

L

I

ALGEBRA A^4 :

Algebraische Strukturen

Algebraische Mengen

Algorithmen

Anwendungen

Literaturquellen:

- Cox, Little, O'Shea: Ideals, Varieties and Algorithms
(Lehrbuch, Vorlage für diesen Kurs)
- Shafarevich: Basic Notions of Algebra
- Lang: Algebra (klassische Weise, 900 Seiten lang)

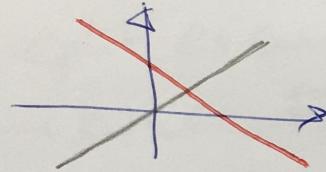
Einführung:

Nichtlineare Fortsetzung der Linearen Algebra

Lineare Algebra & Geometrie

Lineare Gleichungssysteme (LGS)

Mengen, die dadurch definiert sind



Lineare Abbildungen und lineare Funktionen

Algorithmen

(Gaußverfahren, Gram-Schmidt usw.)

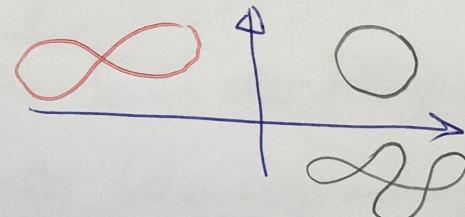
Zahlreiche Anwendungen

(2)

(Nichtlineare) Algebra & Geometrie

Polynomiale Gleichungssysteme (PGS)

Mengen, die dadurch definiert sind



Polynomiale Abbildungen und Polynome

Algorithmen

(Gröbnerbasen usw.)

Zahlreiche Anwendungen

Lineare sowie Nichtlineare Algebra kann über einem ~~reellen~~
beliebigen Körper k entwickelt werden (für manche
Aussagen werden extra Voraussetzungen an k benötigt).

Interessante Spezialfälle: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, F_p := \mathbb{Z}/p\mathbb{Z}$
für eine Primzahl p .

Bei uns geht es um die Kommutative Algebra: Algebra der
kommutativen Ringe. Wir machen den Fall der Polynomringen.

Algebraische Geometrie: die Theorie der Lösungsmengen von PGs.

Highlights:

- Hilbertscher Basisatz
- Algorithmen auf der Basis von Gröbnerbasen
- Hilbertscher Nullstellensatz.

Was für Anwendungen von Algebra gibt es?

[4]

- Robotik.

$$\left. \begin{array}{l} (x,y) \\ (0,0) \\ (x',y') \end{array} \right| \quad \left. \begin{array}{l} x^2+y^2=1 \\ (x'-x)^2+(y'-y)^2=1 \end{array} \right.$$

- Codierungstheorie

- Kryptographie

- Physik : Kristallographie
Quantenphysik
String Theory

- ~~Alte~~ Statistik

- Biologie (Phylogenetische Bäume)

- Anwendungen innerhalb von Mathematik
(Zahlentheorie, Differentialgeometrie etc.)

1. Geometrie, Algebra und Algorithmen.

5

Im Folgenden sei k Körper.

Wir führen Polynome, Ideale, und Varietäten ein und geben Beispiele.

1.1. Polynome und der affine Raum.

Algebra der Polynomringe basiert auf formalen Variablen x_1, \dots, x_n ($n \in \mathbb{Z}_{>0}$), die man auch Unbestimmte oder Symbole nennt.

1.1.1. Def. Der Ausdruck $x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ mit $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_{\geq 0}$, nennt man ein Monom und der Wert $\alpha_1 + \dots + \alpha_n$ ist der (totale) Grad dieses Monoms.

Für Monome benutzen wir die Abkürzung

$$x^\alpha := x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} \text{ mit}$$

$$x = (x_1, \dots, x_n) \text{ und } \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n.$$

Der Vektor $\alpha \in \mathbb{Z}_{\geq 0}^n$ wird Multindex genannt.

(6)

Man sagt auch: α ist der Exponentenvektor von x^α .

für den totalen Grad von x^α benutzt man die Bezeichnung

$$|\alpha| := \alpha_1 + \dots + \alpha_n.$$

1.1.2 Def. Ein Polynom im Variablen x_1, \dots, x_n mit Koeffizienten in k ist ein formaler Ausdruck der Form

$$f = \sum_{\alpha} c_\alpha x^\alpha \quad (1)$$

mit $\alpha \in \mathbb{Z}_{\geq 0}^n$ und $c_\alpha \in k$, in dem $c_\alpha \neq 0$ nur für endlich viele α 's gilt. Die Menge aller solchen Polynome wird als $k[x_1, \dots, x_n]$ bezeichnet.

