg = 0$, $\deg(A) \leq m-1$, $\deg(B) \leq l-1$, A, B nicht beide Null

Ansatz: $A = c_0 X^{m-1} + \dots + c_{m-1}$, $B = d_0 X^{l-1} + \dots + d_{l-1}$

Koeffizientenvergl. in $Af + Bg = 0$ liefert folgendes LGS:

$$\begin{aligned}
a_0 c_0 \qquad\qquad + b_0 d_0 \qquad\qquad &= 0 \quad (\text{Koeff. von } X^{l+m-1}) \\
a_1 c_0 + a_0 c_1 \qquad + b_1 d_0 + b_0 d_1 \qquad &= 0 \quad (\text{Koeff. von } X^{l+m-2}) \\
\vdots \qquad\qquad\qquad \ddots \qquad\qquad\qquad & \\
a_l c_{m-1} + \qquad\qquad b_m d_{l-1} &= 0 \quad (\text{Koeff. von } X^0),
\end{aligned}$$

d.h. $\mathrm{Syl}(f,g) \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{l-1} \end{pmatrix} = 0$

Dieses homogene LGS hat genau dann eine Lösung, wenn $\det(\mathrm{Syl}(f,g)) = \mathrm{Res}(f,g) = 0$. □

Bsp. 14.11: f, g wie in Bsp. 14.9(a), dann ist $\mathrm{Res}(f,g) = 153 \neq 0$, d.h. f, g haben keinen gem. nichtkonst. Faktor in $\mathbb{Q}[X]$

Folgerung 14.12: $f, g \in \mathbb{C}[X]$ nichtkonstant. Dann sind äquivalent:

(i) f, g haben eine gemeinsame Nullstelle in $\mathbb{C}$

(ii) $\mathrm{Res}(f,g) = 0$

Bew.: (i)⇒(ii) Sei $\alpha \in \mathbb{C}$ gem. NS von f, g.

$\overset{4.6}{\Rightarrow}$ $X - \alpha$ ist gemeinsamer Faktor von f, g $\overset{14.10}{\Rightarrow}$ $\mathrm{Res}(f,g) = 0$

(ii)⇒(i) Nach 14.10 ex. wg. $\mathrm{Res}(f,g) = 0$ ein $h \in \mathbb{C}[X]$, h nichtkonstant mit $h \mid f$, $h \mid g$. Sei $\alpha \in \mathbb{C}$ eine NS von h (ex. nach Fundamentalsatz der Algebra) ⇒ $f(\alpha) = g(\alpha) = 0$.

Bem. 14.12: K Körper, $f, g \in K[X]$ nichtkonstant. Dann gilt:

Es existieren $A, B \in K[X]$, sd. gilt:

$$Af + Bg = \mathrm{Res}(f,g),$$

und die Koeffizienten von A, B hängen ganz-polynomial von den Koeffizienten von f, g ab (vgl. Anm. nach Def. 14.8).

Bew.: Falls $\mathrm{Res}(f,g) = 0$, setze $A := B := 0$.

Sei im folgenden $\mathrm{Res}(f,g) \neq 0$.

Sei $f = a_0 X^l + \ldots + a_l$, $a_0 \neq 0$, $g = b_0 X^m + \ldots + b_m$, $b_0 \neq 0$.

Wir suchen zunächst Lösungen $\tilde{A}, \tilde{B} \in K[X]$ der Gleichung

$$\tilde{A} f + \tilde{B} g = 1$$

Ansatz für $\tilde{A}, \tilde{B}$: $\tilde{A} = c_0 X^{m-1} + \ldots + c_{m-1}$, $\tilde{B} = d_0 X^{l-1} + \ldots + d_{l-1}$

Analog zum Bew. von 14.10 ergibt sich das folgende LGS:

$$\mathrm{Syl}(f,g) \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{l-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Wegen $\mathrm{Res}(f,g)$ ist dieses LGS eindeutig lösbar, und es ist (Cramersche Regel)

$$c_i = \frac{\det(S_i)}{\mathrm{Res}(f,g)}, \quad i = 0, \ldots, m-1$$

wobei S_i aus $\mathrm{Syl}(f,g)$ durch Ersetzen der $i+1$-ten Spalte durch $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ entsteht.

$\det(S_i)$ hängt ebenso wie $\mathrm{Res}(f,g)$ ganzpolynomial von $a_0, \ldots, a_l, b_0, \ldots, b_m$ ab.

Wir erhalten:

$$\tilde{A} = \frac{1}{\mathrm{Res}(f,g)} \underbrace{\left(\det(S_0) X^{m-1} + \ldots + \det(S_{m-1})\right)}_{=: A \in K[X]} = \frac{A}{\mathrm{Res}(f,g)},$$

die Koeff. von A hängen ganzpolynomial von den Koeff. von f, g ab.

Analog: $\tilde{B} = \frac{1}{\mathrm{Res}(f,g)} B$ für ein $B \in K[X]$, dessen Koeff. ganz-polynomial von den Koeff. von f, g abh.

Aus $\tilde{A} f + \tilde{B} g = 1$ folgt $Af + Bg = \mathrm{Res}(f,g)$. □

§15. Resultanten und der Fortsetzungssatz

Def. 15.1: K Körper, $f,g \in K[X_1,\dots,X_n]$ mit positivem X_1-Grad.

Wir fassen f,g als Elemente von $K(X_2,\dots,X_n)[X_1]$ auf.

$\mathrm{Res}_{X_1}(f,g) := \mathrm{Res}(f,g)$ heißt die Resultante von f,g bzgl. X_1

Explizit: $f = a_0 X_1^l + \dots + a_l$, $g = b_0 X^m + \dots + b_m$ mit $a_0,\dots,a_l, b_0,\dots,b_m \in K[X_2,\dots,X_n]$

$$\mathrm{Res}_{X_1}(f,g) = \det \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & a_0 & & b_1 & b_0 & \\ \vdots & \vdots & \ddots & \vdots & b_1 & \ddots \\ a_l & \vdots & & b_m & \vdots & \\ & a_l & & & b_m & \\ & & \ddots & & & \ddots \end{pmatrix} \in K[X_2,\dots,X_n]$$

(m Spalten, l Spalten)

Bem. 15.2: K Körper, $f,g \in K[X_1,\dots,X_n]$ mit positivem X_1-Grad, $J = \langle f,g \rangle$.

Dann gilt:

(a) $\mathrm{Res}_{X_1}(f,g) \in J_1 = J \cap K[X_2,\dots,X_n]$

(b) $\mathrm{Res}_{X_1}(f,g) = 0 \Leftrightarrow f,g$ haben einen gemeinsamen Faktor in $K[X_1,\dots,X_n]$ von positivem X_1-Grad

Bew.: (a) $\mathrm{Res}_{X_1}(f,g) \in K[X_2,\dots,X_n]$ klar

Nach 14.13 ex. $A,B \in K(X_2,\dots,X_n)[X_1]$, sd.

$$Af + Bg = \mathrm{Res}_{X_1}(f,g)$$

Die Koeff. von A,B hängen nach 14.13 ganz-polynomial von den Koeff. von f,g ab, insbes. sind $A,B \in K[X_2,\dots,X_n][X_1] = K[X_1,\dots,X_n]$

$\Rightarrow \mathrm{Res}_{X_1}(f,g) \in \langle f,g \rangle = J$

(b) $\mathrm{Res}_{X_1}(f,g) = 0$

$\overset{14.10}{\Leftrightarrow}$ f,g haben gemeinsamen Faktor in $K(X_2,\dots,X_n)[X_1]$ von pos. X_1-Grad

$\overset{14.5}{\Leftrightarrow}$ f,g haben gemeinsamen Faktor in $K[X_1,\dots,X_n]$ von pos. X_1-Grad. □

Bem. 15.3: $f, g \in \mathbb{C}[X_1, \dots, X_n]$, $f = a_0 X_1^\ell + \dots + a_\ell$, $g = b_0 X_1^m + \dots + b_m$ mit $a_0, \dots, a_\ell, b_0, \dots, b_m \in \mathbb{C}[X_2, \dots, X_n]$, $a_0, b_0 \neq 0$. Es sei $(c_2, \dots, c_n) \in \mathbb{C}^{n-1}$ mit

$\operatorname{Res}_{X_1}(f,g)(c_2, \dots, c_n) = 0$.

Dann gilt:

$a_0(c_2, \dots, c_n) = 0$ oder $b_0(c_2, \dots, c_n) = 0$ oder es ex. ein $c_1 \in \mathbb{C}$, sd.

$f(c_1, \dots, c_n) = g(c_1, \dots, c_n) = 0$.

Bew.: Setze $C := (c_2, \dots, c_n)$, $f(X_1, C) := f(X_1, c_2, \dots, c_n) \in \mathbb{C}[X_1]$

Ann.: $a_0(C) \neq 0$ und $b_0(C) \neq 0$

Dann ist $f(X_1, C) = a_0(C) X_1^\ell + \dots + a_\ell(C)$, $a_0(C) \neq 0$,

$g(X_1, C) = b_0(C) X_1^m + \dots + b_m(C)$, $b_0(C) \neq 0$

Wir erhalten

$0 = \operatorname{Res}_{X_1}(f,g)(C) = \operatorname{Res}(f(X_1, C), g(X_1, C))$

$\overset{14.12}{\Rightarrow}$ $f(X_1, C), g(X_1, C)$ haben eine gemeinsame Nullstelle

$\Rightarrow \exists c_1 \in \mathbb{C}$: $f(c_1, c_2, \dots, c_n) = g(c_1, c_2, \dots, c_n) = 0$. □

Satz 15.4: (Fortsetzungssatz für zwei Polynome)

$f, g \in \mathbb{C}[X_1, \dots, X_n]$, $f = a_0 X_1^\ell + \dots + a_\ell$, $g = b_0 X_1^m + \dots + b_m$, $a_0, \dots, a_\ell, b_1, \dots, b_m \in \mathbb{C}[X_2, \dots, X_n]$, $a_0, b_0 \neq 0$.

$J = \langle f, g \rangle$, $J_1 = J \cap \mathbb{C}[X_2, \dots, X_n]$.

Dann gilt:

Ist $(c_2, \dots, c_n) \in V(J_1)$ eine partielle Lösung $(n-1)$-ter Stufe bzgl. J mit $(c_2, \dots, c_n) \notin V(a_0, b_0)$, dann ex. ein $c_1 \in \mathbb{C}$ mit $(c_1, \dots, c_n) \in V(J)$.

