

# Analyse algebraischer Varietäten mit Hilfe von Galois-Theorie

Jugend Forscht 2025

YIMU MAO

## Inhaltsverzeichnis

<b>1</b>	<b>Motivation</b>	<b>2</b>
<b>2</b>	<b>Multivariable Polynome</b>	<b>3</b>
<b>3</b>	<b>Zerfällungskörper und Galoisgruppen von Polynomen in mehreren Variablen</b>	<b>5</b>
3.1	Zerfällungskörper eines Polynoms der Form $g_1(x)g_2(x) \in G[x]$ . . . . .	5
3.1.1	Anleitung zur Bestimmung des Zerfällungskörpers $g_1(x)g_2(x) \in G[x]$ . . . . .	6
3.2	Galoistheorie für ein Polynom in mehreren Variablen . . . . .	6
3.2.1	Anleitung zur Bestimmung des Zerfällungskörpers von $F(x, y) = f_1(x)f_2(y) \in F[x][y]$ . . . . .	6
3.2.2	Galoistheorie für Polynome der Form $F(x, y) = f_1(x) + f_2(y) \in F[x][y]$ . . . . .	8
<b>4</b>	<b>Darstellung von Polynomen in mehreren Variablen</b>	<b>10</b>
4.1	Faktorisierung von Polynomen in einer Variablen . . . . .	11
4.2	Die Faktorisierung von quadratischen Polynomen in mehreren Variablen . . . . .	12
<b>5</b>	<b>Fazit und Ausblick</b>	<b>16</b>
<b>6</b>	<b>Unterstützungsleistung</b>	<b>17</b>

# 1 Motivation

In dieser Arbeit beschäftige ich mich mit der Anzahl von Zusammenhangskomponenten von reell algebraischen Kurven.

Wir definieren für diese Arbeit allgemeine algebraische Varietäten von Kurven über folgende Weise.

**Definition 1.** Es sei  $\mathbb{K}$  ein Körper und  $f : \mathbb{K}^n \rightarrow \mathbb{K}$  ein Polynom. Dann nennen wir

$$V(f) := \{(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = 0\}$$

die algebraische Varietät des Polynoms  $f$  im Affinen Raum  $\mathbb{A}^n(\mathbb{K})$ .

Wir werden in dieser Frage die geometrische Gestalt der Kurven im affinen Raum  $\mathbb{A}^n(\mathbb{R})$  untersuchen. Dies bedeutet, dass es um die tatsächliche Darstellung in  $\mathbb{R}^n$  geht, wir aber gleichzeitig die algebraischen Strukturen über allen möglichen Zahlenräumen (also auch  $\mathbb{C}$ ) berücksichtigen.

Die Untersuchung von algebraischen Kurven spielte auch eine besondere Rolle in *Hilberts 16. Problem*, bei dem er die spezielle Frage stellte, welche allgemeinen Aussagen sich über die gegenseitige Lage von algebraischen Kurven treffen lassen. Insbesondere fragt er auch nach deren Zusammenhangskomponenten.

Eine besondere Aussage diesbezüglich ist der folgende Satz ([BoCoRo91], Seite 286):

**Theorem 1** (Harnack 1876). *Eine nichtsinguläre algebraische Kurve von Grad  $d$  besitzt in  $\mathbb{P}_2(\mathbb{R})$  höchstens  $\frac{(d-1) \cdot (d-2)}{2} + 1$  Zusammenhangskomponenten. Genauer findet sich für jede Zahl  $c$  zwischen  $\frac{1-(-1)^d}{2}$  und  $\frac{(d-1) \cdot (d-2)}{2} + 1$  auch immer eine Kurve mit  $c$  Zusammenhangskomponenten.*

Hierbei werden die Kurven in der projektiven Ebene  $\mathbb{P}_2(\mathbb{R})$  betrachtet.

Ich stelle jedoch bei meiner Analyse von Kurven in  $\mathbb{R}^2$  oder  $\mathbb{R}^3$  fest, dass es auch hier scheinbar Regeln für die Anzahl an Zusammenhangskomponenten gibt. Auch Hilbert hat sich im Jahr 1900 nicht mit dem Resultat von Harnack zufrieden gegeben. Nach Hilberts Fokus auf Kurven sechsten Grades, gelang es Dmitri Andrejewitsch Gudkov im Jahr 1969 sämtliche Kurven sechsten Grades zu klassifizieren [BoCoRo91]. Kurven, welche die maximale Anzahl an Zusammenhangskomponenten besitzen, werden als  $M$ -Kurven bezeichnet. Diese spielen auch in Gudkovs Arbeit eine große Rolle. Doch ist es möglich auch Aussagen über die Anzahl an Zusammenhangskomponenten von anderen Kurven zu treffen?

Dieser Frage möchte ich mich in dieser Arbeit widmen. Leider vermag ich es nicht, allgemeine Aussagen zu beweisen, doch für bestimmte Fälle, scheinen Regeln zu gelten, welche in dieser Form bislang noch nicht formuliert sind.

In Abbildung 1 sind verschiedene Fälle für Kurven zweiter Ordnung in  $\mathbb{R}^2$  dargestellt. Nach dem Satz von Harnack können die Kurven mit Ordnung  $d = 2$  nur keine oder eine Zusammenhangskomponente über  $\mathbb{P}_2(\mathbb{R})$  besitzen. Ich stelle mir in dieser Arbeit vielmehr die Frage, wie ich den Fall der Hyperbeln (Zwei Komponenten in  $\mathbb{R}^2$ ) von den Fällen der Ellipse oder der Parabel unterscheiden kann. In Abbildung 1 sind Beispiele für Kurven irreduzibler Polynome zweiter Ordnung zu sehen. Offensichtlich gilt der folgende Satz:

**Theorem 2.** *Es sei  $f(x_1, \dots, x_n)$  ein reduzibles Polynom. Dies bedeutet, dass es Polynome  $g_1$  und  $g_2$  gibt, mit der Eigenschaft, dass  $f(x_1, \dots, x_n) = g_1(x_1, \dots, x_n) \cdot g_2(x_1, \dots, x_n)$  gilt. Dann setzt sich die durch  $f$  erzeugte algebraische Varietät  $V(f) = V(g_1) \cup V(g_2)$  aus der Vereinigung der Varietäten von  $g_1$  und  $g_2$  zusammen.*

*Beweis.* Aufgrund des Satzes vom Nullprodukt ist die Gleichung

$$f(x_1, \dots, x_n) = g_1(x_1, \dots, x_n) \cdot g_2(x_1, \dots, x_n) = 0$$

genau dann erfüllt, wenn sie für  $g_1$  oder  $g_2$  erfüllt ist. Daher liegt ein Punkt  $(x_1, \dots, x_n)$  genau dann in der algebraischen Varietät  $V(f)$ , wenn es in  $V(g_1)$  oder in  $V(g_2)$  liegt.  $\square$

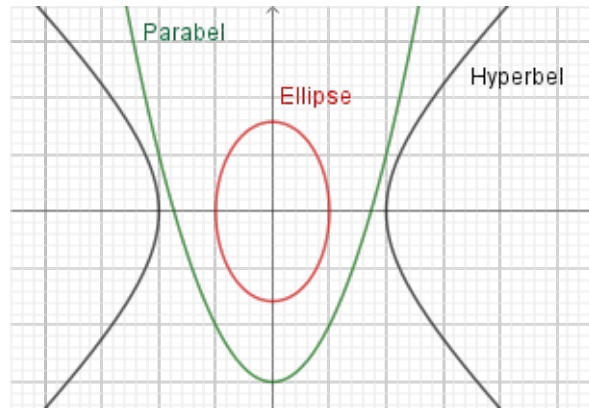


Abbildung 1: Dargestellt sind die möglichen Fälle irreduzibler Kurven zweiter Ordnung. Über  $\mathbb{P}_2(\mathbb{R})$  besitzen alle nur eine Zusammenhangskomponente (eine Kurve der Form  $x^2 + y^2 + r^2 = 0$  hätte beispielsweise gar keine Zusammenhangskomponente). Über  $\mathbb{R}^2$  ist dies jedoch nicht der Fall.

Wir sehen also, dass ein Polynom der Form  $f(x, y) = x^2 - xy$  zwar von Grad 2 ist, sich die entsprechende algebraische Kurve  $V(f)$  jedoch als Vereinigung zweier Geraden ergibt. Daraus resultiert meine weitere Untersuchung, wann man einem Polynom entnehmen kann, reduzibel zu sein.

