Algebraische Geometrie

Algebraische Varietäten und Hilberts Nullstellensatz

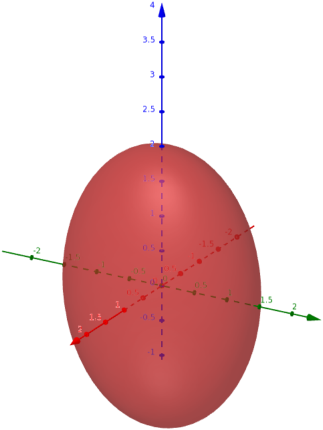
8. Dezember 2020

Inhalt

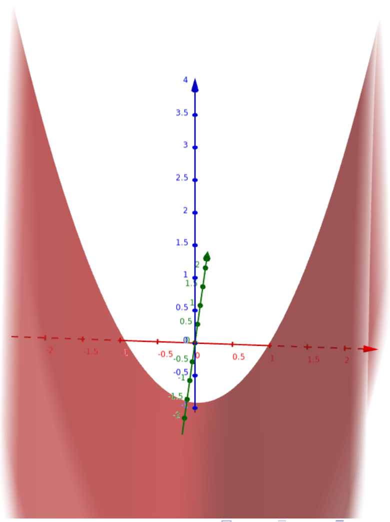
Was ist algebraische Geometrie?

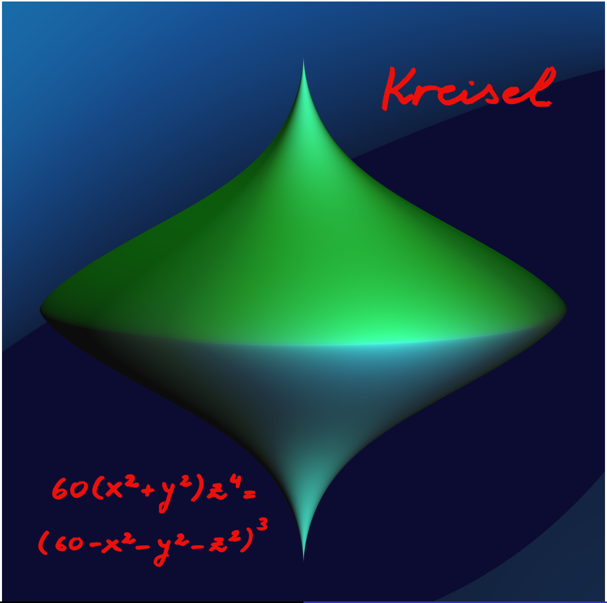
- Untersuchen von Nullstellenmengen von multivariaten Polynomen
  - Einerseits: Geometrische Figuren
  - Andererseits: Algebraische Objekte
- Fermats letzter Satz: Hat $x^n + y^n = z^n, n \geq 3$, eine Lösung in $\mathbb{Q} \setminus \{0\}$?

$$4x^2 + 2y^2 + z^2 = 4$$



$$x^2 = y^2 + z$$




Kreisel
$60(x^2+y^2)z^4=$
$(60-x^2-y^2-z^2)^3$

Was ist algebraische Geometrie?

- Untersuchen von Nullstellenmengen von multivariaten Polynomen
  - Einerseits: Geometrische Figuren
  - Andererseits: Algebraische Objekte
- Fermats letzter Satz: Hat $x^n + y^n = z^n, n \geq 3$, eine Lösung in $\mathbb{Q} \setminus \{ 0 \}$?

Inhalt

Quotientenringe

Definition

Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. $M/\sim$ ist die Menge der Äquivalenzklassen.

- Gegeben:
  - Ring (kommutativ und mit 1) R
  - Äquivalenzrelation $\sim$ auf R
- Frage: Ist $R/\sim$ mit $[a]+[b] := [a+b], [a][b] := [ab]$ wieder ein Ring?