In (1) heißt c_α der Koeffizient von x^α .

Der Ausdruck $c_\alpha x^\alpha$ mit $c_\alpha \neq 0$ heißt Term von f vom totalen Grad $|\alpha|$.

Der Grad $\deg(f)$ von f ist der maximale Grad eines Terms in f . Wenn $f = 0$ ist (d.h. alle $c_\alpha = 0$), dann setzt man $\deg(f) = -\infty$. [7]

Ein Polynom ist durch die Anzahl der Koeffizienten definiert und Gleichheit von Polynomen wird durch Koeffizientenvergleich definiert.

k ist Teilmenge von $k[x_1, \dots, x_n]$, weil jedes $t \in k$ als Polynom f mit $(c_{0, \dots, 0}) = t$ und $c_\alpha = 0$ für $\alpha \neq (0, \dots, 0)$ interpretiert wird.

Die einzelnen Variablen ~~sind~~ x_1, \dots, x_n sind ebenfalls Elemente von $k[x_1, \dots, x_n]$. In $k(x_1, \dots, x_n)$ hat man Addition und Multiplikation:

Für $f = \sum_{\alpha} c_\alpha x^\alpha$ und $g = \sum_{\alpha} d_\alpha x^\alpha$

$$\text{setzt man } f+g := \sum_{\alpha} (c_\alpha + d_\alpha) x^\alpha \quad \text{und } fg := \sum_{\alpha, \beta} c_\alpha d_\beta x^{\alpha+\beta}$$

1.1.3. Bew.
d.h.

$k[x_1, \dots, x_n]$ ist ein kommutativer Ring mit 1

[8]

$$f + g = g + f$$

$$f \cdot g = g \cdot f$$

$$f + 0 = f$$

$$f + (-f) = 0$$

$$f \cdot 1 = f$$

$$f \cdot (g+h) = f \cdot g + f \cdot h$$

Gilt für alle $f, g, h \in k[x_1, \dots, x_n]$ ($-f := (-1) \cdot f$)

Für $n \in \{1, 2, 3\}$ benutzt man standardmäßig die folgenden Namen
für Variablen

n	Variablen	Ring
1	x	$k[x]$
2	x, y	$k[x, y]$
3	x, y, z	$k[x, y, z]$

1.1.4 Def.

$k^n := \{(a_1, \dots, a_n) \in k \mid a_1, \dots, a_n \in k\}$ nennen wir den n -dimensionale affine Raum.

k^1 nennt man die affine Gerade

k^2 nennt man die affine Ebene

Aus der linearen Algebra kennen wir: k^n ist ein n -dim. Vektorraum über k .

1.1.5 Def. Ein Polynom $f = \sum_{\alpha} c_{\alpha} x^{\alpha}$ kann man auf k^n auswerten, indem man für Variable x_1, \dots, x_n Werte aus k einsetzt. Auf diese Weise erzeugt f die sogenannte polynomielle Funktion

$$(a_1, \dots, a_n) \in k^n \mapsto \sum_{\alpha=(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n} c_{\alpha} a_1^{\alpha_1} \cdots a_n^{\alpha_n}$$

Man bezeichnet diese Abbildung

als $f: k^n \rightarrow k$ (ist eine Vernebelung der Bezeichnungen).

Wichtig: Im Allgemeinen sind Polynome und polynomiale Funktionen nicht das Gleiche
(Polynome sind Ausdrücke) [10]

Bsp. $\mathbb{F}_2 = \{0, 1\}$ $1+1=0$

$$f = x^2 + x \in \mathbb{F}_2[x].$$

Was ist die Abbildung $f: \mathbb{F}_2 \rightarrow \mathbb{F}_2$

$$f(0) = 0^2 + 0 = 0$$

$$f(1) = 1^2 + 1 = 1 + 1 = 0 \in \mathbb{F}_2 \quad] \text{ Nullabbildung}$$

f ist aber kein Nullpolynom.