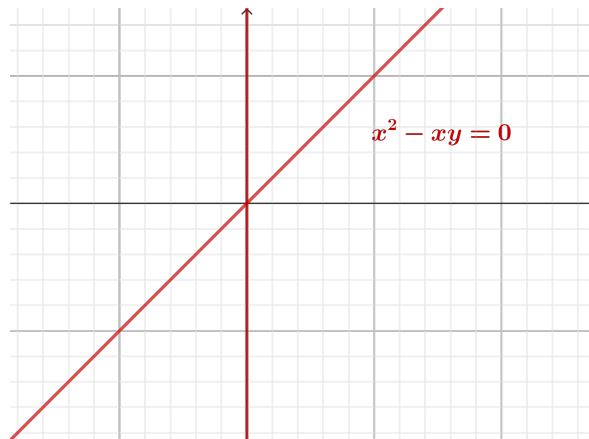


Abbildung 2: Dies ist die Nullstellenmenge der Funktion  $f(x, y) = x^2 - xy$ . Es gilt  $f(x, y) = x \cdot (x - y)$ , weswegen sich die Kurve aus der Vereinigung zweier Geraden zusammensetzt.

## 2 Multivariable Polynome

Im ersten Abschnitt wollen wir algebraisch begründen, wie wir Polynome in mehreren Variablen verstehen. Dabei werden wir feststellen, dass die Variablen bei Polynomen vertauscht werden können, ohne, dass dabei eine Veränderung der algebraischen Struktur oder der Geometrie der erzeugten Kurven entsteht. Dies ist [Hu74] entnommen.

**Theorem 3 ( Der Homomorphismus zwischen Kommutativen Ringen mit Eins).** Seien  $R$  und  $S$  kommutative Ringe, wobei  $e_1$  das Einselement von  $R$  und  $e'_1$  das Einselement von  $S$  ist. Es existiere ein Homomorphismus  $\eta: R \rightarrow S$ . Für jedes Element  $u \in S$  kann der Homomorphismus  $\eta$  eindeutig zu einem Homomorphismus  $\eta_u: R[x] \rightarrow S$  erweitert werden, sodass  $\eta_u(x) = u$  gilt. Diese Erweiterung ist eindeutig, und  $\eta$  bildet  $e_1$  auf  $e'_1$  ab.

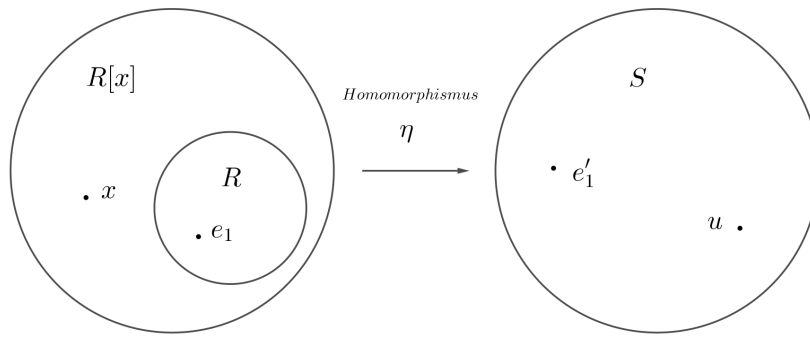


Abbildung 3: Darstellung des Homomorphismus zwischen Kommutativen Ringen mit Eins

*Beweis.* Zuerst beweisen wir die Eindeutigkeit:

$\eta_u$  hängt von  $(\eta, u)$  ab.

$\forall a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$  betrachten wir die Wirkung  $\eta_u(a_0 + a_1x + a_2x^2 + \dots + a_nx^n)$ . Weil  $\eta_u$  eine Homomorphismus ist, gilt insbesondere Linearität und wegen

$$\begin{aligned} & \eta_u(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) \\ &= \eta_u(a_0) + \eta_u(a_1)\eta_u(x) + \dots + \eta_u(a_n)\eta_u(x^n) \\ &= \eta_u(a_0) + \eta_u(a_1)u + \dots + \eta_u(a_n)u^n \end{aligned}$$

muss der Homomorphismus  $\eta_u$  auf  $R[x]$  eindeutig sein, da  $\eta_u$  nur von  $\eta$  und  $u$  abhängt.

Nun beweisen wir die Existenz.

Wir definieren  $\eta_u$  folgendermaßen für alle Polynome  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$ :

$$\eta_u(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) \equiv \eta(a_0) + \eta(a_1)u + \dots + \eta(a_n)u^n.$$

Damit sind die folgenden drei Dinge klar.

- $\eta_u$  ist eine Abbildung von  $R[x]$  bis  $S$ .
- Die Einschränkung von  $\eta_u$  auf  $R$  ist  $\eta$ , nämlich ist  $\eta_u|_R = \eta$ , insbesondere gilt damit  $\eta(e_1) = e'_1$
- $\eta_u$  ist verträglich mit den Ringeigenschaften von  $R[x]$ , denn  $\eta_u(x) = \eta_u(x) = \eta_u(1 * x) = e'_1u = u$ .

Damit ist  $\eta_u$  ein Ringhomomorphismus, welcher nur von  $\eta$  und  $u$  abhängt. □

**Korollar 1. Die Eindeutigkeit des Polynomrings in einer Variablen bis auf Isomorphie**

Sei  $R$  ein kommutativer Ring mit Eins. Für die Polynomringe  $R[x]$  und  $R[y]$  über  $R$  gilt  $R[x] \cong R[y]$ .

*Beweis.* Wir haben schon  $i(1) = 1$ . Wir können zeigen, dass seine Erweiterung ein Homomorphismus ist.

$$\begin{aligned} i_y : R[x] &\longrightarrow R[y] \\ i_y(x) &= y \end{aligned}$$

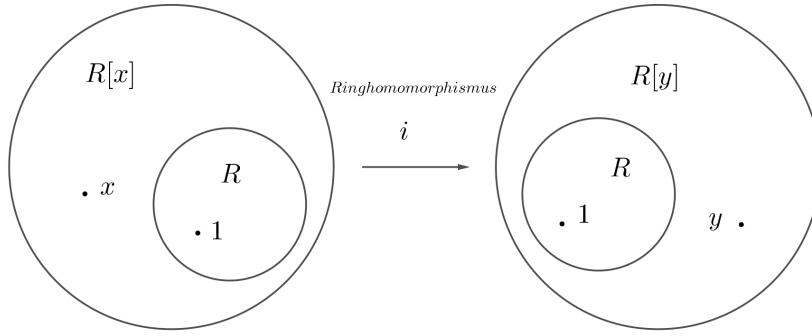


Abbildung 4: Ringhomomorphismus von  $R[x]$  nach  $R[y]$

Wir können zeigen, dass  $i_y$  ein Isomorphismus von  $R[x]$  nach  $R[y]$  ist.

$$\therefore R[x] \cong R[y]$$

Daher erhalten wir die Eindeutigkeit des Polynomrings in einer Variablen bis auf Isomorphie.  $\square$

**Bemerkung 2.1.** Mithilfe von Korollar 1 können wir begründen, warum es Polynomringe in mehreren Variablen gibt. Wir verwenden einen konstruktiven Beweis, ähnlich wie bei eindimensionalen Polynomringen. Weil  $R[x_1]$  ein kommutativer Ring ist, können wir nun sinnvoll den Ring

$$R[x_1, x_2] := R[x_1][x_2]$$

definieren. Dies ist daher ebenfalls ein kommutativer Ring. Aufgrund von Korollar 1 ist dies wohldefiniert, da  $R[x_1][x_2] \cong R[x_2][x_1]$ . Schließlich erhalten wir rekursiv die Definition von  $R[x_1, x_2, \dots, x_n] := R[x_1, \dots, x_{n-1}][x_n]$ .

Insbesondere bedeutet dies, dass im zweidimensionalen Fall, also in  $R[x, y]$  die Variablen  $x$  und  $y$  gleichberechtigt sind.

