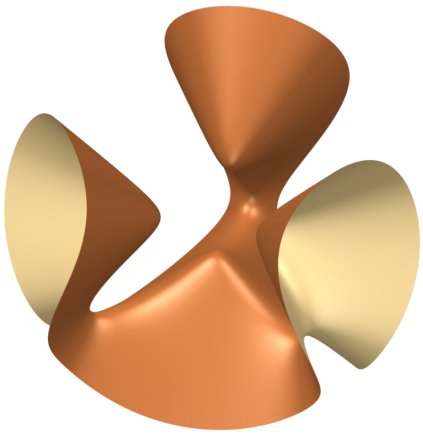
Vorlesungsskript
♢
Faktorielle Ringe, multivariate Polynome und algebraische Hyperflächen

Prof. Dr. Hagen Knaf
Studiengang Angewandte Mathematik
Hochschule RheinMain

WS 2023/24



»Gespräch« – eine algebraische Fläche

Hinweis

Inhaltsverzeichnis

Einleitung

Für den Ring $\mathbb{Z}$ der ganzen Zahlen gilt der als »Hauptsatz der Arithmetik« oder »Fundamentalsatz der elementaren Zahlentheorie« bezeichnete

SATZ: *Jede ganze Zahl $z \in \mathbb{Z} \setminus 0$ lässt sich eindeutig als Produkt*

$$z = u \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

schreiben, wobei $u \in \{-1, 1\}$, $e_1, \ldots, e_r \in \mathbb{N}$ und $p_1, \ldots, p_r$ positive Primzahlen sind.

Ein vollständiger Beweis dieses Satzes findet sich erstmalig(?) in den »Disquisitiones Arithmeticae« [Gau] von Carl Friedrich Gauß. Jedoch war bereits Euklid von Alexandria ein etwas schwächeres Resultat bekannt:

PROPOSITION 14 IN BUCH IX: *Ist eine Zahl die kleinste, welche von gegebenen Primzahlen geteilt wird, so wird sie von keiner anderen Primzahl außer den gegebenen geteilt.*

Aus dieser Proposition lässt sich die Eindeutigkeit der Primfaktorisierung für solche Zahlen folgern, die sich als Produkt paarweise verschiedener Primzahlen darstellen lassen. Der wesentliche Baustein für den Beweis ist dabei:

LEMMA VON EUKLID: *Teilt eine Primzahl ein Produkt zweier ganzer Zahlen, so teilt sie einen der beiden Faktoren.*

Die im Lemma von Euklid formulierte Eigenschaft von Primzahlen kann man zur Verallgemeinerung des Primzahlbegriffs in kommutativen Ringen benutzen, was zum Begriff des Primelements führt. Natürlicherweise stellt sich dann die Frage, in welchen Ringen ein Analogon des Hauptsatzes der Arithmetik gilt. Im vorliegenden Skript wird als ein Hauptergebnis bewiesen, dass dies für die Polynomringe $K[X_1, \ldots, X_n]$ in n Unbestimmten über einem Körper K der Fall ist.

Primelemente und Primfaktorisierungen (in Polynomringen) treten beispielsweise in folgenden Kontexten auf:

- Konstruktion von endlichen Körpern $\mathbb{F}_q$ von Primzahlpotenzordnung $q = p^n$, $n > 1$: Solche Körper sind grundlegend für die mathematische Kryptographie (siehe z.B. [H-P-S]) sowie die Theorie der fehlerkorrigierenden Kodes (siehe z.B. [Mac]).

- Als algorithmisch schwieriger Kern von Kryptosystemen: Systeme vom Rivet-Shamir-Adleman-Typ (RSA-Systeme) nutzen die Primfaktorzerlegung in $\mathbb{Z}$ als Kern. Diese sind inzwischen weitgehend durch Systeme ersetzt, die auf dem diskreten Logarithmenproblem in elliptischen Kurven über endlichen Körpern beruhen – »Elliptic Curve Cryptography« (ECC). Motiviert durch die Entwicklung der Quantencomputertechnologie wird seit etwa 2016 versucht gegen Attacken mit Quantencomputern sichere Kryptosysteme zu identifizieren, die dann wiederum die ECC-Systeme ersetzen werden – Informationen hierzu finden sich auf der Webseite des National Institute of Standards and Technology (NIST, `https://www.nist.gov/`). In diesem Zusammenhang werden auch solche Systeme diskutiert, die auf der Faktorisierung multivariater Polynome beruhen.