Bew.: Sei $C := (c_2, \dots, c_n) \in V(J_1)$ mit $C \notin V(a_0, b_0)$

Wg. 15.2 ist $\operatorname{Res}_{X_1}(f,g) \in J_1 \Rightarrow \operatorname{Res}_{X_1}(f,g)(C) = 0$

Falls $a_0(C) \neq 0$ und $b_0(C) \neq 0$, dann ex. nach 15.3 ein $c_1 \in \mathbb{C}$ mit $(c_1, c_2, \dots, c_n) \in V(J)$.

Nach Vor. ist $C \notin V(a_0, b_0)$, dh. $a_0(C) \neq 0$ <u>oder</u> $b_0(C) \neq 0$.

Ann: $a_0(C) \neq 0$, $b_0(C) = 0$

Ist $N \in \mathbb{N}$, dann ist offenbar

$$\langle f, g \rangle = \langle f, g + X_1^N f \rangle$$

Wir wählen N so groß, daß $X_1^N f$ größeren X_1-Grad hat als g.

$\Rightarrow$ Der Leitkoeff. von $g + X_1^N f$ und von f bzgl. X_1 ist jeweils a_0, und es ist $a_0(C) \neq 0$

$\overset{15.3}{\Rightarrow}$ Es ex. ein $c_1 \in \mathbb{C}$ mit $(c_1, c_2, \dots, c_n) \in V(f, g + X_1^N f) = V(f, g)$.

Anderer Fall $a_0(C) = 0$, $b_0(C) \neq 0$ analog. □

Def. 15.5: K Körper, $(f_1, \dots, f_s) \in K[X_1, \dots, X_n]^s$, $s \geq 3$

Setze $g := u_2 f_2 + \dots + u_s f_s \in K[u_2, \dots, u_s, X_1, \dots, X_n]$

Es ist $\operatorname{Res}_{X_1}(f_1, g) \in K[u_2, \dots, u_s, X_2, \dots, X_n]$.

Wir schreiben

$$\operatorname{Res}_{X_1}(f_1, g) = \sum_{\alpha \in \mathbb{N}_0^{s-1}} h_\alpha(X_2, \dots, X_n)\, \underline{u}^\alpha$$

Die Polynome $h_\alpha \in K[X_2, \dots, X_n]$ heißen die verallgemeinerten Resultanten von $(f_1, \dots, f_s)$.

Bsp. 15.6: $f_1 = X^2 + Y + Z - 1$, $f_2 = X + Y^2 + Z - 1$, $f_3 = X + Y + Z^2 - 1 \in \mathbb{C}[X, Y, Z]$

$$\Rightarrow \operatorname{Res}_{X_1}(f_1, u_2 f_2 + u_3 f_3) = \underbrace{(Y^4 + 2Y^2 Z - 2Y^2 + Z^2 + Y - Z)}_{h_{2,0}} u_2^2$$

$$+ 2\underbrace{(Y^2 Z^2 + Y^3 + Z^3 - Y^2 - Z^2 + YZ)}_{h_{1,1}} u_2 u_3 + \underbrace{(Z^4 + 2YZ^2 + Y^2 - 2Z^2 - Y + Z)}_{h_{0,2}} u_3^2$$

Satz 15.7: (Fortsetzungssatz) $f_1, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$, $J = \langle f_1, \dots, f_s \rangle$, $J_1 = J \cap \mathbb{C}[X_2, \dots, X_n]$

Schreibe für alle $i \in \{1, \dots, s\}$ f_i in der Form

$$f_i = g_i(X_2, \dots, X_n) X_1^{N_i} + \text{Terme von } X_1\text{-Grad} < N_i$$

mit $N_i \geq 0$, $g_i \in \mathbb{C}[X_2, \dots, X_n]$, $g_i \neq 0$ (Falls $f_i = 0$, setze $g_i := 0$)

Dann gilt: Ist $(c_2, \dots, c_n) \in V(J_1)$ eine partielle Lsg. der Stufe $n-1$ bzgl. J mit $(c_2, \dots, c_n) \notin V(g_1, \dots, g_s)$, dann ex. ein $c_1 \in \mathbb{C}$, sd. $(c_1, \dots, c_n) \in V(J)$.

Bew.: Sei $C := (c_2, \dots, c_n) \in V(J_1)$ mit $C \notin V(g_1, \dots, g_s)$.

Gesucht ist eine gemeinsame Nullstelle von $f_1(X_1, C), \dots, f_s(X_1, C)$.

$s=1$: $V(f_1) = V(f_1, f_1) \Rightarrow$ Beh. des Satzes folgt aus 15.4

$s=2$: Beh. des Satzes folgt direkt aus 15.4

$s \geq 3$: Wegen $C \notin V(g_1, \dots, g_s)$ können wir o.E. annehmen: $g_1(C) \neq 0$

① Seien $h_\alpha \in \mathbb{C}[X_2, \dots, X_n]$, $\alpha \in \mathbb{N}_0^{s-1}$ die verallg. Resultanten von $(f_1, \dots, f_s)$, also

$$\mathrm{Res}_{X_1}(f_1, u_2 f_2 + \dots + u_s f_s) = \sum_{\alpha \in \mathbb{N}_0^{s-1}} h_\alpha \underline{u}^\alpha$$

Beh.: Die h_α liegen alle in J_1

Bew.: Wegen 15.2(a) ex. Polynome $A, B \in \mathbb{C}[u_2, \dots, u_s, X_1, \dots, X_n]$, sd.

$$A f_1 + B(u_2 f_2 + \dots + u_s f_s) = \mathrm{Res}_{X_1}(f_1, u_2 f_2 + \dots + u_s f_s)$$

Schreibe $A = \sum_\alpha A_\alpha \underline{u}^\alpha$, $B = \sum_\beta B_\beta \underline{u}^\beta$ mit $A_\alpha, B_\beta \in \mathbb{C}[X_2, \dots, X_n]$

Wir werden durch Koeff. vergl. zeigen: $h_\alpha \in \langle f_1, \dots, f_s \rangle = J$;

wg. $h_\alpha \in \mathbb{C}[X_2, \dots, X_n]$ folgt dann $h_\alpha \in J_1$

Setze $e_1 := (1, 0, \dots, 0), \dots, e_s := (0, 0, \dots, 1)$. Es ergibt sich

$$u_2 f_2 + \dots + u_s f_s = \sum_{i=2}^{s} \underline{u}^{e_i} f_i$$

$$\Rightarrow \sum_\alpha h_\alpha \underline{u}^\alpha = \mathrm{Res}_{X_1}(f_1, u_2 f_2 + \dots + u_s f_s) = \Big(\sum_\alpha A_\alpha \underline{u}^\alpha\Big) f_1 + \Big(\sum_\beta B_\beta \underline{u}^\beta\Big)\Big(\sum_i \underline{u}^{e_i} f_i\Big)$$

$$= \Big(\sum_\alpha A_\alpha f_1\Big)\underline{u}^\alpha + \sum_{i,\beta} B_\beta f_i \underline{u}^{\beta + e_i}$$

$$= \sum_\alpha (A_\alpha f_1)\underline{u}^\alpha + \sum_\alpha \Big(\sum_{\substack{i,\beta \\ \beta + e_i = \alpha}} B_\beta f_i\Big)\underline{u}^\alpha$$

$$= \sum_\alpha \Big(A_\alpha f_1 + \sum_{\substack{i,\beta \\ \beta + e_i = \alpha}} B_\beta f_i\Big)\underline{u}^\alpha$$

$$\overset{\text{Koeffvergl.}}{\Rightarrow} h_\alpha = A_\alpha f_1 + \sum_{\substack{i,\beta \\ \beta + e_i = \alpha}} B_\beta f_i \in \langle f_1, \dots, f_s \rangle = J \Rightarrow \text{Beh.}$$

② Wegen $C \in V(J_1)$ folgt mit ①: $h_\alpha(C) = 0$ für alle $\alpha \in \mathbb{N}_0^{s-1}$.

Für $h := \mathrm{Res}_{X_1}(f_1, u_2 f_2 + \ldots + u_s f_s) \in \mathbb{C}[u_2, \ldots, u_s, X_2, \ldots, X_n]$ ist damit

$h(u_2, \ldots, u_s, C) = 0$

Wir machen folgende Annahme:

$g_2(C) \neq 0$ und f_2 hat größeren X_1-Grad als $f_3, \ldots, f_s$.

Beh.: Dann ist $h(\overleftarrow{C}, u_2, \ldots, u_s) = \mathrm{Res}_{X_1}(f_1(X_1, C), u_2 f_2(X_1, C) + \ldots + u_s f_s(X_1, C)) \overset{5.0}{=} 0$

Bew.: Der Leitkoeff. von f_1 (bzgl. X_1) ist gegeben durch g_1, und es ist $g_1(C) \neq 0$.

Der Leitkoeff. von $u_2 f_2 + \ldots + u_s f_s$ (bzgl. X_1) ist wg. obiger Annahme durch $u_2 g_2$ gegeben, und ebenfalls nach Ann. ist $g_2(C) \neq 0$.

Analog zum Bew. von 15.3 ist dann

$$h(\overleftarrow{C}, u_2, \ldots, u_s) = \mathrm{Res}_{X_1}(f_1, u_2 f_2 + \ldots + u_s f_s)(\overleftarrow{C}, u_2, \ldots, u_s)$$
$$\doteq \mathrm{Res}_{X_1}(f_1(X_1, C), u_2 f_2(X_1, C) + \ldots + u_s f_s(X_1, C))$$

③ Wegen ② ist $\mathrm{Res}_{X_1}(\underbrace{f_1(X_1, C)}, \underbrace{u_2 f_2(X_1, C) + \ldots + u_s f_s(X_1, C)}) = 0$

$\in \mathbb{C}[u_2, \ldots, u_s, X_1]$

$\overset{15.2}{\Rightarrow}$ $f_1(X_1, C)$, $u_2 f_2(X_1, C) + \ldots + u_s f_s(X_1, C)$ haben gem. Faktor F in $\mathbb{C}[u_2, \ldots, u_s, X_1]$ von pos. X_1-Grad;

wegen $F \mid f_1(X_1, C) \in \mathbb{C}[X_1]$ folgt $F \in \mathbb{C}[X_1]$

Beh.: $F \mid f_2(X_1, C), \ldots, F \mid f_s(X_1, C)$

Bew.: Nach obigem gilt $F \mid u_2 f_2(X_1, C) + \ldots + u_s f_s(X_1, C) \in \mathbb{C}[X_1, u_2, \ldots, u_s]$

$\Rightarrow F(X_1) A(X_1, u_2, \ldots, u_s) = u_2 f_2(X_1, C) + \ldots + u_s f_s(X_1, C)$ für ein $A \in \mathbb{C}[X_1, u_2, \ldots, u_s]$

$\Rightarrow$ Beh. folgt aus Koeff.-vergleich.