### 3 Zerfällungskörper und Galoisgruppen von Polynomen in mehreren Variablen

In der **Galoistheorie** werden die Symmetrien der Nullstellen von Polynomen untersucht. Dies ist auch für Polynome in mehreren Variablen möglich, bei denen die Nullstellenmengen dann algebraische Varietäten definieren. In diesem Abschnitt soll erläutert werden, wie man die Galoisgruppen und damit die Symmetrieeigenschaften der algebraischen Varietäten bestimmt. Dazu möchten wir die **Zerfällungskörper** der Polynome bestimmen. Dies sind die kleinstmöglichen Körper über denen das Polynom in Linearfaktoren zerfällt. Die monovariablen Galois-Theorie ist [Hu74] entnommen. Die multivariable Galois-Theorie wird üblicherweise mit Hilfe der Motivtheorie behandelt, wie in [CoMa]. Daher wurde dieser Aspekt für diese Arbeit im Sinne der klassischen Galois-Theorie überarbeitet, weswegen die einzelnen Aussagen und die Anleitungen hier explizit angegeben werden.

#### 3.1 Zerfällungskörper eines Polynoms der Form $g_1(x)g_2(x) \in G[x]$

$G[x]$  bezeichne den Polynomring mit Koeffizienten im Körper  $G$ . Für ein Polynom  $g(x) \in G[x]$  verwenden wir hier die Notation

$$\langle g(x) \rangle := \{h(x) \cdot g(x) \mid h(x) \in G[X]\}$$

für die Beschreibung des Ideals von  $g(x)$  im Polynomring.  
Wir starten mit einem Polynom der Form  $g_1(x) \cdot g_2(x)$ .

### 3.1.1 Anleitung zur Bestimmung des Zerfällungskörpers $g_1(x)g_2(x) \in G[x]$

Zunächst werden die Polynome auf Irreduzibilität überprüft. Angenommen  $g_1(x)$  und  $g_2(x)$  seien irreduzibel. Dann untersuchen wir, ob  $g_1(x) \in \frac{G[x]}{\langle g_1(x) \rangle}$  zerfällt. Falls dies nicht der Fall ist, so fügen wir die entsprechende Nullstelle zu  $G$  hinzu. Nach und nach werden so alle Nullstellen  $\alpha_1, \dots, \alpha_k$  von  $g_1$  hinzugefügt, die nicht bereits über einem anderen Körper zerfallen. Auf diese Weise erhält man den Zerfällungskörper  $K_1 = G(\alpha_1, \dots, \alpha_k)$ .

Nun wird der Prozess mit dem irreduziblen Polynom  $g_2(x)$  weitergeführt. Der Polynomring wird aber direkt über dem Zerfällungskörper  $K_1[x]$  betrachtet. Wir schauen, ob  $g_2(x) \in \frac{K_1[x]}{\langle g_2(x) \rangle}$  zerfällt. Falls nicht, so fügen wir die Nullstellen (genau wie zuvor) dem Zerfällungskörper hinzu. Letztlich erhalten wir über die Körpererweiterung mit den entsprechenden Nullstellen  $\beta_1, \dots, \beta_l$  den Zerfällungskörper des gesamten Polynoms, nämlich  $K = K_1(\beta_1, \dots, \beta_l)$ .

Falls  $g_1(x)$  oder  $g_2(x)$  reduzible Polynome sind, so können wir  $g_1(x)$  oder  $g_2(x)$  faktorisieren, beispielsweise in der Form  $g_1(x) = t_1(x)t_2(x)$ . Nun lässt sich der Prozess auf die Polynome  $t_1(x)$  und  $t_2(x)$  anwenden. Damit ist auch dieser Fall behandelt.

## 3.2 Galoistheorie für ein Polynom in mehreren Variablen

Wir betrachten zunächst einen Spezialfall und untersuchen Polynome der Form  $F(x, y) = f_1(x)f_2(y) \in F[x][y]$ .

Mit dem Vorwissen über den Zerfällungskörper von Produktpolynomen in einer Variablen können wir nun Aussagen über den Zerfällungskörper von Produktpolynomen in zwei Variablen machen.

### 3.2.1 Anleitung zur Bestimmung des Zerfällungskörpers von $F(x, y) = f_1(x)f_2(y) \in F[x][y]$

Wie im vorherigen Abschnitt können wir annehmen, dass  $f_1(x)$  und  $f_2(y)$  irreduzibel sind, da ansonsten die entsprechenden Faktorisierungen gewählt werden können.

Wir schauen, ob  $f_1(x) \in \frac{F[x][y]}{\langle f_1(x) \rangle}$  zerfällt. Wenn nicht, so fügen wir die Nullstelle, wie in Anleitung 3.1.1 hinzu. Wir erhalten damit den Zerfällungskörper  $K_1$  von  $f_1(x) \in F[x][y]$ . Mit der gleichen Methode analysieren wir, ob  $f_2(y)$  in  $\frac{K_1[x][y]}{\langle f_2(y) \rangle}$  zerfällt. Am Ende erhalten wir den Zerfällungskörper von  $F(x, y) = f_1(x)f_2(y) \in F[x][y]$ .

**Beispiel 3.1.** Wir betrachten die Polynome  $f_1(x) = x^2 - 2$  und  $f_2(y) = y^3 - 3$  über  $\mathbb{Q}$ , welche als Produkt das Polynom  $F(x, y) = f_1(x)f_2(y) = (x^2 - 2)(y^3 - 3) \in \mathbb{Q}[x][y]$  bilden.

Der Zerfällungskörper von  $f_1$  ist  $K_1 = \mathbb{Q}[\sqrt{2}]$ ,  $f_2$  zerfällt jedoch nicht über  $K_1[x][y]$ . Wir fügen die Nullstelle von  $f_2$  dem Körper  $K_1$  hinzu. Am Ende bekommen wir den Zerfällungskörper von  $F(x, y) = f_1(x)f_2(y) = (x^2 - 2)(y^3 - 3) \in \mathbb{Q}[x][y]$ , es ist  $\mathbf{K} = \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}, \omega]$  mit  $(\omega = e^{\frac{2\pi i}{3}})$ . An dieser Stelle können wir nun auch den Grad der Erweiterung bestimmen.

$$\begin{aligned} [K : \mathbb{Q}] &= [\mathbb{Q}[\sqrt{2}, \sqrt[3]{3}, \omega] : \mathbb{Q}] \\ &= [\mathbb{Q}[\sqrt{2}, \sqrt[3]{3}, \omega] : \mathbb{Q}[\sqrt[3]{3}, \omega]] \cdot [\mathbb{Q}[\sqrt[3]{3}, \omega] : \mathbb{Q}[\omega]] \cdot [\mathbb{Q}[\omega] : \mathbb{Q}] \\ &= 2 \cdot 3 \cdot 2 = 12 \end{aligned}$$

Denn es gilt  $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$  wegen  $\omega^2 + \omega + 1 = 0$ .

Die Struktur der Gruppe:

$$\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2 \quad \text{Gal}(\mathbb{Q}(\sqrt[3]{3}, \omega)/\mathbb{Q}) \cong \mathbb{S}_3,$$

da  $\sqrt[3]{3}\omega = \sqrt[3]{3}e^{\frac{2\pi i}{3}}$  die symmetrische Gruppe  $\mathbb{S}_3$  erzeugt.

Das direkte Produkt:

$$\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{S}_3$$

Daher ist die Galois-Gruppe:

$$\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{S}_3$$

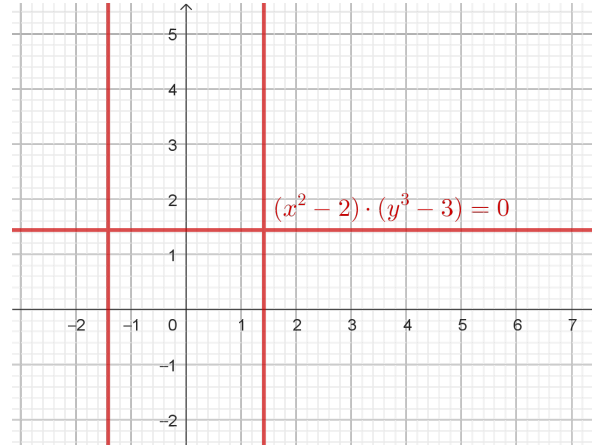


Abbildung 5: Dargestellt ist die Kurve aus Beispiel 3.1. Sie setzt sich aus zwei Teilen zusammen. Während die Kurve durch  $f_1(x) = x^2 - 2$  die beiden vertikalen Geraden definiert, welche über  $\mathbb{Z}_2$  vertauscht werden können, definiert  $f_2(y) = y^3 - 3$  eine horizontale Gerade. Die Symmetrie der Galois-Gruppe  $\mathbb{S}_3$  betrifft hier die Vertauschung in der komplexen Ebene. In  $\mathbb{R}^2$  ist lediglich die Linie für  $\sqrt[3]{3}e^{\frac{2\pi i}{3} \cdot 3}$  sichtbar. Dennoch besitzt die Kurve nicht drei Zusammenhangskomponenten, sondern nur eine. Dies liegt daran, dass sie zwei singuläre Punkte besitzt, an denen die drei Geraden miteinander verbunden sind.