- Geometrie algebraischer Mannigfaltigkeiten: Die Primfaktorisierung eines multivariaten Polynoms oder dessen so genannter Leitform lässt Schlüsse auf die Gestalt der Menge der Nullstellen dieses Polynoms zu. Die Analyse solcher Nullstellenmengen tritt zum Beispiel bei der Untersuchung der Kinematik von Roboterarmen auf (siehe z.B. [BHA]).

Als Literatur zu den Abschnitten 1, 2 und 3 wird das Lehrbuch [K-M] empfohlen. Dort findet man insbesondere im Kapitel 14 die algebraischen Grundlagen zu Polynomen in einer und mehreren Unbestimmten mit Koeffizienten in einem kommutativen Ring. Im Kapitel 24 wird weiter die Konstruktion des algebraischen Abschlusses eines Körpers dargestellt.

Grafiken: Die im Skript vorhandenen Grafiken wurden mit zwei Werkzeugen erstellt:

- dem online unter `https://www.desmos.com/` verfügbaren *Desmos Grafikrechner*,

- der unter `https://www.imaginary.org/` kostenfrei erhältlichen Software *Surfer*.

1 Primfaktorisierung in Integritätsbereichen

Wir betrachten im Folgenden ausschließlich Ringe $(R, +, \cdot)$ mit Eins, in denen das Kommutativgesetz

$$\forall r, s \in R \quad r \cdot s = s \cdot r$$

gilt. Weiter wird die Existenz von sogenannten Nullteilern ausgeschlossen, das heißt es gilt

$$r \cdot s = 0 \Rightarrow r = 0 \vee s = 0.$$

Die dadurch definierte Klasse von Ringen trägt einen eigenen Namen:

DEFINITION 1.1: *Ein Ring $(R, +, \cdot)$ heißt Integritätbereich, falls die Multiplikation in R kommutativ ist und R keine Nullteiler besitzt.*

In einem Integritätsbereich kann man »kürzen«: Für $r, s, t \in R$, $r \neq 0$ gilt nämlich

$$rs = rt \Leftrightarrow 0 = rs - rt = r(s - t) \Leftrightarrow s - t = 0 \Leftrightarrow s = t.$$

Für die Diskussion der Teilbarkeit in Integritätsbereichen spielt die Menge

$$R^\times := \{r \in R : \exists s \in R \quad rs = 1\}$$

der multiplikativ invertierbaren Elemente (»Einheiten«) eines kommutativen Rings R mit Eins eine Rolle. Die Einheiten bilden eine abelsche Gruppe, die erheblich umfangreicher sein kann als im Fall der ganzen Zahlen.

Teilbarkeit wird nun definiert, indem man den Fall ganzer Zahlen imitiert:

DEFINITION 1.2: *Für Elemente $r \in R$ und $d \in R \setminus 0$ eines Integritätsbereichs R definiert man*

$$d|r :\Leftrightarrow \exists q \in R \quad r = qd.$$

Gilt $d|r$, so sagt man »d teilt r« oder »d ist ein Teiler von r« oder »r ist ein Vielfaches von d«.

Gilt $d|r$ und $d, q \notin R^\times$, so bezeichnet man d auch als echten Teiler von r.

Die Eigenschaften der Teilbarkeitsrelation sind nun tatsächlich vergleichbar mit denen der Teilbarkeit ganzer Zahlen.