Ideale

Eine Antwort

$$a \sim b, c \sim d \implies a + c \sim b + d, ac \sim bd$$

Oder mit $I := [0] = \{ a \in R \mid a \sim 0 \}$:

$$a, b \in I, r \in R \implies a - b \in I, ra \in I$$

Ideale

Eine Antwort

$$a \sim b, c \sim d \implies a + c \sim b + d, ac \sim bd$$

Oder mit $I := [0] = \{ a \in R \mid a \sim 0 \}$:

$$a, b \in I, r \in R \implies a - b \in I, ra \in I$$

Definition

$I \subseteq R$ heißt Ideal, wenn es eine Untergruppe bezüglich $+$ ist und für $r \in R, a \in I$ auch $ra \in I$.

Erzeuger von Idealen

Definition

Seien $r_1, \ldots, r_n$ in R. $(r_1, \ldots, r_n) = \{ \sum_{i=1}^n a_i r_i \mid a_i \in R \}$ ist das von $r_1, \ldots, r_n$ erzeugte Ideal.

Beispiel

In den Ringen $\mathbb{Z}$ und $K[x]$ ist jedes Ideal von einem Element erzeugt.

Satz (Hilberts Basissatz)

In $K[x_1, \ldots, x_n]$ ist jedes Ideal von endlich vielen Elementen erzeugt.

Eine nützliche Aussage

Lemma

Für $a \in R$ ist $(a) = R$ genau dann, wenn a in R invertierbar ist.

Eine nützliche Aussage

Lemma

Für $a \in R$ ist $(a) = R$ genau dann, wenn a in R invertierbar ist.

- Wenn $(a) = R \ni 1$ gibt es ein $b \in R$ mit $ab = 1$

Eine nützliche Aussage

Lemma

Für $a \in R$ ist $(a) = R$ genau dann, wenn a in R invertierbar ist.

- Wenn $(a) = R \ni 1$ gibt es ein $b \in R$ mit $ab = 1$
- Wenn a invertierbar ist, gilt für jedes $r \in R$ auch $r = a(a^{-1}r) \in (a)$

Eine nützliche Aussage

Lemma

Für $a \in R$ ist $(a) = R$ genau dann, wenn a in R invertierbar ist.

- Wenn $(a) = R \ni 1$ gibt es ein $b \in R$ mit $ab = 1$
- Wenn a invertierbar ist, gilt für jedes $r \in R$ auch $r = a(a^{-1}r) \in (a)$

Für Polynomringe

$f \in K[x_1, ..., x_n]$ ist invertierbar genau dann, wenn f eine von 0 verschiedene Konstante ist

Maximale Ideale

Definition

Ein Ideal $I \subsetneq R$ heißt maximal, wenn es kein Ideal J mit $I \subsetneq J \subsetneq R$ gibt.

Maximale Ideale

Definition

Ein Ideal $I \subsetneq R$ heißt maximal, wenn es kein Ideal J mit $I \subsetneq J \subsetneq R$ gibt.

Satz

I ist maximal genau dann, wenn R/I ein Körper ist.

Maximale Ideale

Definition

Ein Ideal $I \subsetneq R$ heißt maximal, wenn es kein Ideal J mit $I \subsetneq J \subsetneq R$ gibt.

Satz

I ist maximal genau dann, wenn R/I ein Körper ist.

Beispiel

In $\mathbb{Z}$ ist das Ideal (n) maximal genau dann, wenn n prim ist.

Körpererweiterungen

Definition

Seien L ein Körper und K ein Unterkörper. Man nennt L/K Körpererweiterung.

Eine wichtige Perspektive

Wir können L als K-Vektorraum betrachten, wobei die Skalarmultiplikation die Multiplikation des Körpers ist. Insbesondere existiert eine Basis.

Adjunktion

Definition

Seien L/K eine Körpererweiterung und $\alpha_1, ..., \alpha_n \in L$. Wir definieren

$$K[\alpha_1, ..., \alpha_n] := \{\, f(\alpha_1, ..., \alpha_n) \mid f \in K[x_1, ..., x_n] \,\}.$$

Beispiel

$\mathbb{Q}[i]$ ist der Körper der komplexen Zahlen mit rationalen Real- und Imaginärteilen.

Körpererweiterungen: Eine Einordnung

Definition

Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt algebraisch, wenn es ein $f \in K[x] \setminus \{0\}$ mit $f(\alpha) = 0$ gibt.

Beispiel

$\sqrt{2}$ ist algebraisch bezüglich $\mathbb{R}/\mathbb{Q}$ (als Nullstelle von $x^2 - 2$), π allerdings nicht.