④ Wegen ③ ist F ein gemeinsamer Faktor in $\mathbb{C}[X_1]$ von pos. X_1-Grad von $f_1(X_1,C),\dots,f_s(X_1,C)$

Sei $c_1 \in \mathbb{C}$ eine Nullstelle von F

$\Rightarrow c_1$ ist gemeinsame Nullstelle von $f_1(X_1,C),\dots,f_s(X_1,C)$,

d.h. $(c_1, C) \in V(J)$

$\Rightarrow$ Beh. des Satzes (unter der in ② getätigten Annahme)

⑤ Falls die in ② getätigte Annahme ($g_2(C) \neq 0$, f_2 hat größeren X_1-Grad als $f_3,\dots,f_s$) falsch ist:

Es ist $J = \langle f_1,\dots,f_s\rangle = \langle f_1, f_2 + X_1^N f_1, f_3,\dots,f_s\rangle$

Falls N hinreichend groß gewählt wird, ist der Leitkoeff. von $f_2 + X_1^N f_1$ durch g_1 gegeben, und es ist $g_1(C) \neq 0$.

Durch eventuelles weiteres Vergrößern von N kann man erreichen, daß $f_2 + X_1^N f_1$ größeren X_1-Grad hat als $f_3,\dots,f_s$

Obiges Argument liefert eine gem. NS c_1 von $f_1(X_1,C)$, $f_2(X_1,C) + X_1^{N_1} f_1(X_1,C),\dots,f_s(X_1,C)$

$\Rightarrow c_1$ ist gem. NS von $f_1(X_1,C), f_2(X_1,C),\dots,f_s(X_1,C)$

$\Rightarrow$ Beh.

□

Anm.: Obiger Beweis zeigt, daß der Fortsetzungssatz über jedem algebraisch abg. Körper gilt (diese Eigenschaft von $\mathbb{C}$ wird in ④ verwendet)

Kapitel IV. Das Algebra-Geometrie-Wörterbuch

Ziel: In diesem Kapitel werden wir die Abbildungen

$$\text{affine Varietäten in } K^n \quad \rightleftarrows \quad \text{Ideale in } K[X_1,\dots,X_n]$$

$$V \longmapsto I(V)$$

$$V(I) \longleftarrow I$$

studieren und Aussagen über Varietäten in Aussagen über Ideale und umgekehrt übersetzen.

§16. Der Hilbertsche Nullstellensatz

Def. 16.1: K Körper. K heißt algebraisch abgeschlossen $\Leftrightarrow$ Jedes nichtkonstante Polynom in $K[X]$ hat eine Nullstelle in K

Bsp. 16.2:
- $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra)
- $\mathbb{R}$ ist nicht algebraisch abgeschlossen, denn das Polynom $X^2+1 \in \mathbb{R}[X]$ hat keine Nullstelle in $\mathbb{R}$

Bem. 16.3: K alg. abgeschl. Körper ~~$\Rightarrow K[X]$. Dann trivialerweise~~. Dann gilt: K hat unendlich viele Elemente

Bew.: Ann.: K endlich, etwa $K = \{a_1,\dots,a_n\}$.

Setze $f := \prod_{i=1}^{n}(X-a_i) + 1 \in K[X]$

Dann ist $f(a_i) = 1$ für alle $i \in \{1,\dots,n\}$, d.h. f hat keine Nullstelle in K ↯

Bem. 16.4: K alg. abgeschl. Körper, $f \in K[X]$. Dann sind äquivalent:

(i) $V(f) = \emptyset$

(ii) $\langle f \rangle = K[X]$

Bew.: $V(f) = \emptyset \Leftrightarrow f$ hat keine NS in $K \overset{K \text{ alg.abg.}}{\Leftrightarrow} f$ konstant, $f \neq 0 \Leftrightarrow \langle f \rangle = \langle 1 \rangle = K[X]$.

Anm.: Im Fall $K = \mathbb{C}$ kann man diese Aussage als Umformulierung des Fundamentalsatzes der Algebra ansehen. Der Schwache Nullstellensatz verallgemeinert die Aussage auf Polynome in mehreren Variablen.

Satz 16.5: (Schwacher Nullstellensatz) K Körper, K alg. abg., $J \subset K[X_1,\dots,X_n]$ Ideal.

Dann sind äquivalent:

(i) $V(J) = \emptyset$

(ii) $J = K[X_1,\dots,X_n]$

Bew.: (ii)$\Rightarrow$(i) Es ist $V(K[X_1,\dots,X_n]) = \emptyset$ wg. $1 \in K[X_1,\dots,X_n]$.

(i)$\Rightarrow$(ii) Bew. per Induktion nach n

$n=1$: Nach 4.9 ex. ein $f \in J$, sd. $J = \langle f \rangle$. Beh. folgt aus 16.4.

Induktionsschritt: Die Beh. sei bewiesen für $K[X_2,\dots,X_n]$.

Sei $J \subsetneq K[X_1,\dots,X_n]$ mit $V(J) = \emptyset$.

Sei $(a_2,\dots,a_n) \in K^{n-1}$. Wir betrachten die Abb.

$$\Phi: K[X_1,\dots,X_n] \longrightarrow K[\tilde{X}_1,\dots,\tilde{X}_n]$$

$$\sum_{\underline{i} \in \mathbb{N}_0^n} b_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n} \mapsto \sum_{\underline{i} \in \mathbb{N}_0^n} b_{\underline{i}} \tilde{X}_1^{i_1} (\tilde{X}_2 + a_2 \tilde{X}_1)^{i_2} \cdots (\tilde{X}_n + a_n \tilde{X}_1)^{i_n}$$

① **Beh.:** Φ ist eine bijektive Abbildung mit der Eigenschaft

$$\Phi(f+g) = \Phi(f) + \Phi(g), \quad \Phi(fg) = \Phi(f)\,\Phi(g) \quad \text{für alle } f,g \in K[X_1,\dots,X_n]$$

Bew.: Setzt man

$$\Psi: K[\tilde{X}_1,\dots,\tilde{X}_n] \longrightarrow K[X_1,\dots,X_n]$$

$$\sum_{\underline{i} \in \mathbb{N}_0^n} b_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n} \mapsto \sum_{\underline{i} \in \mathbb{N}_0^n} b_{\underline{i}} X_1^{i_1} (X_2 - a_2 X_1)^{i_2} \cdots (X_n - a_n X_1)^{i_n},$$

rechnet man leicht nach: $\Phi \circ \Psi = \mathrm{id}_{K[\tilde{X}_1,\dots,\tilde{X}_n]}$, $\Psi \circ \Phi = \mathrm{id}_{K[X_1,\dots,X_n]}$

Die Verträglichkeit mit „+" und „·" rechnet man ebenfalls nach.

② **Beh.:** $\tilde{J} := \Phi(J)$ ist ein Ideal in $K[\tilde{X}_1,\dots,\tilde{X}_n]$ mit $V(\tilde{J}) = \emptyset$.

Es gilt ferner: $J = K[X_1,\dots,X_n] \Leftrightarrow \tilde{J} = K[\tilde{X}_1,\dots,\tilde{X}_n]$

Bew.: $\cdot\ 0 = \Phi(0) \in \tilde{J}$

· Seien $\tilde{f},\tilde{g} \in \tilde{J} \Rightarrow$ Es ex. $f,g \in J$ sd. $\tilde{f} = \Phi(f)$, $\tilde{g} = \Phi(g)$

$\Rightarrow \tilde{f}+\tilde{g} = \Phi(f)+\Phi(g) \overset{①}{=} \Phi(f+g) \in \Phi(J) = \tilde{J}$.

· Sei $\tilde{f}\in\tilde{J}$, $\tilde{h}\in K[\tilde{X}_{1,\dots,}\tilde{X}_n] \overset{\Phi\text{ surj.}}{\Rightarrow}$ Es ex. $f\in J$, $h\in K[X_{1,\dots,}X_n]$, sd.

$\tilde{f} = \Phi(f)$, $\tilde{h} = \Phi(h) \Rightarrow \tilde{h}\tilde{f} = \Phi(h)\Phi(f) \overset{②}{=} \Phi(\underbrace{hf}_{\in J}) \in \Phi(J) = \tilde{J}$.

$\Rightarrow \tilde{J}$ Ideal in $K[\tilde{X}_{1,\dots,}\tilde{X}_n]$.

Sei $(a_{1,\dots,}a_n)\in K^n$ mit $(a_{1,\dots,}a_n)\in V(\tilde{J})$.

Sei $f\in J$, setze $\tilde{f} := \Phi(f)$

$\overset{\tilde{f}\in\tilde{J}}{\Rightarrow} \tilde{f}(a_{1,\dots,}a_n) = 0 \Rightarrow f(a_1, a_2+a_2a_1,\dots, a_n+a_na_1) = 0$

Da $f\in J$ beliebig war, folgt $(a_1, a_2+a_2a_1 \dots, a_n+a_na_1)\in V(J)$ ↯ zu $V(J)=\emptyset$

Also $V(\tilde{J})=\emptyset$.

Falls $J = K[X_{1,\dots,}X_n] \overset{\Phi\text{ surj.}}{\Rightarrow} \tilde{J} = \Phi(J) = K[\tilde{X}_{1,\dots,}\tilde{X}_n]$

Falls $\tilde{J} = K[\tilde{X}_{1,\dots,}\tilde{X}_n] \Rightarrow \Phi(J) = \Phi(K[X_{1,\dots,}X_n]) \overset{\Phi\text{ inj.}}{\Rightarrow} J = K[X_{1,\dots,}X_n]$.