FESTSTELLUNG 1.3: *Die Teilbarkeitsrelation besitzt die folgenden Eigenschaften:*

1. $\forall r \in R \setminus 0 \;\; 1|r,\; r|0,\; r|r,$
2. $r|1 \Leftrightarrow r \in R^\times,$
3. $d|r \Rightarrow \forall s \in R \;\; ds|rs,$
4. $d|r_k,\; k = 1, \ldots, n \Rightarrow \forall s_1, \ldots, s_n \in R \;\; d|(r_1 s_1 + \ldots + r_n s_n),$
5. $r|s \wedge s|t \Rightarrow r|t,$
6. $r|s \wedge s|r \Rightarrow \exists u \in R^\times \;\; r = us.$

Diese Eigenschaften zu überprüfen ist eine einfache Übung für das Rechnen in kommutativen Ringen bzw. Integritätsbereichen.

In bezug auf Teilbarkeit verhalten sich $d \in \mathbb{Z}$, $d \neq 0$ und $-d$ völlig gleich, das heißt:

$$\forall z \in \mathbb{Z}\; d|z \Leftrightarrow -d|z.$$

Man beachte dabei, dass $\mathbb{Z}^\times = \{-1, 1\}$ gilt.

Entsprechend gilt in einem beliebigen Integritätsbereich: Ist $d \in R$, $d \neq 0$ und gilt $r = qd$, so folgt $r = (u^{-1}q)(ud)$ für jede Einheit $u \in R^\times$. Man kann also festhalten:

$$\forall r \in R\; \forall u \in R^\times \;\; d|r \Leftrightarrow (ud)|r. \tag{1}$$

Dieses Verhalten motiviert die

DEFINITION 1.4: *Zwei Elemente $r, s \in R$ heißen assoziiert (Notation: $r \sim s$), falls es $u \in R^\times$ mit $s = ur$ gibt.*

Die folgenden Eigenschaften der Assoziiertheitsrelation ergeben sich unmittelbar aus der Definition: $r \sim r$; $r \sim s \Leftrightarrow s \sim r$; $r \sim s \wedge s \sim t \Rightarrow r \sim t$. Mit anderen Worten:

FESTSTELLUNG 1.5: *Assoziiertheit von Elementen ist eine Äquivalenzrelation auf der Menge $R \setminus 0$.*

Die Eigenschaft (1) kann man nun auch so formulieren: Mit d ist auch jedes zu d assoziierte Ringelement ein Teiler von r.

BEISPIEL 1.6: Zu einer ganzen Zahl $m \in \mathbb{Z}$ betrachten wir die Menge

$$\mathbb{Z}[\sqrt{m}] := \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Man prüft leicht nach, dass $\mathbb{Z}[\sqrt{m}]$ zusammen mit der Addition und Multiplikation komplexer Zahlen einen Integritätsbereich bildet, für den $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{m}]$ gilt. Ist $m \geq 0$, so hat man $\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{R}$. Ist m keine Quadratzahl, so ist $\mathbb{Z} \neq \mathbb{Z}[\sqrt{m}]$, was im Weiteren angenommen wird.

Die Abbildung

$$N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z}, a + b\sqrt{m} \mapsto (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

erweist sich im Hinblick auf Teilbarkeitsfragen als nützlich, da sie multiplikativ ist:

$$\begin{aligned} N((a + b\sqrt{m})(c + d\sqrt{m})) &= N(ac + bdm + (ad + bc)\sqrt{m}) \\ &= (ac + bdm)^2 - (ad + bc)^2 m \\ &= a^2c^2 + 2acbdm + b^2d^2m^2 - (a^2d^2 + 2adbc + b^2c^2)m \\ &= a^2(c^2 - d^2m) - b^2(c^2 - d^2m)m \\ &= N(a + b\sqrt{m}) \cdot N(c + d\sqrt{m}). \end{aligned}$$

Aus dieser Eigenschaft ergeben sich:

A. Aus $d|r$ in $\mathbb{Z}[\sqrt{m}]$ folgt $N(d)|N(r)$ in $\mathbb{Z}$.

B. $r \in \mathbb{Z}[\sqrt{m}]^\times \Leftrightarrow N(r) \in \mathbb{Z}^\times$.

Wir bestimmen für einige Fälle Einheiten $a + b\sqrt{m}$ in $\mathbb{Z}[\sqrt{m}]$. Nach der Eigenschaft B der Funktion N sind hierzu die Gleichungen

$$a^2 - mb^2 = \pm 1$$

ganzzahlig zu lösen.