Körpererweiterungen: Eine Einordnung

Definition

Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt algebraisch, wenn es ein $f \in K[x] \setminus \{ 0 \}$ mit $f(\alpha) = 0$ gibt.

Beispiel

$\sqrt{2}$ ist algebraisch bezüglich $\mathbb{R}/\mathbb{Q}$ (als Nullstelle von $x^2 - 2$), π allerdings nicht.

Satz

Wenn $\alpha_1, \ldots, \alpha_n$ algebraisch sind, ist $K[\alpha_1, \ldots, \alpha_n]$ wieder ein Körper.

Inhalt

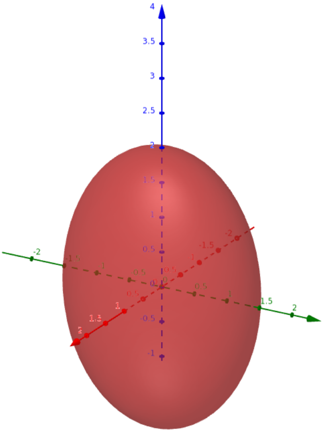
Der affine Raum und Varietäten

Definition

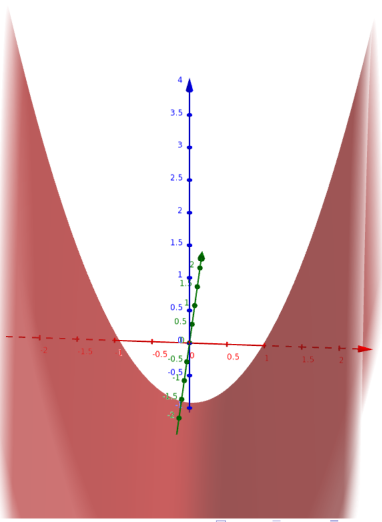
Unser zugrundeliegender Raum wird $\mathbb{A}_k^n := k^n$. Für $T \subseteq k[x_1, \ldots, x_n]$ definieren wir die von T erzeugte Varietät

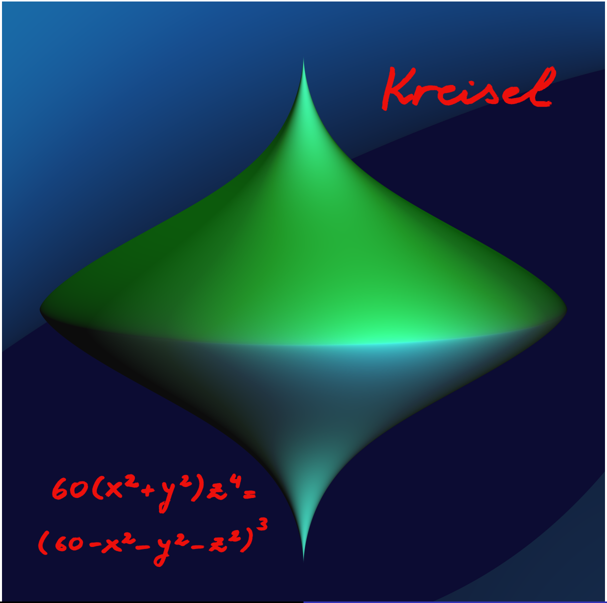
$$V(T) := \{ P \in \mathbb{A}_k^n \mid \forall f \in T : f(P) = 0 \} .$$