③ Beh.: Ist $f\in K[X_{1,\dots,}X_n]$ mit $\deg(f) =: N \geq 1$, dann ist

$$\Phi(f) = c(a_{2,\dots,}a_n)\,\tilde{X}_1^N + \text{Terme von } \tilde{X}_1\text{-Grad} < N,$$

wobei $c\in K[t_{2,\dots,}t_n]\setminus\{0\}$

Bew.: Wir können f schreiben als

$$f = h_N + h_{N-1} + \dots + h_0 \qquad h_0,\dots,h_N\in K[X_{1,\dots,}X_n],\ h_N\neq 0,$$

wobei jedes Monom in h_i Totalgrad i habe (für $i = 0,\dots,N$)

Offenbar ist $\Phi(h_i)$ ein Polynom vom Totalgrad $\leq i$.

$$\Rightarrow \Phi(f) = \Phi(h_N + h_{N-1} + \dots + h_0) \overset{②}{=} \Phi(h_N) + \Phi(h_{N-1}) + \dots + \Phi(h_0)$$
$$= \Phi(h_N) + \text{Terme von Totalgrad} < N$$

Sei $h_N = \sum_{\substack{i\in\mathbb{N}_0^n \\ |i|=N}} b_i\, X_1^{i_1}\cdot\dots\cdot X_n^{i_n}$

$$\Rightarrow \Phi(h_N) = \sum_{\substack{i\in\mathbb{N}_0^n \\ |i|=N}} b_i\, \tilde{X}_1^{i_1}(\tilde{X}_2+a_2\tilde{X}_1)^{i_2}\cdot\dots\cdot(\tilde{X}_n+a_n\tilde{X}_1)^{i_n}$$

$$= \tilde{X}_1^N \sum_{\substack{i \in \mathbb{N}_0^n \\ |i|=N}} b_i a_2^{i_2} \cdot \ldots \cdot a_n^{i_n} + \text{Terme von } \tilde{X}_1\text{-Grad} < N$$

$$= \tilde{X}_1^N h_N(1, a_{2,\ldots,} a_n) + \quad -\!\!-\!\!-$$

$$\Rightarrow \phi(f) = \tilde{X}_1^N h_N(1, a_2, \ldots, a_n) + \quad -\!\!-\!\!-$$

Setze $c := h_N(1, t_2, \ldots, t_n) \in K[t_{2,\ldots,} t_n]$, dann ist

$\phi(f) = c(a_{2,\ldots,} a_n) \tilde{X}_1^N +$ Terme von $\tilde{X}_1$-Grad $< N$

Ann.: $c = 0$

$$\Rightarrow 0 = h_N(1, t_{2,\ldots,} t_n) = \sum_{\substack{i \in \mathbb{N}_0^n \\ |i|=N}} b_i t_2^{i_2} \cdot \ldots \cdot t_n^{i_n}$$

Sind $i, j \in \mathbb{N}_0^n$ mit $|i| = |j| = N$ und $i \neq j$, dann ist auch

$(i_{2,\ldots,} i_n) \neq (j_{2,\ldots,} j_n)$.

$\Rightarrow b_i = 0$ für alle $i \in \mathbb{N}_0^n$ mit $|i| = N$

$$\Rightarrow h_N = \sum_{\substack{i \in \mathbb{N}_0^n \\ |i|=N}} b_i t_1^{i_1} \cdot \ldots \cdot t_n^{i_n} = 0 \quad \lightning$$

Also $c \neq 0$.

④ Sei $J = \langle f_1, f_{2,\ldots,} f_s \rangle$. Man rechnet leicht nach: $\tilde{J} = \tilde{\Phi}(J) = \langle \tilde{\Phi}(f_1)_{,\ldots,} \tilde{\Phi}(f_s) \rangle$.

Falls f_1 konstantes Polynom $\neq 0$, dann folgt $1 \in J$, dh. $J = K[X_{1,\ldots,} X_n]$.

Sei im folgenden also $N := \deg(f) \geq 1$

Nach ③ ist

$\tilde{\Phi}(f_1) = c(a_{2,\ldots,} a_n) \tilde{X}_1^N +$ Terme von $\tilde{X}_1$-Grad $< N$,

hierbei ist $c \in K[t_{2,\ldots,} t_n] \setminus \{0\}$.

Da K wg. 16.3 unendlich ist, können wir nach 1.11 $(a_{2,\ldots,} a_n) \in K^{n-1}$

so wählen, daß $c(a_{2,\ldots,} a_n) \neq 0$ ist.

Es sei $\pi_1 : K^n \to K^{n-1}$ die Proj.abb. auf die letzten $n-1$ Komp.

Setze $\tilde{J}_1 = \tilde{J} \cap K[\tilde{X}_{2,\ldots,} \tilde{X}_n]$.

$\overset{12.4}{\Rightarrow}$ $V(\tilde{J}_1) = \pi_1(V(\tilde{J}))$

(gilt auch für K alg. abg.)

$\Rightarrow V(\tilde{J}_1) = \pi_1(\emptyset) = \emptyset$

$\overset{IV}{\Rightarrow} \tilde{J}_1 = K[\tilde{X}_2, \dots, \tilde{X}_n] \Rightarrow 1 \in \tilde{J}_1 \subset \tilde{J}$

$\Rightarrow \tilde{J} = K[\tilde{X}_1, \dots, \tilde{X}_n]$

$\Rightarrow J = K[X_1, \dots, X_n]$. □

Folgerung 16.6: (Lösung des Konsistenzproblems) K algebraisch abg., $f_1, \dots, f_s \in K[X_1, \dots, X_n]$. Dann sind äquivalent:

(i) $V(f_1, \dots, f_s) = \emptyset$

(ii) $\{1\}$ ist die reduzierte Gröbnerbasis von $\langle f_1, \dots, f_s \rangle$ (bzgl. irgendeiner Monomordnung)

Anm.: Damit läßt sich insbesondere algorithmisch überprüfen, ob ein alg. GS $f_1 = \dots = f_s = 0$ über K eine Lösung besitzt (ohne diese auszurechnen).

Bew.: (i) $\overset{16.5}{\Leftrightarrow}$ $\langle f_1, \dots, f_s \rangle = \langle 1 \rangle \Leftrightarrow$ red. Gröbnerbasis von $\langle f_1, \dots, f_s \rangle$ ist $\{1\}$. □

Ziel: Wir haben bereits in Kap. I gesehen, daß verschiedene Ideale dieselben Varietäten liefern können. (z.B. ist $V(\langle X, Y \rangle) = V(\langle X^2, Y \rangle)$ in K^2).
In diesem Bsp. ist die Ursache dafür, daß die Potenz eines Polynoms auf derselben Menge verschwindet wie das Polynom selbst.
Wir werden im Anschluß den Hilbertschen Nullstellensatz beweisen. Dieser besagt, daß über algebraisch abgeschlossenen Körpern der obige Grund der einzige ist, daß verschiedene Ideale dieselbe Varietät liefern: Verschwindet f auf $V(J)$, dann gibt es eine Potenz von f, die zu J gehört.

Satz 16.7: (Hilbertscher Nullstellensatz)
K alg. abg. Körper, $f, f_1, \dots, f_s \in K[X_1, \dots, X_n]$
Dann sind äquivalent:

(i) $f \in J(V(f_1, \dots, f_s))$

(ii) Es ex. ein $m \geq 1$, sd. $f^m \in \langle f_1, \dots, f_s \rangle$

Bew.: (ii)⇒(i) Sei $f^m \in \langle f_1, \dots, f_s \rangle$.

Ist $a \in V(f_1, \dots, f_s)$, dann ist $f^m(a) = 0 \Rightarrow f(a) = 0$

$\Rightarrow f \in \mathcal{J}(V(f_1, \dots, f_s))$.

(i)⇒(ii) Sei $f \in \mathcal{J}(V(f_1, \dots, f_s))$.

Setze $\tilde{J} := \langle f_1, \dots, f_s, 1 - Yf \rangle \subset K[X_1, \dots, X_n, Y]$

Beh.: $V(\tilde{J}) = \emptyset$

Bew.: Sei $(a_1, \dots, a_n, a_{n+1}) \in K^{n+1}$

1. Fall: $(a_1, \dots, a_n)$ ist eine gemeinsame NS von $f_1, \dots, f_s$.

$f \in \mathcal{J}(V(f_1, \dots, f_s))$

$\Rightarrow f(a_1, \dots, a_n) = 0$

$\Rightarrow (1 - Yf)(a_1, \dots, a_{n+1}) = 1 - a_{n+1} f(a_1, \dots, a_n) = 1 \neq 0.$

$\Rightarrow (a_1, \dots, a_{n+1}) \notin V(\tilde{J})$.

2. Fall: $(a_1, \dots, a_n)$ ist keine gemeinsame NS von $f_1, \dots, f_s$.

Da die Polynome $f_1, \dots, f_s$ nur von $X_1, \dots, X_n$ abhängen,

ist $(a_1, \dots, a_{n+1})$ keine gemeinsame NS von $f_1, \dots, f_s, 1 - Yf$.

$\Rightarrow (a_1, \dots, a_{n+1}) \notin V(\tilde{J})$.

⇒ Beh.

Nach dem schwachen Nullstellensatz folgt: $1 \in \tilde{J}$.

$\Rightarrow$ Es ex. $p_i, q \in K[X_1, \dots, X_n, Y]$, $i = 1, \dots, s$, sd.

$$1 = \sum_{i=1}^{s} p_i f_i + q(1 - Yf)$$

Wir betrachten diese Gleichung in $K(X_1, \dots X_n)[Y]$ und setzen dort

$Y = \frac{1}{f} \in K(X_1, \dots X_n)$ ein:

$$1 = \sum_{i=1}^{s} p_i\left(X_1, \dots X_n, \frac{1}{f}\right) f_i$$

Multiplikation mit f^m für hinreichend großes m ergibt:

$f^m = \sum_{i=1}^{s} A_i f_i$ mit $A_1, \dots A_s \in K[X_1, \dots, X_n]$. $\Rightarrow f^m \in \langle f_1, \dots f_s \rangle$ □

§17. Radikalideale und die Korrespondenz zwischen Idealen und Varietäten

Bem. 17.1: K Körper, $V \subset K^n$ affine Varietät, $f \in K[X_1, \dots, X_n]$, $m \geq 1$. Dann gilt:

$$f^m \in I(V) \Rightarrow f \in I(V)$$

Bew.: $f^m \in I(V) \Rightarrow f(\alpha)^m = 0$ für alle $\alpha \in V \Rightarrow f(\alpha) = 0$ für alle $\alpha \in V$. □

Def. 17.2: K Körper, $I \subset K[X_1, \dots, X_n]$ Ideal.

I heißt **Radikalideal** $\overset{\text{Def}}{\Leftrightarrow}$ $f^m \in I$ für ein $f \in K[X_1, \dots, X_n]$, $m \geq 1$ impliziert stets $f \in I$

Folgerung 17.3: K Körper, $V \subset K^n$ affine Varietät. Dann gilt:

$I(V)$ ist ein Radikalideal.