- $m < 0$: Die Gleichung $a^2 - mb^2 = -1$ besitzt keine Lösung, während die Gleichung $a^2 - mb^2 = 1$ die Lösungen $a = \pm 1$ und $b = 0$ besitzt. Ist $m = -1$, so kommen die Lösungen $a = 0$ und $b = \pm 1$ hinzu. Dies zeigt:

$$\begin{aligned} \mathbb{Z}[i]^\times &= \{\pm 1, \pm i\}, \\ \mathbb{Z}[\sqrt{m}]^\times &= \{\pm 1\} \text{ für } m < -1. \end{aligned}$$

- $m = 2$: Der Ring $\mathbb{Z}[\sqrt{2}]$ besitzt unendlich viele Einheiten. Die Gleichung $a^2 - 2b^2 = -1$ besitzt nämlich die Lösung $a = b = 1$ zu welcher die Einheit $1+\sqrt{2}$ gehört; es gilt $(1+\sqrt{2})^{-1} = -(1-\sqrt{2})$. Da $\mathbb{Z}[\sqrt{2}]^\times$ eine Gruppe ist, sind dann auch alle Potenzen $(1+\sqrt{2})^k$, $k \in \mathbb{N}$, Einheiten. Die Behauptung ist also bewiesen, falls alle diese Potenzen verschieden sind. Wäre dem nicht so, so gäbe es ein $k \in \mathbb{N}$ mit der Eigenschaft $(1+\sqrt{2})^k = 1$, was wegen $1+\sqrt{2} > 1$ unmöglich ist.

  Die Unendlichkeit der Gruppe $\mathbb{Z}[\sqrt{m}]^\times$ lässt sich für alle $m \in \mathbb{N}$ zeigen, die nicht durch eine Quadratzahl teilbar sind.

Auch die Eigenschaft A der Funktion N liefert in Kombination mit Eigenschaft B interessante Einsichten wie etwa: Ist $N(r)$ eine Primzahl, so besitzt das Element $r \in \mathbb{Z}[\sqrt{m}]$ keine echten Teiler. Hierzu einige Beispiele:

- Besitzt das Element $r = a + b\sqrt{m}$ im Ring $\mathbb{Z}[\sqrt{m}]$ keine echten Teiler, so gilt dies auch für die Elemente $s := -a + b\sqrt{m}$ und $t := a - b\sqrt{m}$, da $N(s) = N(r) = N(t)$ gilt.

- Im Ring $\mathbb{Z}[i]$ besitzen die Elemente $1+i$, $1+2i$, $2+i$, $3+2i$ und $2+3i$ keine echten Teiler.

- Im Ring $\mathbb{Z}[\sqrt{3}]$ besitzen die Elemente $1+\sqrt{3}$, $4+\sqrt{3}$ und $5+2\sqrt{3}$ keine echten Teiler.

$\diamond$

Beispiel 1.7: Der Polynomring $R[X]$ mit Koeffizienten in einem kommutativen Ring mit Eins ist genau dann ein Integritätsbereich, wenn dies für R selbst gilt, denn $R \subset R[X]$. Weiter gilt $R[X]^\times = R^\times$: Die Inklusion $\supseteq$ ist klar. Gilt andererseits $p \cdot q = 1$ für Polynome $p, q \in R[X]$, so liefert die Anwendung der Gradfunktion $\deg(p) = \deg(q) = 0$.

Diese Aussagen gelten aufgrund der Gleichung

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$$

auch für Polynomringe in mehreren Unbestimmten.

Ist R ein Integritätsbereich, so ist ein Polynom $p \in R[X]$ genau dann durch ein Polynom der Form $X - \alpha$, $\alpha \in R$ teilbar, wenn $p(\alpha) = 0$ gilt.