Für unendliche Körper k hat man aber eine Bijektion

$$f \in k[x_1, \dots, x_n] \iff f: k^n \rightarrow k$$

1.1.6 Prop. Sei k unendlicher Körper und $f \in k[x_1, \dots, x_n]$.
Dann gilt die folgende Äquivalenz:

f ist Nullpolynom $\Leftrightarrow f: k^n \rightarrow k$ ist eine Nullfunktion

Beweis: " \Rightarrow " ist klar.

" \Leftarrow ". Sei $f: k^n \rightarrow k$ Nullfunktion. Wir zeigen, dass $f \in k[x_1, \dots, x_n]$ ein Nullpolynom ist (d.h. alle Koeffizienten von f sind 0). Im Fall $n=1$ ist das bekannt

(vgl. Lineare Algebra 1, wir reden aber später darüber).

Wir benutzen Induktion. Sei $n \geq 2$ und sei die Aussage

für $k[x_1, \dots, x_{n-1}]$ bereits bewiesen. Wir können f als

$$f = \sum_{i=0}^N g_i(x_1, \dots, x_{n-1}) x_n^i$$

mit $N \in \mathbb{Z}_{>0}$, und $g_0, \dots, g_N \in k[x_1, \dots, x_{n-1}]$ darstellen.

für alle $(a_1, \dots, a_{n-1}) \in k^{n-1}$ ist $f(a_1, \dots, a_{n-1}, x_n) = \sum_{i=0}^N g_i(a_1, \dots, a_{n-1}) x_n^i$

~~ein~~ ein Polynom aus $k[x_n]$, das eine Nullfunktion definiert.

$\Rightarrow g_i(a_1, \dots, a_{n-1}) = 0$ für alle $i = 1, \dots, N$

und alle $a_1, \dots, a_{n-1} \in k$.

Wir benötigen die Induktionsvoraussetzung für die Polynome

g_1, \dots, g_N und erhalten, dass das Nullpolynom sind

$$\Rightarrow f = \sum_{i=1}^N g_i x_n^i \quad \text{ist ebenfalls ein Nullpolynom.}$$

□

1.1.7. Kor. Sei k ein endlicher Körper und seien $f, g \in k[x_1, \dots, x_n]$.

Dann gilt: f und g sind gleich \Leftrightarrow

die polynomielles Funktionen $f, g: k^n \rightarrow k$ sind
gleiches funktionen.

Beweis: Man betrachtet $f - g$ und benutzt dann Prop. 1.1.6. □

1.1.8 Def. Man nennt einen Körper k algebraisch abgeschlossen,

wenn jedes Polynom aus $k[x]$ von Grad
mindestens 1 eine Nullstelle in k hat.

Ken endlicher Körper ist algebraisch abgeschlossen

(Warum?). Die Körper \mathbb{Q} und \mathbb{R} sind nicht algebraisch abgeschlossen, weil $x^2+1 \in \mathbb{Q}[x] \subseteq \mathbb{R}[x]$ weder in \mathbb{Q} noch in \mathbb{R} Nullstellen hat.

1.1.9 Thm (Fundamentalsatz der Algebra) \mathbb{C} ist algebraisch abgeschlossen. D.h., jedes Polynom aus $\mathbb{C}[x]$ vom Grad mindestens 1 hat eine Nullstelle in \mathbb{C} .
Beweis: es gibt einen Beweis auf der Basis der Analysis (finden Sie diesen Beweis). □

1.2. Affine Varietäten.

1.2.1 Def. Für endliche viele Polynome $f_1, f_s \in k[x_1, \dots, x_n]$ nennt man die Menge

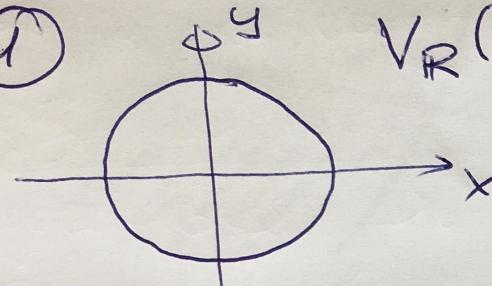
$$V(f_1, \dots, f_s) = \{ (a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \text{ für alle } i = 1, \dots, s \}$$

eine affine algebraische Menge oder eine affine Varietät, die durch f_1, \dots, f_s definiert ist.