Def. 17.4: K Körper, $I \subset K[X_1, \dots, X_n]$ Ideal.

$$\sqrt{I} := \{ f \in K[X_1, \dots, X_n] \mid \exists m \geq 1 : f^m \in I \}$$

heißt das **Radikal** von I.

Bem. 17.5: K Körper, $I \subset K[X_1, \dots, X_n]$ Ideal. Dann gilt:

(a) $\sqrt{I}$ ist ein Ideal in $K[X_1, \dots, X_n]$ mit $\sqrt{I} \supset I$.

(b) $\sqrt{I}$ ist ein Radikalideal.

Bew.: (a) $\cdot\ \sqrt{I} \supset I$ klar nach Def.

$\sqrt{I}$ ist Ideal in $K[X_1, \dots, X_n]$:

- $0 \in \sqrt{I}$, da $0 \in I$
- Seien $f, g \in \sqrt{I} \Rightarrow \exists m, l \geq 1 : f^m, g^l \in I$, o.E. $m \geq l$, d.h. $f^m, g^m \in I$

  Es ist $(f+g)^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} f^i g^{2m-i}$

  Es gilt für alle Summanden: $i \geq m$ oder $2m - i \geq m$, d.h. $f^i \in I$ oder $g^{2m-i} \in I$

  $\Rightarrow$ Jeder Summand liegt in I

  $\Rightarrow (f+g)^{2m} \in I$

  $\Rightarrow f + g \in \sqrt{I}$

· Sei $f \in \sqrt{J}$, $h \in K[X_{1,\dots,}X_n] \Rightarrow \exists m \geq 1: f^m \in J$

$\Rightarrow (hf)^m = h^m f^m \in J$

$\Rightarrow hf \in \sqrt{J}$

(b) Sei $f \in K[X_{1,\dots}X_n]$ mit $f^m \in \sqrt{J}$ für ein $m \geq 1$

$\Rightarrow \exists \tilde{m} \geq 1: (f^m)^{\tilde{m}} \in J \Rightarrow f^{m\tilde{m}} \in J \Rightarrow f \in \sqrt{J}$.

Bsp. 17.6: Sei $J = \langle X^2, Y^3 \rangle \subset \mathbb{Q}[X,Y]$

Beh.: $\sqrt{J} = \langle X, Y \rangle$

Bew.: „$\supset$" Wegen $X^2 \in J$, $Y^3 \in J$ folgt $X \in \sqrt{J}$, $Y \in \sqrt{J}$.

$\Rightarrow \sqrt{J} \supset \langle X,Y \rangle$

„$\subset$" Sei $f \in \sqrt{J}$, dh. es ex. $m \geq 1$, sd. $f^m \in \langle X^2, Y^3 \rangle$

$\Rightarrow f^m = h_1 X^2 + h_2 Y^3$ für geeignete $h_1, h_2 \in \mathbb{Q}[X,Y]$

$\Rightarrow f^m(0,0) = h_1(0,0) \cdot 0 + h_2(0,0) \cdot 0 = 0$

$\Rightarrow f(0,0) = 0$

$\Rightarrow f \in \langle X,Y \rangle$.

Bem. 17.7: K Körper, $J \subset K[X_{1,\dots},X_n]$ Ideal. Dann sind äquivalent:

(i) J ist ein Radikalideal

(ii) $J = \sqrt{J}$

Bew.: (i)$\Rightarrow$(ii) Sei J Radikalideal, $f \in \sqrt{J} \Rightarrow \exists m \geq 1: f^m \in J \overset{J \text{ Rad.id}}{\Rightarrow} f \in J$,

dh. $\sqrt{J} \subset J$. Die andere Inkl. gilt ohnehin (vgl. 17.5(a)).

(ii)$\Rightarrow$(i) Sei $f \in K[X_{1,\dots},X_n]$ mit $f^m \in J$ für ein $m \geq 1$

$\Rightarrow f \in \sqrt{J} \overset{\sqrt{J}=J}{\Rightarrow} f \in J$. □

Satz 17.8: (Starker Nullstellensatz) K alg. abg. Körper, $J \subset K[X_{1,\dots},X_n]$ Ideal.

Dann gilt: $\mathcal{I}(V(J)) = \sqrt{J}$.

Bew.: „$\supset$" Sei $f \in \sqrt{J} \Rightarrow \exists m \geq 1: f^m \in J \Rightarrow f^m(a) = 0 \ \forall a \in V(J)$

$\Rightarrow f(a) = 0 \ \forall a \in V(J) \Rightarrow f \in \mathcal{I}(V(J))$.

„⊂" Sei $f \in \mathcal{J}(V(J)) \overset{\text{Hilb. NS-Satz}}{\Rightarrow} \exists m \geq 1 : f^m \in J \Rightarrow f \in \sqrt{J}$. □

Satz 17.9: (Korrespondenz zwischen Idealen und Varietäten)

K Körper, $n \in \mathbb{N}$. Dann gilt:

(a) Die Abbildungen

$$\text{affine Varietäten im } K^n \xrightarrow{\mathcal{J}} \text{Ideale in } K[X_1, \dots, X_n]$$

und

$$\text{Ideale in } K[X_1, \dots, X_n] \xrightarrow{\mathcal{V}} \text{affine Varietäten im } K^n$$

sind inklusionsumkehrend.

Des weiteren gilt für jede Varietät V in K^n:

$$V(\mathcal{J}(V)) = V,$$

d.h. $\mathcal{J}$ ist injektiv.

(b) Ist K algebraisch abgeschlossen, dann sind die Abbildungen

$$\text{affine Varietäten im } K^n \xrightarrow{\mathcal{J}} \text{Radikalideale in } K[X_1, \dots, X_n]$$

$$\text{Radikalideale in } K[X_1, \dots, X_n] \xrightarrow{\mathcal{V}} \text{affine Varietäten in } K^n$$

inklusionsumkehrende Bijektionen, die zueinander invers sind.

Bew.: (a) ① Seien $J_1, J_2 \subset K[X_1, \dots, X_n]$ Ideale mit $J_1 \subset J_2$.

Sei $a \in V(J_2) \Rightarrow f(a) = 0 \ \forall f \in J_2 \Rightarrow f(a) = 0 \ \forall f \in J_1 \Rightarrow a \in V(J_1)$

② Seien $V_1, V_2 \subset K^n$ Varietäten mit $V_1 \subset V_2$.

Sei $f \in \mathcal{J}(V_2) \Rightarrow f(a) = 0 \ \forall a \in V_2 \Rightarrow f(a) = 0 \ \forall a \in V_1 \Rightarrow f \in \mathcal{J}(V_1)$.

③ Sei $V \subset K^n$ eine affine Varietät

zz.: $V(\mathcal{J}(V)) = V$

Bew.: „⊃" $a \in V \Rightarrow f(a) = 0 \ \forall f \in \mathcal{J}(V) \Rightarrow a \in V(\mathcal{J}(V))$.

„⊂" Sei $V = V(J)$ für ein Ideal $J \subset K[X_1, \dots, X_n]$

$\Rightarrow J \subset \mathcal{J}(V) \overset{①}{\Rightarrow} V(\mathcal{J}(V)) \subset V(J) = V$

(b) Die Abb. $\mathcal{J}$: affine Varietäten im $K^n \longrightarrow$ Radikalideale in $K[X_1, \dots, X_n]$ ist wohldef. nach 17.3

Wissen bereits: $V(\mathcal{J}(V)) = V$ für alle affinen Var. im K^n.

Noch zz.: Ist $J \subset K[X_1,\dots,X_n]$ ein Radikalideal, dann ist $J(V(J)) = J$

Bew.: Wegen starkem Nullstellensatz (17.8) ist $J(V(J)) = \sqrt{J} \underset{17.7}{=} J$.

Damit sind J, V zueinander invers (u. insb. bijektiv) □

Bem. 17.10: (Radikalmitgliedschaft)

K Körper, $f_1,\dots,f_s \in K[X_1,\dots X_n]$, $J = \langle f_1,\dots,f_s\rangle$, $\tilde{J} = \langle f_1,\dots,f_s, 1-Yf\rangle \subset K[Y,X_1,\dots,X_n]$.

Dann sind äquivalent:

(i) $f \in \sqrt{J}$

(ii) $\tilde{J} = K[Y,X_1,\dots,X_n]$

(iii) $\{1\}$ ist die reduzierte Gröbnerbasis von $\tilde{J}$ (bzgl. irgendeiner Monomordnung)

Bew.: (i)⇒(ii) Sei $f \in \sqrt{J}$, Dann ex. ein $m \geq 1$, sd. $f^m \in J \subset \tilde{J}$

Wegen $1-Yf \in \tilde{J}$ folgt

$$1 = Y^m f^m + (1-Y^m f^m) = \underbrace{Y^m f^m}_{\in \tilde{J}} + \underbrace{(1-Yf)}_{\in \tilde{J}}(1+Yf+\dots+Y^{m-1}f^{m-1}) \in \tilde{J}$$

$$\Rightarrow \tilde{J} = K[Y,X_1,\dots,X_n].$$

(ii)⇒(i) Vgl. Bew. zu Hilberts Nullstellensatz (die folgenden Implikationen benötigen nicht, dass K alg. abg. ist)

$$1 \in \tilde{J} \Rightarrow 1 = \sum_{i=1}^{s} p_i f_i + q\,(1-Yf) \quad \text{mit } p_1,\dots,p_s, q \in K[X_1,\dots,X_n,Y]$$

Betrachte diese Gleichung in $K(X_1,\dots,X_n)[Y]$, setze $Y = \frac{1}{f}$.

Multipliziere die entstehende Gleichung mit f^m für hinreichend großes m

$$\Rightarrow f^m = \sum_{i=1}^{s} A_i f_i \in \langle f_1,\dots,f_s\rangle$$

$$\Rightarrow f \in \sqrt{J}$$

(ii)⇔(iii) klar. □

Anm.: Dies liefert insbesondere einen Algorithmus zur Bestimmung, ob $f \in \sqrt{J}$.

Einen Algorithmus zur Berechnung von $\sqrt{J}$ anzugeben, ist ebenfalls möglich, allerdings deutlich schwieriger.

Bsp. 17.11: $J = \langle XY^2+2Y^2, X^4-2X^2+1\rangle \subset \mathbb{Q}[X,Y]$

Ist $f = Y-X^2+1 \in \sqrt{J}$?