**Bemerkung 3.1.** Die Betrachtung dieses Beispiels zeigt das Verfahren zur Bestimmung des Zerfällungskörpers und auch des Grades der Erweiterung. Dieses Verfahren ist individuell auf die angegebenen Polynome anzuwenden. Wir stellen außerdem fest, dass alleine die Betrachtung der Galois-Struktur nicht ausreicht, da die einzelnen Komponenten sich auch schneiden können. Dies bedeutet aber, dass an diesen Stellen sogenannte singuläre Punkte vorliegen.

**Definition 2.** Es sei  $F(x_1, \dots, x_n)$  ein Polynom über einem Körper  $\mathbb{K}$  und  $P \in V(F) \subseteq \mathbb{A}^n(\mathbb{K})$  ein Punkt auf der algebraischen Varietät von  $F$ . Dann heißt

- $P$  *singulärer Punkt*, falls für alle Koordinaten gilt, dass

$$\frac{\partial F(x_1, \dots, x_n)}{\partial x_1}(P) = \dots = \frac{\partial F(x_1, \dots, x_n)}{\partial x_n}(P) = 0$$

vorliegt.

- Andernfalls heißt  $P$  *glatter Punkt*.

Kurven mit singulären Punkten können somit grundsätzlich Zusammenhangskomponenten miteinander verbinden ohne, dass dies über die Galois-Theorie direkt erkennbar ist.

### 3.2.2 Galoistheorie für Polynome der Form $F(x, y) = f_1(x) + f_2(y) \in F[x][y]$

Als nächstes sollen Polynome der Form  $F(x, y) = f_1(x) + f_2(y) \in F[x][y]$  in zwei Variablen untersucht werden. Auch hier kann man mit derselben Methode aus Anleitung 3.2.1 vorgehen.

**Beispiel 3.2.** Wir haben  $f_1(x) = x^2 - 2$  und  $f_2(x) = y^3 - 3$ , nämlich haben wir  $F(x, y) = f_1(x) + f_2(y) = x^2 + y^3 - 5 \in \mathbb{R}[x][y]$

Die gegebene Gleichung kann äquivalent wie folgt umgeschrieben werden:

$$x^2 = 5 - y^3.$$

Um den Zerfällungskörper zu bestimmen, müssen wir alle möglichen Lösungen  $(x, y)$  finden. Diese Lösungen umfassen:

- Die Wurzeln von  $x = \pm\sqrt{5 - y^3}$ .
- Die Wurzeln von  $y^3 = 5 - x^2$ , was ein kubisches Polynom ist.

Der Zerfällungskörper enthält also:

1. Die Wurzeln des kubischen Polynoms  $y^3 - y_0 = 0$ , wobei  $y_0$  eine konstante Zahl ist.
2. Die Wurzeln des quadratischen Polynoms  $x^2 - (5 - y^3) = 0$ .

Daraus ergibt sich der Zerfällungskörper als:

$$K = \mathbb{R}(\sqrt{5 - y^3}, \omega),$$

wobei  $\omega = e^{2\pi i/3}$  eine primitive dritte Einheitswurzel ist.

Die Galois-Gruppe ist die Gruppe der Automorphismen des Zerfällungskörpers  $K$  über dem Grundkörper  $\mathbb{R}$ . Diese Automorphismen sind Symmetrien, die die Grundoperationen unverändert lassen. Es gibt zwei Symmetrien:

1. **Vertauschung der Wurzeln von  $x = \pm\sqrt{5 - y^3}$ :** Diese Symmetrie entspricht der quadratischen Gleichung  $x^2 - (5 - y^3) = 0$ . Die zugehörige Gruppe ist isomorph zu  $\mathbb{Z}_2$ , da es zwei Wurzeln gibt.
2. **Symmetrie der Wurzeln der kubischen Gleichung  $y^3 - y_0 = 0$ :** Diese Symmetrie entspricht den drei Wurzeln des kubischen Polynoms. Die zugehörige Gruppe ist  $\mathbb{S}_3$  (die symmetrische Gruppe auf drei Elementen).

Falls  $5 - y^3 > 0$  stets gilt, bleibt die Gleichung definiert über  $\mathbb{R}$ , und die Galois-Gruppe ist das direkte Produkt:

$$G = \mathbb{Z}_2 \times \mathbb{S}_3.$$

Die Anwendung der Galois-Theorie auf diese Kurve lässt vermuten, dass es sich um zwei Zusammenhangskomponenten in  $\mathbb{R}^2$  handelt, denn auch hier erhält man eine Spiegelung (durch  $\mathbb{Z}_2$ ) der Wurzeln  $x = \pm\sqrt{5 - y^3}$  an der Achse  $x = 0$ .  $\mathbb{S}_3$  beschreibt wie in 3.1 eine Vertauschung der Kurven in der komplexen Ebene. Dies führt zu keinen weiteren Zusammenhangskomponenten in  $\mathbb{R}^2$ .

Betrachten wir nun jedoch Abbildung 6, so stellen wir fest, dass die Wirkung von  $\mathbb{Z}_2$  keine zwei Komponenten erstellt. Dies liegt daran, dass die Gleichung für alle  $x \in \mathbb{R}$  Nullstellen liefert und damit der linke Ast (für  $x < 0$ ) und der rechte Ast (für  $x > 0$ ) an  $(0, \sqrt{5})$  miteinander verbunden sind. Die Kurve besitzt daher in  $\mathbb{R}^2$  lediglich eine Zusammenhangskomponente.



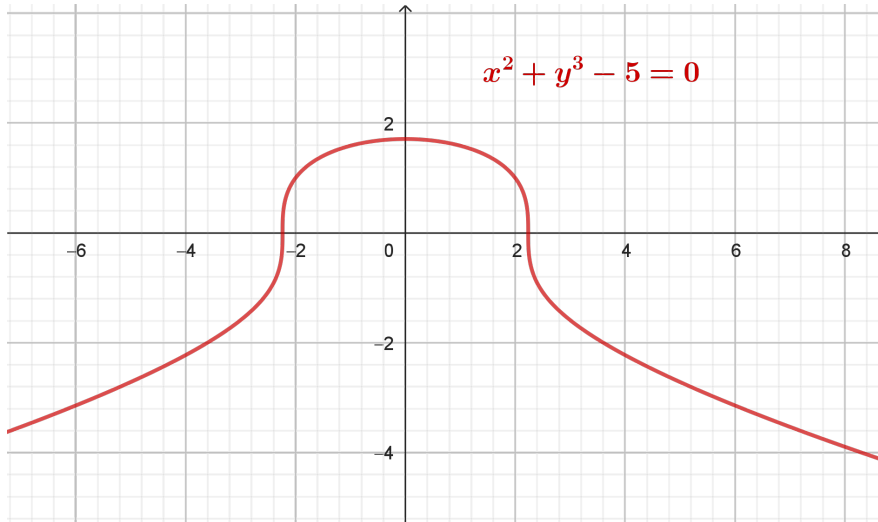


Abbildung 6: Die Kurve aus Beispiel 3.2 in  $\mathbb{R}^2$ . Man erkennt deutlich, dass es in  $\mathbb{R}^2$  nur eine Zusammenhangskomponente gibt.

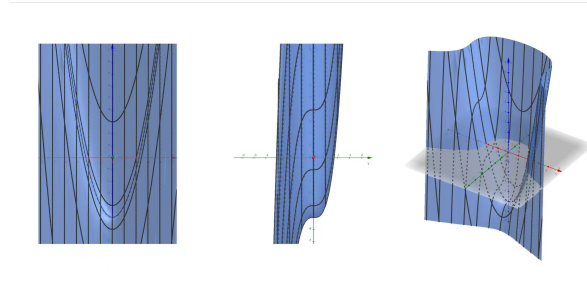


Abbildung 7: Das Verständnis der Kurve aus Beispiel 3.2: Die dargestellte Fläche entsteht durch die Bewegung der Scheitelpunkte unzähliger Parabeln (im  $xz$ -Ebene) entlang einer Kurve, die durch eine kubische Funktion (in  $yz$ -Ebene) beschrieben wird. Zu sehen ist der Schnitt mit der  $xz$ -Ebene (links), mit der  $yz$ -Ebene (Mitte) und eine Total in der 3D-Projektion (rechts)

**Bemerkung 3.2.** Für die Kurve aus Beispiel 3.2 haben wir über die 'Multi-Galois Theorie'  $G = \mathbb{Z}_2 \times \mathbb{S}_3$  ermittelt. Betrachtet man  $(x, y) \in \mathbb{C}^2$ , also  $(x, y) = (u + vi, m + ni) \in \mathbb{C}^2$ , so können wir etwas Interessantes entdecken. Wir legen  $x$  oder  $y$  fest, und stellen die 3. Achse als  $(u, v, |f|)$  oder  $(m, n, |f|)$  auf. Die entsprechenden Plots sind in Abbildung 8 zu finden.