Im Fall $R = \mathbb{C}$ gilt daher für jedes $p \in \mathbb{C}[X]\backslash 0$ nach dem Fundamentalsatz der Algebra

$$p = c \prod_{i=1}^{r} (X - \alpha_i)^{e_i}, \tag{2}$$

wobei $c \in \mathbb{C}\backslash 0$ der Leitkoeffizient von p, $\alpha_1, \ldots, \alpha_r$ die verschiedenen Nullstellen von p in $\mathbb{C}$ und $e_1, \ldots, e_r$ deren Vielfachheiten sind. Diese Faktorzerlegung von p ist also eindeutig. Hieraus folgt: Ist d ein Teiler von p, so ist d Produkt von Faktoren der Form $(X - \alpha_i)^{f_i}$, $f_i \leq e_i$, und einer Konstanten $c' \neq 0$.

Für den Fall $R = \mathbb{R}$ kann man aus der Faktorisierung (2) Folgendes schließen: Jedes $p \in \mathbb{R}[X] \setminus 0$ lässt sich eindeutig in der Form

$$p = c \prod_{i=1}^{r} (X - \alpha_i)^{e_i} \prod_{j=1}^{s} q_j^{f_j} \tag{3}$$

darstellen, wobei $c \in \mathbb{R} \setminus 0$ der Leitkoeffizient von p, $\alpha_1, \ldots, \alpha_r$ die verschiedenen Nullstellen von p in $\mathbb{R}$, $e_1, \ldots, e_r$ deren Vielfachheiten und $q_1, \ldots, q_s$ paarweise verschiedene, normierte quadratische Polynome ohne reelle Nullstellen sind. Die Faktorisierung (3) ergibt sich aus (2) aufgrund folgender einfacher Beobachtung: *Ist $\alpha \in \mathbb{C}$ eine Nullstelle des Polynoms $p \in \mathbb{R}[X]$, so ist auch die komplex-konjugierte Zahl $\overline{\alpha}$ eine Nullstelle von p.* $\diamond$

Die in den Beispielen 1.6 und 1.7 betrachteten Ringe R besitzen eine Gemeinsamkeit: Im beiden Fällen existiert eine Funktion $\delta : R \setminus 0 \to \mathbb{N}_0$ mit der Eigenschaft

$$r = dq \text{ mit } d, q \in R \setminus R^\times \quad \Rightarrow \quad \delta(d) < \delta(r). \tag{4}$$

Im ersten Fall ist $\delta = N$ und im zweiten $\delta = \deg$. Die Existenz einer solchen Funktion hat eine interessante Konsequenz: Besitzt ein gegebenes Element $r \in R \setminus 0$ eines solchen Rings echte Teiler, so lässt es sich als $r = q_1 q_2$ mit $\delta(q_1) < \delta(r)$ und $\delta(q_2) < \delta(r)$ schreiben. Diesen Schluss kann man nun auch auf die Elemente q_1 und q_2 anwenden. Fährt man so fort, ergibt sich nach *endlich vielen Schritten* eine Darstellung der Form

$$r = p_1 \cdot p_2 \cdot \ldots \cdot p_r, \tag{5}$$

in der keiner der Faktoren p_i noch echte Teiler besitzt. Man beachte dabei, dass die p_i nicht notwendigerweise paarweise verschieden sind. Die Faktorisierungen (2) und (3) sind von der Form (5), wenn man als Faktoren die

jeweils vorkommenden Polynome der Gestalt $X - \alpha$ beziehungsweise $X - \alpha$ und q wählt. Die Konstante c (eine Einheit!) kann man einem beliebigen der genannten Polynome zuschlagen.

Es drängt sich die Frage auf, ob die Faktorisierung (5), falls sie für ein Element r existiert, als Verallgemeinerung der Primfaktorzerlegung ganzer Zahlen betrachtet werden kann. Dies ist im allgemeinen nicht der Fall, wie das folgende Beispiel zeigt:

BEISPIEL 1.8: Wir betrachten den Ring $\mathbb{Z}[\sqrt{-5}]$ und die zugehörige Funktion

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

– siehe Beispiel 1.6.