$\tilde{J} = \langle XY^2+2Y^2, X^4-X^2+1, 1-Z(Y-X^2+1)\rangle \subset \mathbb{Q}[X,Y,Z]$

$\tilde{J}$ hat reduzierte Gröbnerbasis $\{1\}$

Mit Hilfe einer Gröbnerbasis von J rechnet man nach: $f^3 \in J$, aber $f, f^2 \notin J$

Geometrisch: $V(J) = \{(\pm 1, 0)\}$, $f \in J(V(J))$, aber $f \notin J$.

Behn. 17.12: K Körper, $f \in K[X_1,\dots,X_n]$, $J = \langle f\rangle$, $f = f_1^{e_1} \cdot \dots \cdot f_s^{e_s}$ mit $f_1,\dots,f_s \in K[X_1,\dots,X_n]$ irreduzibel, paarw. versch. Dann gilt:

$$\sqrt{J} = \sqrt{\langle f\rangle} = \langle f_1 \cdot \dots \cdot f_s\rangle.$$

Bew.: „$\supset$" Sei $N := \max_{i=1,\dots,s} e_i$

$\Rightarrow f \mid (f_1 \cdot \dots \cdot f_s)^N \Rightarrow (f_1 \cdot \dots \cdot f_s)^N \in J \Rightarrow f_1 \cdot \dots \cdot f_s \in \sqrt{J} \Rightarrow \langle f_1 \cdot \dots \cdot f_s\rangle \subset \sqrt{J}$.

„$\subset$" Sei $g \in \sqrt{J}$. Dann ex. $M \geq 1$, sd. $g^M \in J$.

$\Rightarrow$ Es ex. $h \in K[X_1,\dots,X_n]$, sd. $g^M = hf$

Sei $g = g_1^{d_1} \cdot \dots \cdot g_r^{d_r}$ mit $g_1,\dots,g_r \in K[X_1,\dots,X_n]$ irreduzibel, paarw. versch.

$\Rightarrow g^M = g_1^{d_1 M} \cdot \dots \cdot g_r^{d_r M} = h f_1^{e_1} \cdot \dots \cdot f_s^{e_s}$

$\overset{14.6}{\underset{f_i \text{ irred.}}{\Rightarrow}}$ Jedes f_i ist konstantes Vielfaches von einem der g_j

$\Rightarrow f_1 \cdot \dots \cdot f_s \mid g$

$\Rightarrow g \in \langle f_1 \cdot \dots \cdot f_s\rangle$ □

Anm.: Man nennt $f_1 \cdot \dots \cdot f_s$ auch Reduktion von f, Bez.: f_{red} (Diese ist allerdings nur bis auf Multipl. mit Konstanten eindeutig).

Falls $\mathbb{Q} \subset K$, kann f_{red} auch ohne Faktorisierung von f berechnet werden.

Bsp. 17.13: $f = Y^3(X+1)X^5 \in \mathbb{Q}[X,Y]$

$\Rightarrow \sqrt{\langle f\rangle} = \langle Y(X+1)X\rangle$.

§18. Summe, Produkt und Durchschnitt von Idealen

Def. 18.1: K Körper, $I, J \subset K[X_1, \dots, X_n]$ Ideale

$I + J := \{ f + g \mid f \in I, g \in J \}$ heißt die Summe von I und J

Bem. 18.2: K Körper, $I, J \subset K[X_1, \dots, X_n]$ Ideale. Dann gilt:

(a) $I + J$ ist ein Ideal in $K[X_1, \dots, X_n]$.

(b) $I + J$ ist das kleinste Ideal in $K[X_1, \dots, X_n]$, das I und J enthält.

(c) Ist $I = \langle f_1, \dots, f_s \rangle$, $J = \langle g_1, \dots, g_t \rangle$, dann ist $I + J = \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$

Bew.: (a) ① $0 = 0 + 0 \in I + J$

② Seien $h_1, h_2 \in I + J \Rightarrow$ Es ex. $f_1, f_2 \in I$, $g_1, g_2 \in J$, sd. $h_1 = f_1 + g_1$, $h_2 = f_2 + g_2$

$$\Rightarrow h_1 + h_2 = (f_1 + g_1) + (f_2 + g_2) = (\underbrace{f_1 + f_2}_{\in I} + \underbrace{(g_1 + g_2)}_{\in J}) \in I + J$$

③ Sei $h \in I + J$, $p \in K[X_1, \dots, X_n]$

$\Rightarrow$ Es ex. $f \in I$, $g \in J$, sd. $h = f + g$

$\Rightarrow ph = p(f + g) = pf + pg \in I + J$.

(b) Sei $H \subset K[X_1, \dots, X_n]$ Ideal mit $H \supset I$, $H \supset J$

$\overset{H \text{ Ideal}}{\Rightarrow} H \supset \{ f + g \mid f \in I, g \in J \} = I + J$.

(c) „$\subset$" $I, J \subset \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle \overset{(b)}{\Rightarrow} I + J \subset \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$

„$\supset$" klar. □

Folgerung 18.3: K Körper, $f_1, \dots, f_r \in K[X_1, \dots, X_n]$. Dann gilt:

$$\langle f_1, \dots, f_r \rangle = \langle f_1 \rangle + \dots + \langle f_r \rangle$$

Bem. 18.4: K Körper, $I, J \subset K[X_1, \dots, X_n]$ Ideale.

Dann gilt: $V(I + J) = V(I) \cap V(J)$.

Bew.: „$\subset$" Sei $a \in V(I + J) \Rightarrow a \in V(I)$ wg. $I \subset I + J$, analog $a \in V(J)$

$\Rightarrow a \in V(I) \cap V(J)$

„$\supset$" Sei $a \in V(I) \cap V(J)$, $h \in I + J \Rightarrow$ Es ex. $f \in I, g \in J$, sd. $h = f + g$

$\overset{\substack{a \in V(I) \\ a \in V(J)}}{\Rightarrow} h(a) = f(a) + g(a) = 0 + 0 = 0$. Damit $a \in V(I + J)$. □

Def. 18.5: K Körper, $\mathfrak{I},\mathfrak{J} \subset K[X_1,\dots,X_n]$ Ideale

$$\mathfrak{I}\mathfrak{J} := \{ f_1 g_1 + \dots + f_r g_r \mid f_1,\dots,f_r \in \mathfrak{I},\ g_1,\dots,g_r \in \mathfrak{J},\ r \geq 1 \}$$

heißt das Produkt von $\mathfrak{I}$ und $\mathfrak{J}$

Bem. 18.6: K Körper, $\mathfrak{I},\mathfrak{J} \subset K[X_1,\dots,X_n]$ Ideale. Dann gilt:

(a) $\mathfrak{I}\mathfrak{J}$ ist ein Ideal in $K[X_1,\dots,X_n]$ mit $\mathfrak{I}\mathfrak{J} \subseteq \mathfrak{I} \cap \mathfrak{J}$.

(b) Ist $\mathfrak{I} = \langle f_1,\dots,f_r \rangle$, $\mathfrak{J} = \langle g_1,\dots,g_s \rangle$, dann ist

$$\mathfrak{I}\mathfrak{J} = \langle f_i g_j \mid i = 1,\dots,r,\ j = 1,\dots,s \rangle$$

Bew.: (a) ① $0 = 0 \cdot 0 \in \mathfrak{I}\mathfrak{J}$

② $h_1, h_2 \in \mathfrak{I}\mathfrak{J} \overset{\text{Def } \mathfrak{I}\mathfrak{J}}{\Rightarrow} h_1 + h_2 \in \mathfrak{I}\mathfrak{J}$

③ $h \in \mathfrak{I}\mathfrak{J}$, $p \in K[X_1,\dots,X_n]$

$\Rightarrow$ Es ex. $f_1,\dots,f_r \in \mathfrak{I}$, $g_1,\dots,g_r \in \mathfrak{J}$, sd. $h = f_1 g_1 + \dots + f_r g_r$

$\Rightarrow ph = (pf_1) g_1 + \dots + (pf_r) g_r \in \mathfrak{I}\mathfrak{J}$

$\mathfrak{I}\mathfrak{J} \subseteq \mathfrak{I} \cap \mathfrak{J}$, da $\mathfrak{I}, \mathfrak{J}$ Ideale

(b) „$\supseteq$" klar

„$\subseteq$" Sei $h \in \mathfrak{I}\mathfrak{J} \Rightarrow h$ ist Summe von Polynomen d. Form fg mit $f \in \mathfrak{I}, g \in \mathfrak{J}$.

Es ist $f = a_1 f_1 + \dots + a_r f_r$, $g = b_1 g_1 + \dots + b_s g_s$

mit geeigneten $a_1,\dots,a_r, b_1,\dots,b_s \in K[X_1,\dots,X_n]$

$\Rightarrow fg = \sum_{i,j} c_{ij} f_i g_j$ mit geeigneten $c_{ij} \in K[X_1,\dots,X_n]$

$\Rightarrow h \in \langle f_i g_j \mid i = 1,\dots,r,\ j = 1,\dots,s \rangle$. □

Bem. 18.7: K Körper, $\mathfrak{I},\mathfrak{J} \subset K[X_1,\dots,X_n]$ Ideale. Dann gilt:

$V(\mathfrak{I}\mathfrak{J}) = V(\mathfrak{I}) \cup V(\mathfrak{J})$

Bew.: „$\subseteq$" Sei $a \in V(\mathfrak{I}\mathfrak{J}) \Rightarrow g(a)\,h(a) = gh(a) = 0$ für alle $g \in \mathfrak{I}, h \in \mathfrak{J}$.

1. Fall: $g(a) = 0$ für alle $g \in \mathfrak{I}$. Dann ist $a \in V(\mathfrak{I})$.

2. Fall: Es ex. ein $g \in \mathfrak{I}$ mit $g(a) \neq 0$

$\Rightarrow h(a) = 0$ für alle $h \in \mathfrak{J} \Rightarrow a \in V(\mathfrak{J})$.