Das sieht sehr interessant aus, wenn wir  $x$  festlegen. Wir finden, dass es zwei 'Gruben' oder 'Löcher' gibt, und wenn wir  $y$  festlegen, finden wir, dass es drei 'Gruben' oder 'Löcher' gibt. Allein aus der Galois-Gruppe lässt sich jedoch nicht erkennen, wie der Zusammenhang zwischen den 'Löchern' und den Gruppen  $\mathbb{Z}_2$  und  $\mathbb{S}_3$  aussieht.

Wir stellen folgendes Ergebnis fest:

**Bemerkung 3.3.** Die Galois-Gruppe eines Polynoms  $f$  beschreibt die Symmetrie der Nullstellenmengen der zugehörigen Varietät  $V(f)$ .

- Für jede Nullstelle, die bei der Körpererweiterung hinzugefügt wird, beschreibt die zugehörige Galois-Gruppe die Symmetrie.
- Ist die Nullstelle rein reell, so werden entsprechend viele Zusammenhangskomponenten erzeugt. Dabei entsteht nur dann eine neue Zusammenhangskomponente, wenn bei der Symmetriegruppe kein kontinuierlicher Übergang vorliegt, so wie in Beispiel 3.2 für  $x > 0$

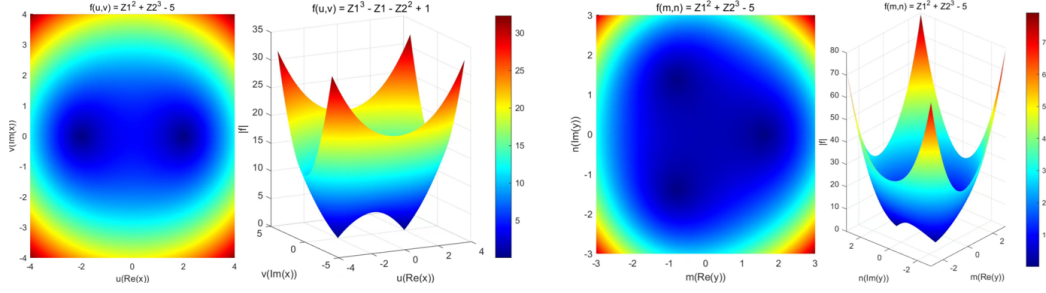


Abbildung 8: Darstellung von  $u, v$  und  $|f|$  im linken Plot sowie  $n, m$  und  $|f|$  im rechten Plot in der komplexen Ebene

und  $x < 0$ . Außerdem muss die Kurve noch auf singuläre Punkte untersucht werden, da möglicherweise verschiedene Komponenten der Kurve an diesen zusammengeführt werden.

- Wird eine Komponente über komplexe Nullstellen hinzugefügt, so entsteht entweder eine oder keine reelle Zusammenhangskomponente, je nachdem ob der Grad des Polynoms gerade oder ungerade ist.

Daher wird deutlich, dass die Galois-Gruppe eines Polynoms großen Aufschluss über die Zusammenstellung der Zusammenhangskomponenten gibt. Weiterhin muss die Kurve aber auch auf singuläre Punkte überprüft werden.

Ist das Polynom irreduzibel, so ist es sehr interessant die zugehörige Galois-Gruppe zu untersuchen. Dies resultiert in einer Fragestellung, die es weiter zu untersuchen gilt:

**Fragestellung:** Wir untersuchen die Kurve  $V(f)$  eines Polynoms von Grad  $n$ . Angenommen

- Das Polynom ist irreduzibel,
- Die Galois-Gruppe von  $f$  ist maximal  $\text{Gal}(f) = \mathbb{S}_n$ ,
- Die Kurve besitzt keine singulären Punkte.

Welche zusätzlichen Eigenschaften muss  $f$  besitzen, um sicher sein zu können, dass die Anzahl der Zusammenhangskomponenten gerade  $n$  beträgt und die Galois-Gruppe damit die Symmetrie zwischen den verschiedenen Komponenten beschreibt?

Wir haben bereits gesehen, dass man sicherstellen muss, dass die Komponenten entlang der Symmetrie nicht miteinander verbunden sind (wie in Beispiel 3.2). Hier entsteht schließlich nur eine Zusammenhangskomponente in  $\mathbb{A}^2(\mathbb{R})$ . Wir haben in unserer bisherigen Untersuchung beispielsweise festgestellt, dass Kurven, welche aus symmetrischen Polynomen entstehen (und somit automatisch eine Symmetrie bezüglich der  $x = y$ -Achse besitzen) die Untersuchung vereinfachen. Dies ist in Abbildung 9 an einem symmetrischen Polynom von Grad 5 zu erkennen.

Wie aber erkennt man, ob ein Polynom irreduzibel ist oder nicht? Dies soll im Folgenden untersucht werden.

## 4 Darstellung von Polynomen in mehreren Variablen

Wir haben gesehen, dass es einfach ist Kurven von reduziblen Polynomen auf ihre irreduziblen Komponenten zurückzuführen (siehe Theorem 2). Mit Anleitung 3.2.1 ist es ebenso einfach die Galois-Gruppe eines multivariablen Polynoms der Form  $F = f_1 \cdot f_2$  zu bestimmen. Sobald aber das Polynom aus der Summe irreduzibler Polynome zusammengesetzt wird, ist es sehr schwer

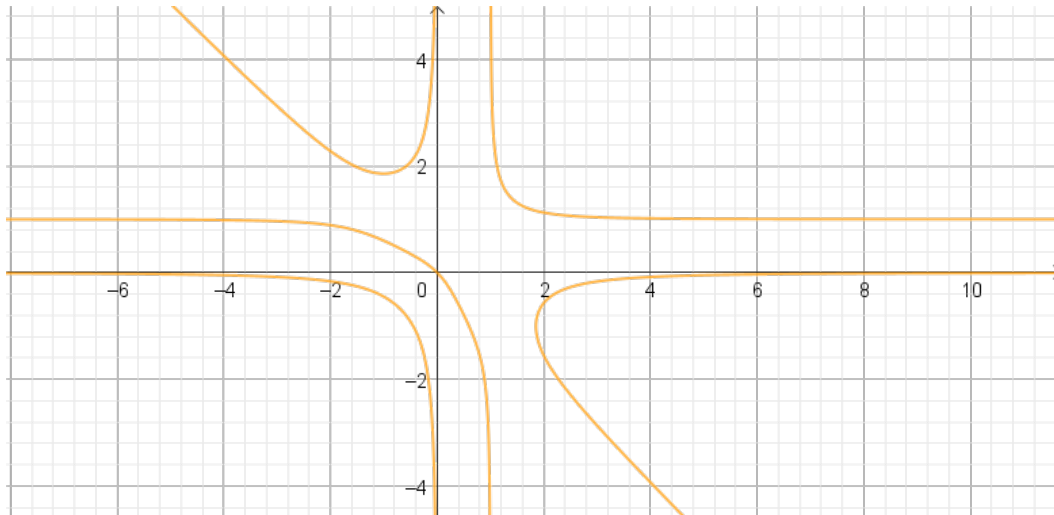


Abbildung 9: Ein symmetrisches, irreduzibles Polynom von Grad 5 ohne singuläre Punkte, ohne Absolutterm und mit maximaler Galois-Gruppe erfüllt die Bedingungen für 5 Zusammenhangskomponenten. Doch welche weiteren Bedingungen benötigt man, um zu verhindern, dass es keine geschlossenen Komponenten gibt?

herauszufinden, wie die Galois-Gruppe aussieht und damit auch sehr schwer zu entscheiden, wie die Zusammenhangskomponenten der Kurve zueinander stehen.

Kann es gelingen ein multivariables Polynom mit Hilfe von Division zu reduzieren?