Die Elemente 3, $2+\sqrt{-5}$ und $2-\sqrt{-5}$ dieses Rings besitzen keine echten Teiler: Ist r eines der drei Elemente, so gilt $N(r) = 9$. Sei nun d ein Teiler von r. Dann gilt nach Eigenschaft A $N(d)|9$ und damit $N(d) = 1$, $N(d) = 3$ oder $N(d) = 9$. Im ersten Fall folgt $d = 1$ oder $d = -1$. Der zweite Fall kann nicht vorkommen, da für $d \neq 0$ stets $N(d)$ eine Qudratzahl oder größer gleich 5 ist. Im dritten Fall gilt $N(q) = 1$ für $r = qd$, womit $q = -1$ oder $q = 1$ folgt. Insgesamt ist d also kein echter Teiler von r.

Die Gleichung

$$3^2 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

zeigt, dass das Element $r = 9$ zwei verschiedene Faktorisierungen in Elemente ohne echte Teiler besitzt. Das wäre nichts Besonderes, wenn das Element 3 zu einem der beiden Faktoren auf der rechten Seite assoziiert wäre. Dies ist aber nicht der Fall, da aus Beispiel 1.6 bekannt ist, dass $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$ gilt. ◇

Trotz ihres mit dem Beispiel 1.8 demonstrierten unhandlichen Verhaltens im Hinblick auf die Eindeutigkeit von Faktorisierungen, sind Ringelemente ohne echte Teiler von Bedeutung in der Ringtheorie und erhalten daher einen eigenen Namen:

DEFINITION 1.9: *Sei R ein Integritätsbereich. Ein Element $q \in R$ heißt irreduzibel, falls q keine Einheit ist und es keine Faktorzerlegung $q = ab$ mit $a, b \notin R^\times$ gibt.*

BEMERKUNG: Ist q irreduzibel und $q' \sim q$, so ist auch q' irreduzibel.

Analysiert man den Beweis für die Eindeutigkeit der Primfaktorisierung ganzer Zahlen, so erkennt man, dass dafür die im Lemma von Euklid (siehe Einleitung) formulierte Eigenschaft verantwortlich ist. Man imitiert diese daher im Bereich der Ringe:

DEFINITION 1.10: *Ein Element $p \in R$ heißt Primelement, falls p keine Einheit ist und die Eigenschaft*

$$\forall a, b \in R \quad p|(ab) \Rightarrow (p|a \vee p|b)$$

besitzt.

BEMERKUNGEN:

1. Ist p ein Primelement und $p' \sim p$, so ist auch p' ein Primelement.
2. Per Induktion zeigt man leicht, dass für ein Primelement p die folgende allgemeinere Teilbarkeitseigenschaft gilt:

$$\forall a_1, \ldots, a_m \in R \quad p|(a_1 \cdot \ldots \cdot a_m) \Rightarrow (p|a_1 \vee \ldots \vee p|a_m).$$

FESTSTELLUNG 1.11: *Jedes Primelement ist irreduzibel.*

BEWEIS: Für da Primelement p gelte $p = ab$. Ohne Einschränkung folgt dann $p|a$ also $p = pcb$ und damit $cb = 1$. Folglich ist b eine Einheit. □

Eine Darstellung eines Elements $r \in R \setminus 0$ der Form

$$r = \prod_{i=1}^{m} p_i^{e_i} \tag{6}$$

mit Primelementen $p_1, \ldots, p_m$ und Exponenten $e_1, \ldots, e_m \in \mathbb{N}$ bezeichnet man als *Primfaktorisierung von r*. Man kann nun tatsächlich wie im Fall des Rings $\mathbb{Z}$ eine Eindeutigkeitsaussage für solche Darstellungen beweisen:

SATZ 1.12: *Es seien $p_1, \ldots, p_m$ und $q_1, \ldots, q_n$ paarweise nicht assoziierte Primelemente des Integritätsbereichs R. Aus einer Gleichung der Gestalt*

$$\prod_{i=1}^{m} p_i^{e_i} = \prod_{j=1}^{n} q_j^{f_j} \tag{7}$$

folgt dann $m = n$ und nach geeigneter Umnummerierung der Faktoren $p_i \sim q_i$ und $e_i = f_i$ für alle i.