Wenn man den Körper explizit angeben möchte, schreibt (14)
 man auch $V_k(f_1, f_5)$.

1.2.2 Bsp.

①

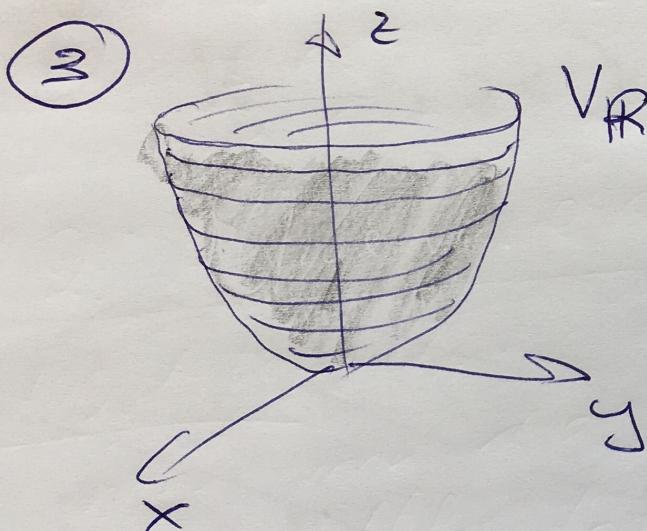


$$V_{\mathbb{R}}(x^2 + y^2 - 1)$$

②

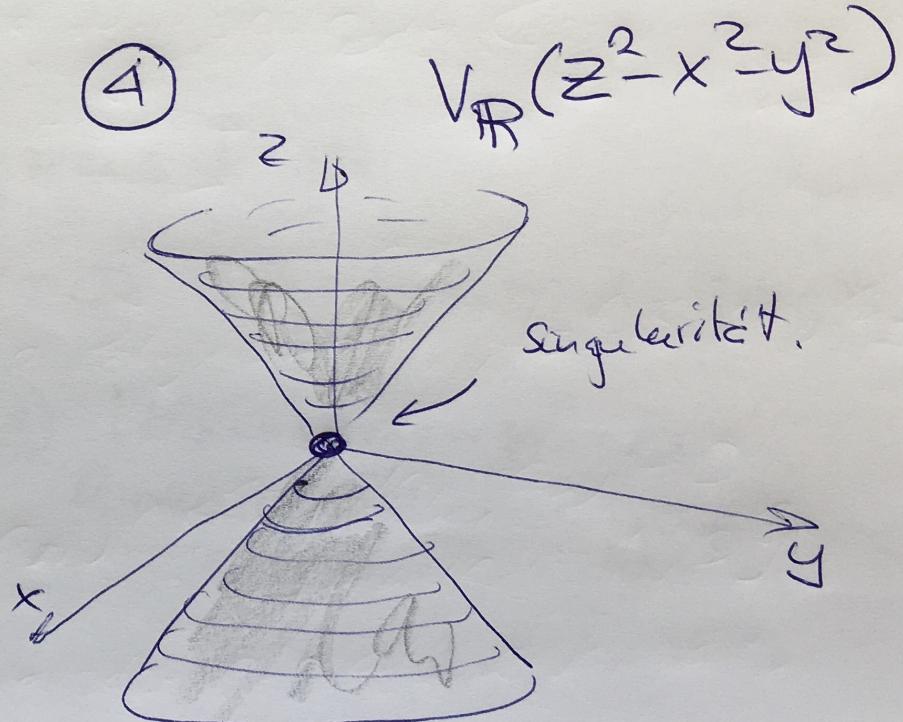
Graphen von polynomellen
 Funktionen sind
 affine Varietäten.