$$4x^2 + 2y^2 + z^2 = 4$$

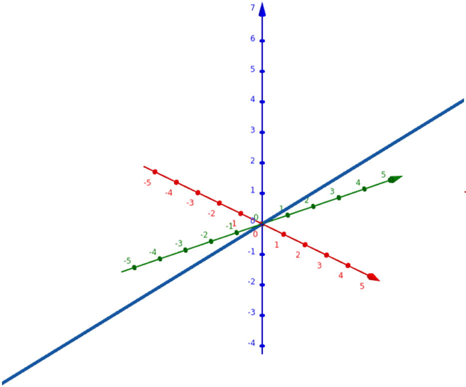


$$x^2 = y^2 + z$$

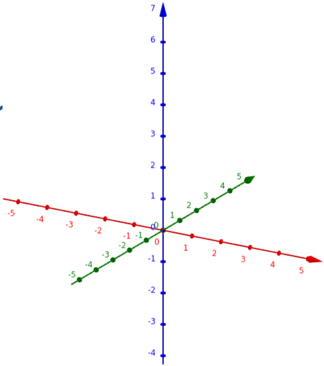



Kreisel
$60(x^2+y^2)z^4=$
$(60-x^2-y^2-z^2)^3$

$$x = y = z$$



$$x^2 + 1 = 0$$



Varietäten und Ideale

Zur Erinnerung

$$V(T) := \{\, P \in \mathbb{A}_k^n \mid \forall f \in T : f(P) = 0 \,\}$$

Lemma

Sei $J = (T)$ das von T erzeugte Ideal. Dann ist $V(T) = V(J)$.

- $V(J) \subseteq V(T)$ folgt aus $T \subseteq J$
- $V(T) \subseteq V(J)$ gilt, da aus $f_i(x) = 0$ auch $\sum_{i=1}^n r_i f_i(x) = 0$ folgt

Varietäten und Ideale

Zur Erinnerung

$$V(T) := \{\, P \in \mathbb{A}_k^n \mid \forall f \in T : f(P) = 0 \,\}$$

Lemma

Sei $J = (T)$ das von T erzeugte Ideal. Dann ist $V(T) = V(J)$.

- $V(J) \subseteq V(T)$ folgt aus $T \subseteq J$
- $V(T) \subseteq V(J)$ gilt, da aus $f_i(x) = 0$ auch $\sum_{i=1}^n r_i f_i(x) = 0$ folgt

Folgerung

Eine Varietät wird bereits durch endlich viele Polynome beschrieben.

Zariski-Topologie

Satz

$$\mathbb{A}_k^n = V(\{0\}), \emptyset = V(k[x_1, \ldots, x_n])$$

$$V(I) \cup V(J) = V(I \cap J)$$

$$\bigcap_{i \in I} V(J_i) = V\left(\bigcup_{i \in I} J_i\right)$$

Zariski-Topologie

Satz

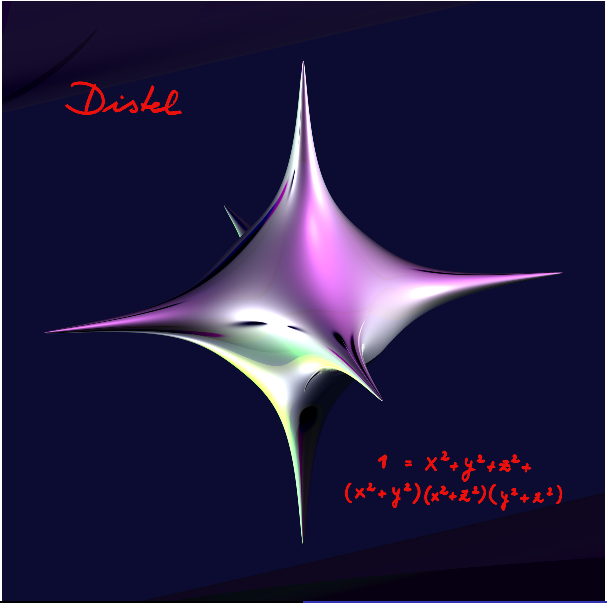
$$\mathbb{A}_k^n = V(\{0\}), \emptyset = V(k[x_1, \ldots, x_n])$$

$$V(I) \cup V(J) = V(I \cap J)$$

$$\bigcap_{i \in I} V(J_i) = V\left(\bigcup_{i \in I} J_i\right)$$

Für Interessierte

Wenn man die algebraischen Varietäten als abgeschlossene Mengen wählt, erhält man eine Topologie auf $\mathbb{A}_k^n$, die Zariski-Topologie.