„⊃" Sei $a \in V(J) \cup V(J)$

$\Rightarrow g(a)=0$ für alle $g \in J$ oder $h(a)=0$ für alle $h \in J$

$\Rightarrow g(a)\,h(a)=0$ für alle $g \in J, h \in J$

$\Rightarrow f(a)=0$ für alle $f \in J\cdot J$

$\Rightarrow a \in V(J\cdot J)$. □

Bem. 18.8: K Körper, $J, J \subset K[X_1, \dots, X_n]$ Ideale. Dann gilt:

(a) $J \cap J$ ist ein Ideal in $K[X_1, \dots, X_n]$

(b) $V(J \cap J) = V(J) \cup V(J)$

Bew.: (a) ① $0 \in J \cap J$ wg. $0 \in J$, $0 \in J$

② $f, g \in J \cap J \Rightarrow f+g \in J, f+g \in J \Rightarrow f+g \in J \cap J$

③ $f \in J \cap J$, $h \in K[X_1, \dots, X_n] \Rightarrow hf \in J, hf \in J \Rightarrow hf \in J \cap J$

(b) „⊃" $a \in V(J) \cup V(J) \Rightarrow f(a)=0$ für alle $f \in J$ oder $f(a)=0$ für alle $f \in J$

$\Rightarrow f(a)=0$ für alle $f \in J \cap J \Rightarrow a \in V(J \cap J)$

„⊂" Offenbar ist $J \cdot J \subset J \cap J \overset{17.9(b)}{\Rightarrow} V(J \cap J) \subset V(J\cdot J) \overset{18.7}{=} V(J) \cup V(J)$.

Bem. 18.9: K Körper, J, J Ideale in $K[X_1, \dots, X_n]$. Dann gilt:

(a) $\sqrt{J \cap J} = \sqrt{J} \cap \sqrt{J}$

(b) Sind J, J Radikalideale, dann ist $J \cap J$ ein Radikalideal.

Bew.: (a) „⊂" Sei $f \in \sqrt{J \cap J} \Rightarrow$ Es ex. $m \geq 1$: $f^m \in J \cap J \Rightarrow f^m \in J \Rightarrow f \in \sqrt{J}$,

analog $f \in \sqrt{J}$

„⊃" Sei $f \in \sqrt{J} \cap \sqrt{J} \Rightarrow$ Es ex. $m, l \geq 1$: $f^m \in J$, $f^l \in J \Rightarrow f^m f^l = f^{m+l} \in J \cdot J$

$\Rightarrow f \in \sqrt{J \cdot J}$.

(b) J, J Radikalideale $\overset{17.7}{\Rightarrow} J = \sqrt{J}$, $J = \sqrt{J} \Rightarrow \sqrt{J \cdot J} \overset{(a)}{=} \sqrt{J} \cap \sqrt{J} = J \cap J$

$\overset{17.7}{\Rightarrow} J \cap J$ ist Radikalideal.

Bsp. 18.10: Sei $J = \langle X \rangle \subset \mathbb{Q}[X] \Rightarrow J \cdot J \overset{1.16}{=} \langle X^2 \rangle \subset \mathbb{Q}[X]$, insb. ist $J \cdot J$ kein Radikalideal, obwohl J ein Radikalideal ist.

D.h.: Im allg. sind Produkte von Radikalidealen keine Radikalideale.

Anm.: Es ist zwar $V(\mathfrak{J}) = V(\mathfrak{J} \cap \mathfrak{J}) (= V(\mathfrak{J}) \cup V(\mathfrak{J}))$, allerdings ist das Bilden von Durchschnitten verträglich mit Radikalidealen; für Produkte gilt dies nicht.

Wir werden daher im folgenden einen Algorithmus zur Berechnung des Durchschnitts von Idealen studieren.

Bem. 18.11: K Körper, $p_1, \dots, p_r \in K[X_1, \dots, X_n]$, $\mathfrak{J} = \langle p_1, \dots, p_r \rangle$, $f \in K[t]$, $g \in K[X_1, \dots, X_n, t]$
Dann gilt:

(a) $f\mathfrak{J} := \underbrace{\langle f \cdot p \mid p \in \mathfrak{J} \rangle_{K[X_1,\dots,X_n,t]}}_{\text{„}\cdot\text{“ in } K[X_1,\dots,X_n,t]} = \underbrace{\langle fp_1, \dots, fp_r \rangle}_{\text{in } K[X_1,\dots,X_n,t]} \subset K[X_1, \dots, X_n, t]$

(b) Falls $g \in f\mathfrak{J}$, $a \in K$, dann ist $g(X, a) \in \mathfrak{J}$.

Bew.: (a) Sei $g \in f\mathfrak{J} \Rightarrow g$ ist Summe von Polynomen der Form hfp

mit $h \in K[X_1, \dots, X_n, t]$, $p \in \mathfrak{J}$

$\Rightarrow \exists\, q_1, \dots, q_r \in K[X_1, \dots, X_n]: p = \sum_{i=1}^{r} q_i p_i$

$\Rightarrow hfp = \sum_{i=1}^{r} hq_i f p_i \in \langle fp_1, \dots, fp_r \rangle$

$\Rightarrow g \in \langle fp_1, \dots, fp_r \rangle$.

(b) Nach (a) ist $g = \sum_{i=1}^{r} h_i f p_i$ mit geeign. $h_1, \dots, h_r \in K[X_1, \dots, X_n, t]$

$\Rightarrow g(X, a) = \sum_{i=1}^{r} h_i(X, a) f(a) p_i(X) \in \mathfrak{J}$. □

Satz 18.12: K Körper, $\mathfrak{J}, \mathfrak{J} \subset K[X_1, \dots, X_n]$. Dann gilt:

$$\mathfrak{J} \cap \mathfrak{J} = (t\mathfrak{J} + (1-t)\mathfrak{J}) \cap K[X_1, \dots, X_n]$$

Bew.: „$\subset$“ Sei $f \in \mathfrak{J} \cap \mathfrak{J}$.

Wegen $f \in \mathfrak{J}$ ist $tf \in t\mathfrak{J}$, wegen $f \in \mathfrak{J}$ folgt $(1-t)f \in (1-t)\mathfrak{J}$

$\Rightarrow f = tf + (1-t)f \in t\mathfrak{J} + (1-t)\mathfrak{J}$

Da $f \in \mathfrak{J} \cap \mathfrak{J} \subset K[X_1, \dots, X_n]$ folgt $f \in (t\mathfrak{J} + (1-t)\mathfrak{J}) \cap K[X_1, \dots, X_n]$.

„⊃" Sei $f \in (t\mathcal{I} + (1-t)\mathcal{J}) \cap K[X_1,\dots,X_n]$

$\Rightarrow f = g + h$ mit $g \in t\mathcal{I}$, $h \in (1-t)\mathcal{J}$

$\Rightarrow f = f(X,0) = \underbrace{g(X,0)}_{=0 \text{ wg. } g \in t\mathcal{I}} + h(X,0) = h(X,0) \in \mathcal{J}$ nach 18.11(b),

$f = f(X,1) = g(X,1) + \underbrace{h(X,1)}_{=0 \text{ wg. } h \in (1-t)\mathcal{J}} = g(X,1) \in \mathcal{I}$ nach 18.11(b)

$\rightarrow f \in \mathcal{I} \cap \mathcal{J}$ □

Algorithmus

~~Folgerung~~ 18.13: (Algorithmus zur Bestimmung des Durchschnitts von Idealen)

K Körper, $\mathcal{I}, \mathcal{J} \subset K[X_1,\dots,X_n]$ Ideale.

Dann gilt: Der folgende Algorithmus berechnet $\mathcal{I} \cap \mathcal{J}$.

Eingabe: $\mathcal{I} = \langle f_1,\dots,f_r \rangle$, $\mathcal{J} = \langle g_1,\dots,g_s \rangle$

Algorithmus: 1. Setze $\tilde{\mathcal{J}} := t\mathcal{I} + (1-t)\mathcal{J} = \langle tf_1,\dots,tf_r, (1-t)g_1,\dots,(1-t)g_s \rangle \subset K[X_1,\dots,X_n,t]$

2. Bestimme Gröbnerbasis $\tilde{G}$ von $\tilde{\mathcal{J}}$ bzgl. „$\geq_{lex}$" mit $t > X_1 > \dots > X_n$.

3. $G := \tilde{G} \cap K[X_1,\dots,X_n]$

Ausgabe: G ist eine Gröbnerbasis von $\mathcal{I} \cap \mathcal{J}$.

Bew.: aus 18.12 und Eliminationssatz (11.4) □

Bsp. 18.14: $\mathcal{I} = \langle X^2Y \rangle$, $\mathcal{J} = \langle XY^2 \rangle \subset \mathbb{Q}[X,Y]$

Es ist $\tilde{\mathcal{J}} = t\mathcal{I} + (1-t)\mathcal{J} = \langle tX^2Y, (1-t)XY^2 \rangle \subset \mathbb{Q}[X,Y,t]$.

Gröbnerbasis von $\tilde{\mathcal{J}}$: $\tilde{G} = \{tX^2Y, tXY^2 - XY^2, X^2Y^2\}$

$\rightarrow G = \{X^2Y^2\}$ ist Gröbnerbasis von $\mathcal{I} \cap \mathcal{J}$, also $\mathcal{I} \cap \mathcal{J} = \langle X^2Y^2 \rangle$.

In diesem Bsp. ist $\mathcal{I}\mathcal{J} = \langle X^2Y \cdot XY^2 \rangle = \langle X^3Y^3 \rangle \subsetneq \mathcal{I} \cap \mathcal{J}$.

§19. Zariski-Abschluß und der Quotient von Idealen

Def. 19.1: K Körper, $S \subset K^n$

$\mathcal{I}(S) := \{ f \in K[X_1, \dots, X_n] \mid f(a) = 0 \text{ für alle } a \in S \}$ heißt das Verschwindungsideal von S

Bem. 19.2: K Körper, $S \subset K^n$. Dann gilt:

(a) $\mathcal{I}(S)$ ist ein Radikalideal in $K[X_1, \dots, X_n]$

(b) $V(\mathcal{I}(S))$ ist die kleinste affine Varietät in K^n, die S enthält.

(d.h. ist $W \subset K^n$ eine affine Varietät mit $W \supset S$, dann ist $V(\mathcal{I}(S)) \subset W$).

Bew.: (a) Dass $\mathcal{I}(S)$ ein Ideal ist, folgt analog zum Bew. von 3.9.

Sei $f \in K[X_1, \dots, X_n]$ mit $f^m \in \mathcal{I}$ für ein $m \geq 1 \Rightarrow f^m(a) = 0 \ \forall a \in S$

$\Rightarrow f(a) = 0 \ \forall a \in S \Rightarrow f \in \mathcal{I}$, dh. $\mathcal{I}(S)$ ist Radikalideal.

(b) Sei $W \subset K^n$ affine Varietät mit $W \supset S \overset{12.9}{\Rightarrow} \mathcal{I}(W) \subset \mathcal{I}(S) \Rightarrow V(\mathcal{I}(W)) \supset V(\mathcal{I}(S))$.