③



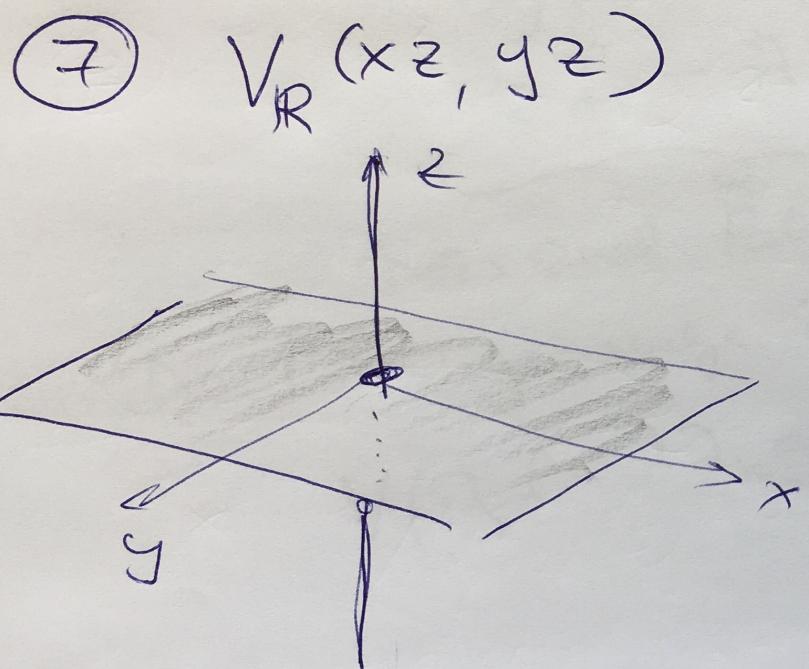
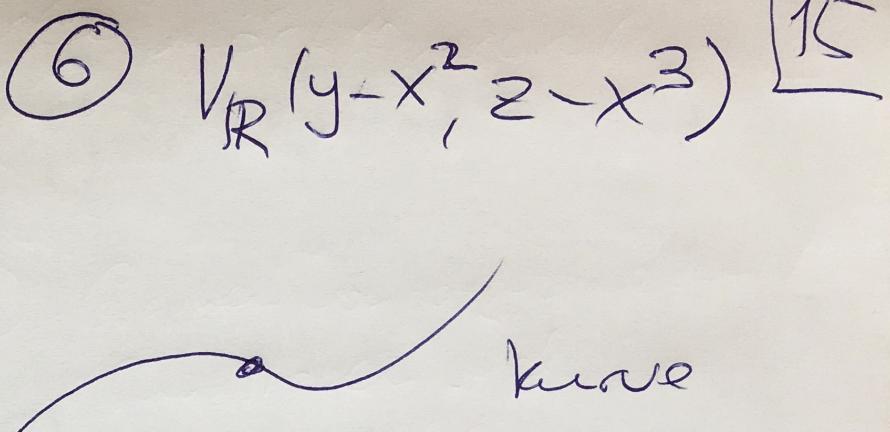
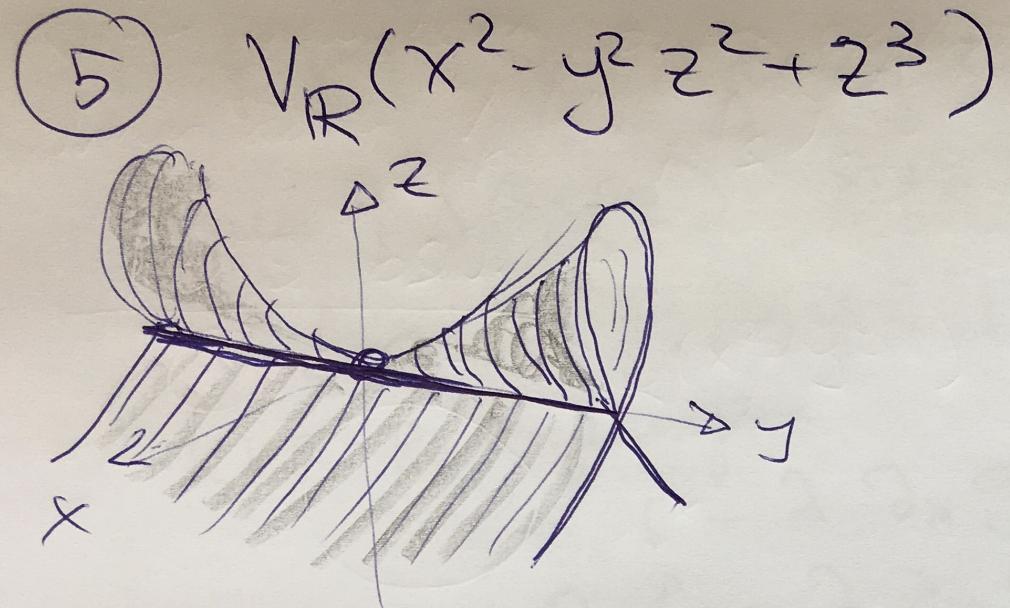
$$V_{\mathbb{R}}(z - x^2 - y^2)$$

④



singularität.