#### 4.1 Faktorisierung von Polynomen in einer Variablen

Im Falle einer Variablen ist es immer möglich dies zu tun. So lässt sich die folgende Umformung machen

$$F(x) = x^3 + 2x^2 - x + 1 = x \cdot (x^2 + 2x - 1) + 1 = f_1(x) \cdot f_2(x) + r,$$

es lässt sich somit für jedes  $F$  sofort eine Paarung  $f_1, f_2, r$  finden mit  $\deg(r) < \deg(f_1) \leq \deg(f_2) \leq \deg(F)$  finden. Dies geht nach folgender Anleitung:

**Lemma 1.** *Es sei  $F(x)$  ein Polynom von Grad  $\deg(F) = d$ . Dann gibt es durch das folgende Verfahren eine Zerlegung von  $F$ :*

- Wähle ein Polynom  $f_1$  von Grad  $\deg(f_1) < d$ .
- Führe nun eine Polynomdivision  $F/f_1$  durch.
- Brich diese Division gerade dann ab, dass der Restterm  $r$  noch ein Polynom ist.

Auf diese Weise entsteht eine Zerlegung  $F(x) = f_1(x) \cdot f_2(x) + r(x)$  mit  $\deg(r) \leq \deg(f_2) = d - \deg(f_1)$

**Beispiel 4.1.** *Im Fall von mehreren Variablen geht dies nicht so einfach, denn es gilt beispielsweise*

$$x_1 x_2^3 + x_1 x_2 + 4x_3 = x_1^2 \left( \frac{1}{x_1} x_2^3 + \frac{1}{x_1} x_2 + 4x_3 \frac{1}{x_1^2} \right)$$

Obwohl  $\deg(x_1^2) = 2 < \deg(F)$  ist, entsteht keine valide Zerlegung, denn  $\frac{1}{x_1} x_2^3 + \frac{1}{x_1} x_2 + 4x_3 \frac{1}{x_1^2}$  ist kein Element von  $F[x_1, \dots, x_3]$ . Auf diese Weise gelingt es also nicht eine Darstellung als  $F = f_1 \cdot f_2 + r$  zu finden.

Für  $n > 1$  können wir den Grad eines  $n$ -variablen Polynoms somit nicht effektiv reduzieren. Das bedeutet, dass  $F[x_1, x_2, \dots, x_n]$  keine Division mit Rest besitzt, und wir daher den  $n$ -variablen Polynomring nicht aus der Perspektive der Division mit Rest untersuchen können. Trotzdem können wir die Divisionsbeziehung immer noch definieren, nämlich können wir  $F(x_1, \dots, x_n) = f_1(x_1, \dots, x_n)f_2(x_1, \dots, x_n)$  definieren, wie wir durch die folgende Aussage sehen werden.

**Theorem 4.** *Der Polynomring in  $n$  Variablen über einem eindeutigen Faktorisierungsring ist selbst ein eindeutiger Faktorisierungsring. Dies bewirkt, dass sich Polynome in  $n$  Variablen eindeutig faktorisieren lassen.*

*Beweis.* Wir wissen bereits, dass der Polynomring in einer Variablen über einem eindeutigen Faktorisierungsring selbst ein eindeutiger Faktorisierungsring ist. Nun nehmen wir an, dass der Polynomring in  $(n-1)$  Variablen über einem eindeutigen Faktorisierungsring ebenfalls ein eindeutiger Faktorisierungsring ist. Da der Polynomring in  $n$  Variablen als ein Polynomring in einer Variablen über dem Polynomring in  $(n-1)$  Variablen betrachtet werden kann, folgt offensichtlich, dass der Polynomring in  $n$  Variablen über einem eindeutigen Faktorisierungsring ebenfalls ein eindeutiger Faktorisierungsring ist.  $\square$

Dies soll im folgenden untersucht werden. Zunächst betrachten wir ein Beispiel.

## 4.2 Die Faktorisierung von quadratischen Polynomen in mehreren Variablen

**Beispiel 4.2 (Faktorisierung einer quadratischen Gleichung in zwei Variablen).** *Den einfachsten nichttrivialen Fall stellt die Faktorisierung Funktion von Grad 2 in zwei Variablen dar. Denn, falls  $f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$  sich faktorisieren lässt, dann hat die Faktorisierung eindeutig die Form  $(\alpha x + \beta y + p)(qx + ry + s) = 0$ .*

*Wir möchten die auftretenden Fälle klassifizieren und führen dazu eine Transformation durch. Dazu setzen wir*

$$\begin{cases} \Delta := b^2 - 4ac \\ \Delta_x := d^2 - 4af \\ \Delta_y := e^2 - 4cf \end{cases}$$

*Mithilfe dieser Transformation lässt sich die notwendige und hinreichende Bedingung für die Faktorisierbarkeit einer quadratischen Gleichung in zwei Variablen einfach darstellen. Diese Umformung entstammt [Zhang].*

$$\begin{cases} \Delta = b^2 - 4ac \geq 0 \\ \Delta_x = d^2 - 4af \geq 0 \\ \Delta_y = e^2 - 4cf \geq 0 \\ bde = ae^2 + cd^2 + f\Delta \end{cases}$$

$\Delta$  ist die Diskriminante der Gleichung und  $\Delta_x$  und  $\Delta_y$  erweitern diese Idee auf die Faktorisierbarkeit. Daher erhält man drei mögliche Fälle für die Darstellung des faktorisierten Polynoms.

$$f(x, y) = \begin{cases} \frac{1}{4a} \left[ 2ax + (b + \sqrt{\Delta})y + d + \sqrt{\Delta_x} \right] \cdot \left[ 2ax + (b - \sqrt{\Delta})y + d - \sqrt{\Delta_x} \right] & \text{falls } (bd - 2ae > 0) \\ \frac{1}{4a} \left[ 2ax + (b + \sqrt{\Delta})y + d \right] \cdot \left[ 2ax + (b - \sqrt{\Delta})y + d \right] & \text{falls } (bd - 2ae = 0) \\ \frac{1}{4a} \left[ 2ax + (b + \sqrt{\Delta})y + d - \sqrt{\Delta_x} \right] \cdot \left[ 2ax + (b - \sqrt{\Delta})y + d + \sqrt{\Delta_x} \right] & \text{falls } (bd - 2ae < 0) \end{cases}$$

**Beispiel 4.3 (Faktorisierung eines höhergradigen Polynoms).** *Bei einem höhergradigen Polynom fällt es sehr schwer zu erkennen, ob dieses faktorisiert ist. Liegt beispielsweise eine solche Gleichung  $f(x, y) = 0$  vor, so ist die Geometrie der zugehörigen algebraischen Kurve*

kaum zu erkennen.  $f(x, y) = x^5 + x^4 y - 7x^4 + 2x^3 y^2 - 12x^3 y + 30x^3 + 2x^2 y^3 - 18x^2 y^2 + 42x^2 y - 50x^2 + x y^4 - 12x y^3 + 30x y^2 + 12x y - 31x + y^5 - 11y^4 + 42y^3 - 46y^2 - 43y + 57 = 0$   
Führt man jedoch die entsprechende Faktorisierung durch und formt diesen Term, so erhält man die äquivalente Darstellung

$$f(x, y) = (x + y - 3) (x^2 + y^2 - 1) \left( (x - 2)^2 + (y - 4)^2 - 1 \right) = 0$$

Und nun ist es offensichtlich, dass es sich um drei Zusammenhangskomponenten handelt, da die Kurve sich aus einer Geraden und zwei Kreisen zusammensetzt.

Im Falle nur einer Variablen fällt die Darstellung  $F(x) = f_1(x) \cdot f_2(x) + r(x)$  nach Lemma 1 leicht. Im multivariablen Fall funktioniert diese Methode nicht mehr, wie wir in Beispiel 4.1 gesehen haben. Allerdings gibt es für die höherdimensionalen Fälle als Kriterien zur Bestimmung der eindeutigen Faktorisierbarkeit das Eisenstein-Kriterium (siehe [Bo09]).

**Theorem 5** (Eisensteinkriterium). Sei  $P(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$  ein Polynom und  $p$  eine Primzahl. Falls folgende Bedingungen erfüllt sind:

1. Der führende Koeffizient von  $P(x_1, x_2, \dots, x_n)$  (hinsichtlich der Ordnung der Variablen) ist nicht durch  $p$  teilbar.
2. Alle übrigen Koeffizienten von  $P(x_1, x_2, \dots, x_n)$  sind durch  $p$  teilbar.
3. Der konstante Term (falls vorhanden) von  $P(x_1, x_2, \dots, x_n)$  ist nicht durch  $p^2$  teilbar.