Distel
$1 = x^2+y^2+z^2+$
$(x^2+y^2)(x^2+z^2)(y^2+z^2)$

Inhalt

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra, anders betrachtet)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra, anders betrachtet)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$V(\{\, f \,\}) \neq \emptyset.$$

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra, anders betrachtet)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$V((f)) \neq \emptyset.$$

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra, anders betrachtet)

Sei $f \in \mathbb{C}[x]$ mit $(f) \subsetneq \mathbb{C}[x]$. Dann gilt

$$V((f)) \neq \emptyset.$$

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra, anders betrachtet)

Sei $I \subsetneq \mathbb{C}[x]$ ein Ideal. Dann gilt

$$V(I) \neq \emptyset.$$

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Fundamentalsatz der Algebra, anders betrachtet)

Sei $I \subsetneq \mathbb{C}[x]$ ein Ideal. Dann gilt

$$V(I) \neq \emptyset.$$

Satz (Fundamentalsatz der Algebra)

Sei $f \in \mathbb{C}[x]$ nicht konstant. Dann gilt

$$f(a) = 0 \text{ für ein } a \in \mathbb{C}.$$

Satz (Hilberts Nullstellensatz)

Sei $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$ ein Ideal. Dann gilt

$$V(I) \neq \emptyset.$$

Lemma (Zariski)

Seien $K/\mathbb{C}$ eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in K$, sodass $\mathbb{C}[\alpha_1, \ldots, \alpha_n]$ ein Körper ist. Dann sind bereits $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.

Lemma (Zariski)

Seien $K/\mathbb{C}$ eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in K$, sodass $\mathbb{C}[\alpha_1, \ldots, \alpha_n]$ ein Körper ist. Dann sind bereits $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.

- $\mathbb{C}[\alpha_1, \ldots, \alpha_n]$ hat eine abzählbare Basis, da $\mathbb{C}[x_1, \ldots, x_n]$ eine hat (nämlich $\{ x_1^{i_1} \ldots x_n^{i_n} \mid i \in \mathbb{N}_0^n \}$)
- $\left\{ \frac{1}{\alpha_i - c} \,\middle|\, c \in \mathbb{C} \setminus \{ \alpha_i \} \right\}$ ist überabzählbar, also linear abhängig:

$$\sum_{j=1}^{n} \frac{b_j}{\alpha_i - c_j} = 0 \iff \sum_{j=1}^{n} b_j \prod_{k=1, k \neq j}^{n} \alpha_i - c_k = 0$$

- dieser Term hat als Polynom alle Nullstellen in $\mathbb{C}$

$\square$

Maximale Ideale im Polynomring

Da $k[x_1, ..., x_n]/(x_1 - \alpha_1, ..., x_n - \alpha_n) \cong k$ ein Körper ist, ist $(x_1 - \alpha_1, ..., x_n - \alpha_n)$ ein maximales Ideal.

Maximale Ideale im Polynomring

Da $k[x_1, \dots, x_n]/(x_1 - \alpha_1, \dots, x_n - \alpha_n) \cong k$ ein Körper ist, ist $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ ein maximales Ideal.

Satz

Für jedes maximale Ideal $m \subseteq \mathbb{C}[x_1, \dots, x_n]$ gibt es $\alpha_i \in \mathbb{C}$ mit

$$m = (x_1 - \alpha_1, \dots, x_n - \alpha_n).$$

- $\pi : \mathbb{C}[x_1, ..., x_n] \to \mathbb{C}[x_1, ..., x_n]/m, f \mapsto [f]$
- $\mathbb{C}[x_1, ..., x_n]/m$ ist ein Körper

- $\pi : \mathbb{C}[x_1, ..., x_n] \to \mathbb{C}[x_1, ..., x_n]/m, f \mapsto [f]$
- $\mathbb{C}[x_1, ..., x_n]/m$ ist ein Körper

$$\begin{aligned} & \mathbb{C}[x_1, ..., x_n]/m \cong \mathbb{C}[\pi(x_1), ..., \pi(x_n)] \\ \overset{Lemma}{\Longrightarrow} & \pi(x_1), ..., \pi(x_n) \in \mathbb{C} \\ \Longrightarrow & \mathbb{C}[x_1, ..., x_n]/m \cong \mathbb{C} \end{aligned}$$