W affine Varietät $\overset{12.9(a)}{\Rightarrow} V(\mathcal{I}(W)) = W$, dh. $W \supset V(\mathcal{I}(S))$.

Def.+Bem. 19.3: K Körper, $S \subset K^n$

Der Zariski-Abschluß $\bar{S}$ von S in K^n ist die kleinste affine Varietät in K^n, die S enthält.

Es ist $\bar{S} = V(\mathcal{I}(S))$.

Satz 19.4: (Satz vom Abschluß) K alg. abg. Kp., $f_1, \dots, f_s \in K[X_1, \dots, X_n]$,

$\mathcal{I} := \langle f_1, \dots, f_s \rangle$, $V := V(\mathcal{I}) \subset K^n$, $\pi_m : K^n \to K^{n-m}$ Projektionsabb. auf die letzten $n-m$ Komponenten, $\mathcal{I}_m := \mathcal{I} \cap K[X_{m+1}, \dots, X_n]$.

Dann gilt:

$V(\mathcal{I}_m) \subset K^{n-m}$ ist der Zariski-Abschluß von $\pi_m(V)$ in K^{n-m}: $V(\mathcal{I}_m) = \overline{\pi_m(V)}$

Bew.: Es ist zz.: $V(\mathcal{I}_m) = V(\mathcal{I}(\pi_m(V))$

„$\supset$" Wegen 12.1 ist $\pi_m(V) \subset V(\mathcal{I}_m)$

$V(\mathcal{I}(\pi_m(V))$ ist die kleinste affine Varietät, die $\pi_m(V)$ umfaßt

$\Rightarrow V(\mathcal{I}(\pi_m(V)) \subset V(\mathcal{I}_m)$.

„⊂" Sei $f \in \mathcal{I}(\pi_m(V)) \subset K[X_{m+1}, \dots, X_n]$.

$\Rightarrow f(a_{m+1}, \dots, a_n) = 0$ für alle $(a_{m+1}, \dots, a_n) \in \pi_m(V)$

Fasse f als Polynom in $K[X_1, \dots, X_n]$ auf

$\Rightarrow f(a_1, \dots, a_n) = 0$ für alle $(a_1, \dots, a_n) \in V = V(\mathcal{I}) \Rightarrow f \in \mathcal{I}(V(\mathcal{I}))$

$\overset{\text{Hilb. NS-Satz}}{\Rightarrow}$ Es ex. $N \geq 1$, sd. $f^N \in \mathcal{I}$

Wg. $f \in K[X_{m+1}, \dots, X_n]$ ist $f^N \in \mathcal{I} \cap K[X_{m+1}, \dots, X_n] = \mathcal{I}_m$

$\Rightarrow f \in \sqrt{\mathcal{I}_m}$

Damit: $\mathcal{I}(\pi_m(V)) \subset \sqrt{\mathcal{I}_m}$

$\Rightarrow V(\mathcal{I}_m) = V(\sqrt{\mathcal{I}_m}) \underset{17.9}{\subset} V(\mathcal{I}(\pi_m(V)))$. □

Ziel: Sind V, W affine Varietäten in K^n mit $W \subset V$, dann ist $V \setminus W$ im allg. keine Varietät, jedoch $\overline{V \setminus W}$. Was ist das idealtheoret. Analogon zu $\overline{V \setminus W}$?

Def. 19.5: K Körper, $\mathcal{I}, \mathcal{J} \subset K[X_1, \dots, X_n]$ Ideale

$$\mathcal{I} : \mathcal{J} = \{ f \in K[X_1, \dots, X_n] \mid fg \in \mathcal{I} \text{ für alle } g \in \mathcal{J} \}$$

heißt der Idealquotient von $\mathcal{I}$ durch $\mathcal{J}$.

Bsp. 19.6: In $\mathbb{Q}[X,Y,Z]$ ist

$$\begin{aligned} \langle XZ, YZ \rangle : \langle Z \rangle &= \{ f \in \mathbb{Q}[X,Y,Z] \mid fZ \in \langle XZ, YZ \rangle \} \\ &= \{ f \in \mathbb{Q}[X,Y,Z] \mid \exists A, B \in \mathbb{Q}[X,Y,Z] : fZ = AXZ + BYZ \} \\ &= \{ f \in \mathbb{Q}[X,Y,Z] \mid \exists A, B \in \mathbb{Q}[X,Y,Z] : f = AX + BY \} \\ &= \langle X, Y \rangle. \end{aligned}$$

Bem. 19.7: K Körper, $\mathcal{I}, \mathcal{J} \subset K[X_1, \dots, X_n]$ Ideale. Dann gilt:

(a) $\mathcal{I} : \mathcal{J}$ ist ein Ideal in $K[X_1, \dots, X_n]$

(b) $\mathcal{I} : \mathcal{J} \supset \mathcal{I}$.

Bew.: (b) Sei $f \in \mathcal{I} \Rightarrow fg \in \mathcal{I}$ für alle $g \in K[X_1, \dots, X_n] \supset \mathcal{J} \Rightarrow f \in \mathcal{I} : \mathcal{J}$

(a) ① $0 \in \mathcal{I} : \mathcal{J}$ wg. $0g = 0 \in \mathcal{I}$ für alle $g \in \mathcal{J}$

② Seien $f_1, f_2 \in \mathcal{I} : \mathcal{J} \Rightarrow f_1 g, f_2 g \in \mathcal{I}$ für alle $g \in \mathcal{J}$

$\Rightarrow (f_1 + f_2) g \in \mathcal{I}$ für alle $g \in \mathcal{J} \Rightarrow f_1 + f_2 \in \mathcal{I} : \mathcal{J}$.

③ Sei $f \in J:J$, $h \in K[X_1,\dots,X_n] \Rightarrow fg \in J$ für alle $g \in J$

$\Rightarrow hfg \in J$ für alle $g \in J \Rightarrow hf \in J:J$. □

Satz 19.8: K Körper, $J, J \subset K[X_1,\dots,X_n]$ Ideale. Dann gilt:

(a) $V(J:J) \supset \overline{V(J) \setminus V(J)}$

(b) Falls K alg. abg. ist und J ein Radikalideal ist, dann ist

$$V(J:J) = \overline{V(J) \setminus V(J)}$$

Bew.: (a) Beh.: $J:J \subset J(V(J) \setminus V(J))$

Bew.: Sei $f \in J:J$, $x \in V(J) \setminus V(J)$

$\Rightarrow fg \in J$ für alle $g \in J$

$\overset{x \in V(J)}{\Rightarrow} f(x)g(x) = 0$ für alle $g \in J$

Wegen $x \notin V(J)$ ex. ein $g \in J$ mit $g(x) \neq 0$

$\Rightarrow f(x) = 0$ für alle $x \in V(J) \setminus V(J)$

$\rightarrow f \in J(V(J) \setminus V(J)) \rightarrow$ Beh.

Aus 17.9 folgt $V(J:J) \supset V(J(V(J) \setminus V(J)) = \overline{V(J) \setminus V(J)}$

(b) Sei K alg. abg., $J = \sqrt{J}$.

Sei $x \in V(J:J)$, $h \in J(V(J) \setminus V(J))$.

Sei $g \in J$. Dann ist $(hg)(a) = 0$ für alle $a \in V(J)$, denn:

$h(a) = 0$, falls $a \in V(J) \setminus V(J)$, $g(a) = 0$, falls $a \in V(J)$.

$\overset{\text{Hilb. NS-Satz}}{\Rightarrow} hg \in \sqrt{J} = J$

Damit $hg \in J$ für alle $g \in J$

$\Rightarrow h \in J:J$

$\overset{x \in V(J:J)}{\Rightarrow} h(x) = 0$

$\Rightarrow x \in V(J(V(J) \setminus V(J))$

$\Rightarrow V(J:J) \subset V(J(V(J) \setminus V(J))) = \overline{V(J) \setminus V(J)}$. □

Folgerung 19.10: K Körper, V, W Varietäten in K^n. Dann gilt:

$$J(V) : J(W) = J(V \setminus W)$$

Bew.: Setze $J := J(V)$, $J := J(W)$.

„$\subset$" Im Bew. von Satz 19.8 wurde gezeigt: $J : J \subset J(V(J) \setminus V(J)) = J(V(J(V) \setminus V(J(W)) \overset{17.9}{=} J(V \setminus W)$.

„$\supset$" Sei $f \in J(V \setminus W)$, $g \in J(W)$.

Dann ist für $a \in V$:

$(fg)(a) = f(a)\, g(a) = 0$

$\Rightarrow fg \in J(V)$

Damit $f \in J(V) : J(W)$. □

Bem. 19.10: K Körper, $J, J_1, \dots, J_r$ Ideale in $K[X_1, \dots, X_n]$. Dann gilt:

$$J : (J_1 + \dots + J_r) = (J : J_1) \cap \dots \cap (J : J_r)$$

Bew.: Nachrechnen / Übungsaufgabe

Bem. 19.11: K Körper, $J \subset K[X_1, \dots, X_n]$, $g \in K[X_1, \dots, X_n]$, $J \cap \langle g \rangle = \langle h_1, \dots, h_s \rangle$.

Dann gilt: $J : \langle g \rangle = \left\langle \frac{h_1}{g}, \dots, \frac{h_s}{g} \right\rangle$.

Bew.: „$\supset$" Sei $f \in \left\langle \frac{h_1}{g}, \dots, \frac{h_s}{g} \right\rangle$, $d \in \langle g \rangle$

$\Rightarrow d = bg$ für ein $b \in K[X_1, \dots, X_n]$

$\Rightarrow df = bgf \in \langle h_1, \dots, h_s \rangle = J \cap \langle g \rangle \subset J$

$\Rightarrow f \in J : \langle g \rangle$

„$\subset$" Sei $f \in J : \langle g \rangle \Rightarrow fg \in J$, $wg.\ fg \in \langle g \rangle$ folgt $fg \in J \cap \langle g \rangle = \langle h_1, \dots, h_s \rangle$

$\Rightarrow fg = \sum_{i=1}^{s} r_i h_i$ für geeignete $r_1, \dots, r_s \in K[X_1, \dots, X_n]$

$\Rightarrow f = \sum_{i=1}^{s} r_i \frac{h_i}{g}$ (die $\frac{h_i}{g}$ sind wohldef. wg. $h_i \in \langle g \rangle$)

$\Rightarrow f \in \left\langle \frac{h_1}{g}, \dots, \frac{h_s}{g} \right\rangle$. □

Anm: 19.11 und 19.10 liefern einen Algorithmus zur Berechnung von Idealquotienten.