Dann ist  $P(x_1, x_2, \dots, x_n)$  irreduzibel im Polynomring  $\mathbb{Z}[x_1, x_2, \dots, x_n]$ .

Wie aber geht man vor, wenn das Eisensteinkriterium nicht anwendbar ist? Daher möchten wir nun zunächst für einfache Polynome in mehreren Variablen eine Bedingung finden.

**Definition 3** (Koeffizientenmatrix). Es sei  $F$  ein quadratisches Polynom in  $n$  Variablen. Dann besitzt  $F$  eine Darstellung in der folgenden Form

$$\begin{aligned} F(x_1, x_2, \dots, x_n) = & c_{11}x_1^2 + c_{12}x_1x_2 + \dots + c_{1n}x_1x_n + c_{1,n+1}x_1 \\ & + c_{22}x_2^2 + \dots + c_{2n}x_2x_n + c_{2,n+1}x_2 \\ & + \dots \\ & + c_{nn}x_n^2 + c_{n,n+1}x_n \\ & + c_{n+1,n+1} \end{aligned}$$

Diese können wir nun in ihre quadratische Form überführen. Das Polynom lässt sich eindeutig über eine Koeffizientenmatrix der Form

$$\mathbf{C} = \begin{pmatrix} c_{11} & c_{12} & c_{13} & \dots & c_{1n} & c_{1,n+1} \\ 0 & c_{22} & c_{23} & \dots & c_{2n} & c_{2,n+1} \\ 0 & 0 & c_{33} & \dots & c_{3n} & c_{3,n+1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & c_{n+1,n+1} \end{pmatrix} \quad (1)$$

beschreiben. Denn verwenden wir nun den erweiterten Variablenvektor

$$\mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_n \\ 1 \end{pmatrix} \quad (2)$$

so erhalten wir die Darstellung von  $F$  in der Form  $F(x_1, \dots, x_n) = \mathbf{X}^T \mathbf{C} \mathbf{X}$ .

**Theorem 6 ( Die notwendige und hinreichende Bedingung für die Zerlegung eines quadratischen Polynoms mit mehreren Variablen ).** Sei  $F(x_1, \dots, x_n)$  ein quadratisches Polynom mit  $n$  Variablen über dem reellen (komplexen) Zahlenkörper, und sei  $\mathbf{C}$  die zugehörige Koeffizientenmatrix mit  $F(x_1, \dots, x_n) = \mathbf{X}^T \mathbf{C} \mathbf{X}$ , (siehe Definition 3). Dann ist  $F$  genau dann faktorisiert - es existiert also eine Darstellung der Form

$$F(x_1, \dots, x_n) = (a_1 x_1 + \dots + a_n x_n + a_{n+1})(b_1 x_1 + \dots + b_n x_n + b_{n+1}),$$

wenn es eine  $(n+1)$ -dimensionale reelle (komplexe) schiefsymmetrische Matrix  $\mathbf{C}$  gibt, sodass

$$F(x_1, \dots, x_n) = \mathbf{X}^T (\mathbf{C} + \mathbf{Q}) \mathbf{X},$$

und eine der folgenden Bedingungen erfüllt ist:

1.  $\mathbf{C} + \mathbf{Q}$  lässt sich direkt über das Tensorprodukt eines Vektors mit einem Kovektor schreiben, also  $\mathbf{C} + \mathbf{Q} = \begin{bmatrix} a_1 \\ \dots \\ a_n \end{bmatrix} [b_1, \dots, b_{n+1}]$ .
2. Die Elemente von zwei beliebigen Zeilen (oder Spalten) von  $\mathbf{C} + \mathbf{Q}$  sind paarweise proportional.
3. Alle  $2 \times 2$ -Unterdeterminanten von  $\mathbf{C} + \mathbf{Q}$  sind gleich null.
4. Der Rang von  $\mathbf{C} + \mathbf{Q}$  ist gleich 1.

*Beweis.* Nach [Hu74] sind die Bedingungen 1. bis 4. äquivalent zueinander. Wir beweisen daher lediglich die Äquivalenz der Faktorisierung mit Bedingung 1.

Es gelte  $F(x_1, \dots, x_n) = (a_1 x_1 + \dots + a_n x_n + a_{n+1})(b_1 x_1 + \dots + b_n x_n + b_{n+1})$ . Wir definieren

für die Kurznotation  $G = \begin{bmatrix} a_1 \\ \dots \\ a_n \end{bmatrix}$ ,  $H = [b_1, \dots, b_{n+1}]$  und multiplizieren damit die faktorisierte Darstellung von  $f$  aus.

$$\begin{aligned} f(x_1, \dots, x_n) &= (a_1 x_1 + \dots + a_n x_n + a_{n+1})(b_1 x_1 + \dots + b_n x_n + b_{n+1}) \\ &= (\mathbf{X}^T G)(H \mathbf{X}) = X^T (GH) \mathbf{X} = X^T \begin{pmatrix} a_1 b_1 & a_1 b_2 & \dots & a_1 b_{n+1} \\ a_2 b_1 & a_2 b_2 & \dots & a_2 b_{n+1} \\ \dots & \dots & \dots & \dots \\ a_{n+1} b_1 & a_{n+1} b_2 & \dots & a_{n+1} b_{n+1} \end{pmatrix} \mathbf{X} \\ &= X^T \begin{pmatrix} a_1 b_1 & a_1 b_2 + a_2 b_1 & a_1 b_3 + a_3 b_1 & \dots & a_1 b_{n+1} + a_{n+1} b_1 \\ 0 & a_2 b_2 & a_2 b_3 + a_3 b_2 & \dots & a_2 b_{n+1} + a_{n+1} b_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{n+1} b_{n+1} \end{pmatrix} \mathbf{X}. \end{aligned}$$

Dies gilt, weil die Einträge in der Koeffizientenmatrix jeweils die Koeffizienten des Polynoms beschreiben. Der Koeffizient vor  $x_i x_j$  ergibt sich aber aus  $a_i b_j$  und  $a_j b_i$ . Damit haben wir nun also eine Dreiecksmatrix, die sich aus der Summe zweier Matrizen darstellen lässt. Wir können nun genauer die Einträge der Matrizen  $\mathbf{C}$  und  $\mathbf{Q}$  angeben.

Nach der Darstellung in Definition 3 erhalten wir somit die Beschreibung

$$c_{ii} = a_i b_i, \quad c_{ij} = a_i b_j + a_j b_i \text{ für } i < j$$

Wir definieren dann

$$q_{ij} = \begin{cases} -a_j b_i & \text{falls } i < j \\ 0 & \text{falls } i = j, \\ a_i b_j & \text{falls } i > j \end{cases}$$

für jedes  $i, j = 1, 2, \dots, n+1$ , gibt es nun eine schiefsymmetrische Matrix  $Q = (q_{ij})$ . Dann haben wir

$$f(x_1, \dots, x_n) = \mathbf{X}^T(\mathbf{C} + \mathbf{Q})\mathbf{X}$$

wobei

$$\mathbf{C} + \mathbf{Q} = \mathbf{H} \cdot \mathbf{G}$$

gilt. Damit ist die erste Richtung bewiesen.