(14)



$xz = yz = 0$ heißt
 $z=0$ oder sonst $x=y=0$

8) Lösungsmenge der
 linearen Gleichungen gegeben

L 16

⑨ KKT-Bedingungen.

$\min \{ f(x,y,z) : x, y, z \in \mathbb{R}, g(x,y,z) = 0^3 \}$

mit $f, g \in \mathbb{R}[x,y,z]$.

KKT Bedingungen

$$\partial_x f - \lambda \partial_x g = 0$$

$$\partial_y f - \lambda \partial_y g = 0$$

$$\partial_z f - \lambda \partial_z g = 0$$

$\underbrace{\quad}_{\text{dies sind Polynome in } \mathbb{R}[x,y,z,\lambda]}$

dies sind Polynome in $\mathbb{R}[x,y,z,\lambda]$

Die Lösungsmenge ist die Varietät

$$V(\partial_x f - \lambda \partial_x g, \partial_y f - \lambda \partial_y g, \partial_z f - \lambda \partial_z g) \subseteq \mathbb{R}^4.$$

⑩

$V_R(x^2+y^2+1)$ ist leere Menge aber

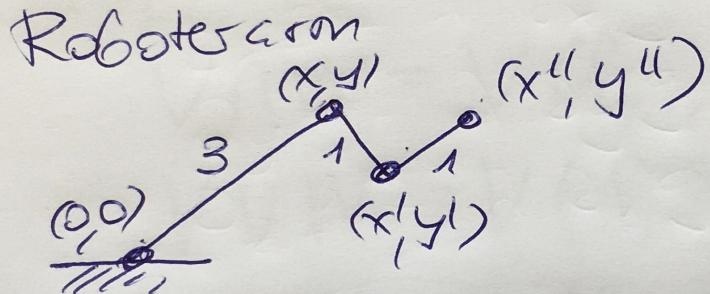
| 17

$V_C(x^2+y^2+1) \neq \emptyset$

⑪

$V(\cancel{x}y, xy-1) = \emptyset$ unabhängig von k

⑫



$$V_R(x^2+y^2-3^2, (x-x')^2+(y-y')^2-1, (x-x'')^2+(y-y'')^2-1) \\ \in \mathbb{R}(x, y, \cancel{x}, x', y', \cancel{x}, x'', y'')$$

$\in \mathbb{R}^6$

1.2.3 Lem. Seien $V, W \subseteq k^n$ affine Varietäten. Dann sind $V \cup W$ und $V \cap W$ ebenfalls affine Varietäten.

[18]

Beweis: Sei $V = V(\underbrace{f_1, \dots, f_s}_{\in k[x_1, \dots, x_n]})$ und $W = V(\underbrace{g_1, \dots, g_t}_{\in k[x_1, \dots, x_n]})$

Wir zeigen:

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

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

(*) ist klar. Wir zeigen (**).

Sei $a = (a_1, \dots, a_n) \in k^n$. Ist $a \in V \cup W$, so gilt $f_1(a) = \dots = f_s(a) = 0$ oder $g_1(a) = \dots = g_t(a) = 0$.

In den beiden Fällen hat man $f_i(a) \cdot g_j(a) = 0$

für alle i, j , da einer der beiden Faktoren ist stets gleich 0. Ist $a \notin V \cup W$, so gilt

\Rightarrow Man findet ein $i' = 1, \dots, s$ mit $f_{i'}(a) \neq 0$

[19]

und ein $j' = 1, \dots, t$ mit $g_{j'}(a) \neq 0$

$\Rightarrow f_{i'}(a) \cdot g_{j'}(a) \neq 0$

$\Rightarrow a \notin V(f_i g_j : i=1, \dots, s, j=1, \dots, t)$. \square

Nach diesem Beweis kann man

$$V(zx, zy) = V(z) \cup V(xy) \text{ schreiben.}$$

3 algorithmische Fragen zum System $f_1 = \dots = f_s = 0$

für $f_1, \dots, f_s \in k[x_1, \dots, x_n]$.

Konsistenz: Ist $V(f_1, \dots, f_s) \neq \emptyset$?