- $\varphi : \mathbb{C} \cong \mathbb{C}[x_1, ..., x_n]/m, f \mapsto \pi(f)$

- $\pi : \mathbb{C}[x_1, ..., x_n] \to \mathbb{C}[x_1, ..., x_n]/m, f \mapsto [f]$
- $\mathbb{C}[x_1, ..., x_n]/m$ ist ein Körper

$$\begin{aligned} \mathbb{C}[x_1, ..., x_n]/m &\cong \mathbb{C}[\pi(x_1), ..., \pi(x_n)] \\ \overset{Lemma}{\Longrightarrow} &\pi(x_1), ..., \pi(x_n) \in \mathbb{C} \\ \Longrightarrow &\mathbb{C}[x_1, ..., x_n]/m \cong \mathbb{C} \end{aligned}$$

- $\varphi : \mathbb{C} \cong \mathbb{C}[x_1, ..., x_n]/m, f \mapsto \pi(f)$
- Homomorphiesatz: $x_i - \varphi^{-1}(\pi(x_i)) \in \ker \pi = m$

$$(x_1 - \varphi^{-1}(\pi(x_1)), ..., x_n - \varphi^{-1}(\pi(x_n))) \subseteq m$$

$\square$

Satz (Hilberts Nullstellensatz)

Sei $I \subsetneq \mathbb{C}[x_1, ..., x_n]$ ein Ideal. Dann gilt

$$V(I) \neq \emptyset.$$

- Fall 1: I ist maximal. $I = (x_1 - \alpha_1, ..., x_n - \alpha_n)$, sodass $(\alpha_1, ..., \alpha_n) \in V(I)$

Satz (Hilberts Nullstellensatz)

Sei $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ ein Ideal. Dann gilt

$$V(I) \neq \emptyset.$$

- Fall 1: I ist maximal. $I = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$, sodass $(\alpha_1, \dots, \alpha_n) \in V(I)$
- Fall 2: I ist nicht maximal. Wir suchen ein maximales Ideal J mit $I \subseteq J$, da $V(I) \supseteq V(J) \neq \emptyset$
- Idee: Mit $I = (f_1, \dots, f_n) \subsetneq (f_1, \dots, f_{n+1}) \subsetneq \dots$ findet man eine aufsteigende Kette, die stationär werden muss

$\square$

Ein letztes Detail

Lemma

Sei $I_0 \subsetneq k[x_1, \ldots, x_n]$ ein Ideal. Dann gibt es ein maximales Ideal $J \supseteq I_0$.

Ein letztes Detail

Lemma

Sei $I_0 \subsetneq k[x_1, ..., x_n]$ ein Ideal. Dann gibt es ein maximales Ideal $J \supseteq I_0$.

- Annahme: Es gibt kein solches maximales Ideal
- Es gibt Ideale $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq ...$ (wobei $I_k \subsetneq k[x_1, ..., x_n]$)

Ein letztes Detail

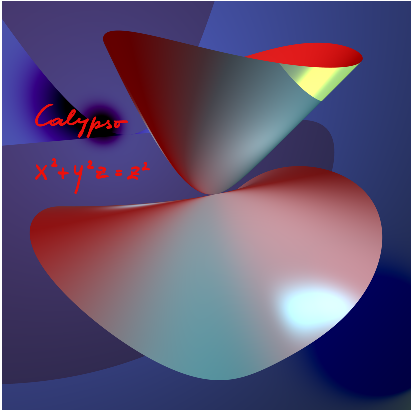
Lemma

Sei $I_0 \subsetneq k[x_1, \ldots, x_n]$ ein Ideal. Dann gibt es ein maximales Ideal $J \supseteq I_0$.

- Annahme: Es gibt kein solches maximales Ideal
- Es gibt Ideale $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$ (wobei $I_k \subsetneq k[x_1, \ldots, x_n]$)
- $\bigcup_{k \in \mathbb{N}} I_k$ ist ein Ideal
- $\bigcup_{k \in \mathbb{N}} I_k = (f_1, \ldots, f_m)$, und $f_j \in I_{n_j}$
- $\bigcup_{k \in \mathbb{N}} I_k \subseteq I_p, p := \max \{ n_j \mid 1 \leq j \leq m \}$, Widerspruch

$\square$

Quellen



- Klaus Hulek: Elementare algebraische Geometrie
- Klaus Pommerening: Hilbert's Nullstellensatz over the complex numbers
- Graphiken
  - imaginary.org/gallery/herwig-hauser-classic
  - GeoGebra