Betrachten wir nun die Rückrichtung: Angenommen es gilt

$$F(x_1, \dots, x_n) = \mathbf{X}^T(\mathbf{C} + \mathbf{Q})\mathbf{X},$$

mit  $\mathbf{C} + \mathbf{Q} = \begin{bmatrix} a_1 \\ \dots \\ a_n \end{bmatrix} [b_1, \dots, b_{n+1}]$ . Dann muss man jedoch nur die Matrizen ausmultiplizieren und erhält sofort das Ergebnis

$$F(x_1, \dots, x_n) = (a_1x_1 + \dots + a_nx_n + a_{n+1})(b_1x_1 + \dots + b_nx_n + b_{n+1}).$$

Damit ist der Beweis abgeschlossen.  $\square$

**Beispiel 4.4.** Wir betrachten ein Polynom zweiten Grades in drei Variablen und möchten Theorem 6 anwenden.

- Es sei  $F(x, y, z) = 2x^2 + 5xy + 3xz - 2x + 2y^2 + 3yz - y + z^2 - z$ . Dann können wir die Koeffizientenmatrix  $\mathbf{C}$  bilden und erhalten

$$\mathbf{C} = \begin{pmatrix} 2 & 5 & 3 & -2 \\ & 2 & 3 & -1 \\ & & 1 & -1 \\ & & & 0 \end{pmatrix}$$

Nach Theorem 6 suchen wir nun eine schiefsymmetrische Matrix  $\mathbf{Q}$ , sodass  $\mathbf{C} + \mathbf{Q}$  Rang 1 besitzt (4). Dies lässt sich einfach konstruieren, da alle Spalten von  $\mathbf{C} + \mathbf{Q}$  kollinear zur letzten Spalte von  $\mathbf{C}$  sein müssen, gleichzeitig die Diagonaleinträge aber nicht geändert werden können, weil  $\mathbf{Q}$  auf der Diagonale nur Nullen stehen hat. Somit können wir eindeutig eine Matrix  $\mathbf{Q}$  konstruieren mit

$$\mathbf{C} + \mathbf{Q} = \begin{pmatrix} 2 & 4 & 2 & -2 \\ 1 & 2 & 1 & -1 \\ 1 & 2 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 3 & -2 \\ & 2 & 3 & -1 \\ & & 1 & -1 \\ & & & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 & -1 & 0 \\ 1 & 0 & -2 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Damit ist  $F(x, y, z)$  faktorisiert und es gilt  $F(x, y, z) = (x + 2y + z - 1) \cdot (2x + y + z)$

- Verändern wir die obige Funktion ein wenig und verwenden die Koeffizientenmatrix

$$\mathbf{C} = \begin{pmatrix} 2 & 5 & 3 & -2 \\ & 2 & 3 & -1 \\ & & 1 & -1 \\ & & & 1 \end{pmatrix}$$

so lässt sich keine passende Matrix  $\mathbf{Q}$  finden, denn nun müsste jede Spalte von  $\mathbf{C} + \mathbf{Q}$

kollinear zu  $\begin{pmatrix} -2 \\ -1 \\ -1 \\ 1 \end{pmatrix}$  sein. Insbesondere muss dann, weil  $c_{33} = 1$  ist, die dritte Spalte den

Ausdruck  $\begin{pmatrix} 2 \\ 1 \\ 1 \\ -1 \end{pmatrix}$  besitzen. Dies definiert aber den Eintrag  $q_{43} = -1$ . Weil  $\mathbf{Q}$  schiefssymmetrisch sein muss, ist somit  $q_{34} = 1$ . Damit müsste aber  $-1 = c_{34} = c_{34} + q_{34} = 0$  gelten, was falsch ist. Es gibt somit nach Theorem 6 keine Faktorisierung dieses Polynoms, es ist irreduzibel.

**Bemerkung 4.1.** Wir können den Fall für den zweiten Grad auf den  $m$ -ten Grad erweitern, das heißt, wir müssen die Matrizen durch Tensoren ersetzen und das Skalarprodukt durch das Tensorprodukt.

Dies bedeutet, dass wir eine algorithmische Methode gefunden haben, um Polynome auf Linearisierung zu untersuchen. Lässt sich eine Gleichung vollständig in lineare Polynome zerlegen, so können wir damit auch bestimmen, wie viele zusammenhängende Komponenten sie genau hat, da lediglich die Linearkomponenten verglichen werden müssen. Beispielsweise findet man mit dieser Methode eine Linearzerlegung von

$$f(x, y) = x^3 + 6x^2y + 12xy^2 - x + 8y^3 - 2y = (x + 2y + 1)(x + 2y + 0)(x + 2y - 1).$$

Damit wird deutlich, dass  $V(f)$  aus drei parallelen Geraden besteht und es somit drei Zusammenhangskomponenten gibt.

**Bemerkung 4.2.** Den von uns betrachteten Fall von quadratischen Polynomen in  $n$  Variablen, können wir auf ähnliche Weise auf Polynome beliebigen Grades in zwei Variablen übertragen. Liegen lediglich zwei Variablen  $x$  und  $y$  vor, so können wir symbolische Vektoren der

Form  $\mathbf{x} = \begin{pmatrix} x^n \\ \vdots \\ x^0 \end{pmatrix}$  und  $\mathbf{y} = \begin{pmatrix} y^n \\ \vdots \\ y^0 \end{pmatrix}$  verwenden, um damit die Polynome mit einer Koeffizien-

tenmatrix  $\mathbf{A}$  als  $F(x, y) = \mathbf{y}^T \mathbf{A} \mathbf{x}$  darzustellen. Im Spezialfall von symmetrischen Polynomen in  $x$  und  $y$  lässt sich die Gesamtinformation des Polynoms wieder in einer Dreiecksmatrix erfassen, sodass möglicherweise eine ähnliche Methode wie in Theorem 6 angewendet werden kann, um die Irreduzibilität zu überprüfen.

## 5 Fazit und Ausblick

Bei der Untersuchung algebraischer Varietäten haben wir die Galois-Theorie verwendet, um Aussagen über die Anzahl ihrer Zusammenhangskomponenten zu treffen. Dabei haben wir festgestellt, dass die Galois-Theorie zwar Hinweise auf die Gestalt der Kurven gibt, sie alleine jedoch nicht ausreicht, um die Kurven zu klassifizieren.

Des weiteren haben wir uns auf einen Spezialfall fokussiert, nämlich dass ein reelles quadratisches Polynom in  $n$  Variablen in Linearfaktoren zerlegt werden kann. Diese Methode können wir auf beliebige reelle Polynome  $f(x_1, x_2, \dots, x_n)$  vom Grad  $m$  in  $n$  Variablen erweitern. Mit Hilfe von Theorem 6 kann dieser Spezialfall explizit untersucht werden.

Als nächsten Schritt müssen wir irreduzible Polynome in  $\mathbb{K}[x, y]$  untersuchen. Natürlich ist die Anzahl ihrer zusammenhängenden Komponenten über dem komplexen Zahlenfeld eins, da ihre algebraischen Varietäten nicht als Vereinigung zweier algebraischer Varietäten ausgedrückt werden können. Die Untersuchung über den komplexen Zahlen ist ein sehr bekanntes Forschungsgebiet - in der klassischen algebraischen Geometrie werden Kurven in der Zariski-Topologie betrachtet. Der Satz von Bézout kann als Fundamentalsatz der Algebra für zwei Variablen verstanden werden. Letztlich kann man damit für irreduzible Polynome die Zariski-Zusammenhangskomponenten bestimmen [MIT-Lecture].

Ein weiterer Ansatz besteht darin, mithilfe der Clifford-Algebra Matrizen zu definieren, um mehrdimensionale hochgradige Polynome im komplexen Zahlenfeld zu zerlegen, wie zum



Beispiel  $\mathbf{I}(x^2 + y^2) = (\mathbf{A}_1 x + \mathbf{A}_2 y)^2$ , wobei

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathbf{A}_2 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

Die entscheidende Bedingung ist hier die Antikommutativität der verwendeten Matrizen.  
 $\mathbf{A}_1 \mathbf{A}_2 + \mathbf{A}_2 \mathbf{A}_1 = 0$

## 6 Unterstützungsleistung

Beim Verfassen der schriftlichen Arbeit hat mich mein Projektbetreuer Christopher Tropp unterstützt.

## Literatur

- [BoCoRo91] Jacek Bochnak, Michael Coste, Marie-Francoise Roy, *Real Algebraic Geometry, 3rd edition*. Springer-Verlag (1991)
- [Bo09] Siegfried Bosch, *Algebra*. Springer-Verlag (2009)
- [Hu74] Thomas W. Hungerford, *Algebra*. Springer-Verlag (1974)
- [Mo96] Patrick Morandi, *Field and Galois Theory*. Springer-Verlag (1996)
- [Ed84] Harold M. Edwards, *Galois Theory*. Springer-Verlag (1984)
- [CoMa] Alain Connes, Matilde Marcolli [Noncommutative Geometry, Quantum Fields and Motives](#)
- [AtMcD69] M. F. Atiyah, I.G. McDonald *Introduction to Commutative Algebra*. CRC Press (1969)
- [Va24] Ravi Vakil, *The Rising Sea - Foundations of Algebraic Geometry*. math216 Worldpress (2024)
- [MIT-Lecture] [Bezout theorem Lecture 13](#), MIT Education.
- [Zhang] [Forumseintrag bei zhihu.com](#), Xu Zhang, National Taiwan Normal University
- [Gao] Shuhong Gao, [Factoring multivariate Polynomials via Partial Differential Equations](#).