Eindeutigkeit: Ist $V(f_1, \dots, f_s)$ eine endliche Menge?

Dimension: Was ist die Dimension von $V(f_1, \dots, f_s)$?

(Die Dimensionen müssen wir noch erläutern).

Im Fall von linearen Gleichungssystemen haben wir

zur Lösung dazu (Gauß-Verfahren).

1.2.4 Aufgaben.

(20)

- ① Zeigen Sie, dass kein endlicher Körper alg. abgeschlossen ist.
- ② Finden Sie einen Beweis des Fundamentalsatzes von Algebra (Googeln oder so).
- ③ Man zeige, dass jede endliche Teilmenge k^n eine affine Varietät ist.
Sind $\mathbb{R} \setminus \{(0)\}$, $\mathbb{R}^2 \setminus \{(0,0)\}$, $\mathbb{R} \times \mathbb{R} > 0$,
 $\mathbb{R} \times \mathbb{R} \geq 0$ affine Varietäten bzgl. $k = \mathbb{R}$.
- ④ Man zeige: Durchschnitt und Vereinigung endlich vieler aff. Varietäten sind affine Varietäten
- ⑤ Seien $V, W \subseteq k^n$ affine Varietäten.
Man zeige, dass $V \times W$ affine Varietät ist.

1.3. Parametrisierung offener Varietäten.

(2)

Bsp. $\begin{cases} x + y + z = 1 \\ x + 2y - z = 3 \end{cases}$ definiert offen
Untermannigf. $U \subseteq \mathbb{K}^3$

Wie kann man U parametrisch darstellen?

$$\begin{cases} x + y + z = 1 & (\text{I}) \\ x + 2y - z = 3 & (\text{II}) \end{cases} \quad (\text{II}) := (\text{II}) - (\text{I})$$

$$\begin{cases} x + y + z = 1 & (\text{I}) \\ y - 2z = 0 & (\text{II}) \end{cases} \quad (\text{I}) := (\text{I}) - (\text{II})$$

$$\begin{cases} x + 3z = 1 \\ y - 2z = 0 \end{cases}$$

$$U = \{ (1-3t, 2t, t) : t \in \mathbb{K} \}$$

Bsp. Wie kann man den Kreis $x^2 + y^2 = 1$ rational parametrisieren?

22

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

Übung:

$$(1-t^2)^2 + (2t)^2 = 1 - 2t^2 + t^4 + 4t^2 \\ = 1 + 2t^2 + t^4 = (1+t^2)^2$$

Zum Punkt $x=-1, y=0$ findet man aber
kein passendes t .

$$V_{\mathbb{R}}(x^2+y^2-1) \neq \{(-1,0)\} = \left\{ \left(\frac{1+t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{R} \right\}$$

1.B.1 Def Formale Quotienten von Polynomen nennt man rationale Funktionen. (Wort Funktion ist eigentlich eine Fehlbezeichnung). Generell: wir definieren die Menge aller rationalen Funktionen in x_1, \dots, x_n mit Koeffizienten in k als die Menge der formalen Quotienten f/g mit $f \in k[x_1, \dots, x_n], g \in k[x_1, \dots, x_n] \setminus \{0\}$.

Wir bezeichnen diese Menge als $k(x_1, \dots, x_n)$. (23)

Die Gleichheit $\frac{f}{g} = \frac{u}{v}$ wird durch

$f \cdot v = u \cdot g$ definiert. Den Polynomring interpretiert man als Teilmenge von $k(x_1, \dots, x_n)$, denn $f \in k[x_1, \dots, x_n]$ entspricht dem Quotienten $\frac{f}{1} \in k(x_1, \dots, x_n)$.

Des Weiteren werden $+ \text{ und } \cdot$ in $k(x_1, \dots, x_n)$ folgendermaßen eingeführt:

$$\frac{f}{g} + \frac{u}{v} := \frac{f \cdot v + g \cdot u \cdot g}{g \cdot v}$$

$$\frac{f}{g} \cdot \frac{u}{v} := \frac{f \cdot u}{g \cdot v}$$

Es ist wohldefiniert, dann aus $g, v \in k[x_1, \dots, x_n] \setminus \{0\}$ folgt $g \cdot v \in k[x_1, \dots, x_n] \setminus \{0\}$. (Warum?)