Insbesondere gilt: Die Primfaktorisierung (6) eines Elements $r \in R \setminus 0$ ist, falls sie existiert, bis auf das Ersetzen von Primfaktoren durch dazu assoziierte Elemente eindeutig.

Beweis: Man führt eine Induktion nach der Anzahl

$$N := \sum_{i=1}^{m} e_i$$

der Faktoren auf der linken Seite der Gleichung (7) durch.

Im Fall $N = 1$ steht auf der linken Seite der Gleichung (7) nur ein Primelement p. Da dieses irreduzibel ist, kann auch auf der rechten Seite nur ein Primelement q stehen und die Behauptung ist bewiesen.

Es sei nun $N \geq 2$. Die linke Seite der Gleichung (7) besitzt dann die Form $p_1 \cdot s$ mit $s \in R \setminus R^\times$. Damit ist p_1 ein echter Teiler der rechten Seite und da p_1 ein Primelement ist, folgt $p_1 | q_j$ für ein $j \in \{1, \ldots, n\}$ – ohne Einschränkung kann man $j = 1$ annehmen. Da q_1 ein Primelement ist, folgt $p_1 \sim q_1$, womit sich die Gleichung

$$p_1^{e_1} \prod_{i=2}^{m} p_i^{e_i} = u p_1^{f_1} \prod_{j=2}^{n} q_j^{f_j}$$

mit einer Einheit $u \in R^\times$ ergibt. Nun muss $e_1 = f_1$ gelten: Wäre nämlich $e_1 > f_1$, so ergäbe die Division durch $p_1^{f_1}$ die Gleichung

$$p_1^{e_1 - f_1} \prod_{i=2}^{m} p_i^{e_i} = u \prod_{j=2}^{n} q_j^{f_j},$$

also $p_1 \sim q_j$ für ein $j > 1$ und damit $q_1 \sim q_j$ im Widerspruch zur Annahme, dass die Primelemente q_j paarweise nicht assoziiert sind. Der Fall $e_1 < f_1$ wird analog behandelt.

Kürzen liefert nun

$$\prod_{i=2}^{m} p_i^{e_i} = u \prod_{j=2}^{n} q_j^{f_j},$$

womit die Induktionsannahme anwendbar ist, da die linke Seite $N - e_1$ Faktoren besitzt und die Einheit u zu einem der Faktoren q_j zugeschlagen werden kann. □

Motiviert durch Satz 1.12 definiert man:

DEFINITION 1.13: *Ein faktorieller Ring ist ein Integritätsbereich, in dem jedes Element eine Primfaktorisierung besitzt.*

Die Primfaktorisierung eines irreduziblen Elements q eines Integritätsbereichs R muss, falls sie existiert, aus genau einem Primfaktor bestehen, da sich sonst ein Widerspruch zur Irreduzibilität ergäbe. Folglich ist q dann selbst ein Primelement. Dies zeigt:

FESTSTELLUNG 1.14: *In einem faktoriellen Ring ist jedes irreduzible Element ein Primelement.*

Wir kennen bereits Beispiele sowohl für faktorielle wie für nicht faktorielle Ringe:

- $\mathbb{Z}$ ist ein faktorieller Ring – siehe Einleitung.
- $\mathbb{C}[X]$ ist ein faktorieller Ring.

  Wegen der auf dem Fundamentalsatz der Algebra beruhenden Gleichung (2) ist nur zu zeigen, dass Polynome der Form $X - \alpha$ Primelemente sind. Aus $(X - \alpha)|(f \cdot g)$ folgt aber $0 = (f \cdot g)(\alpha) = f(\alpha)g(\alpha)$, also $f(\alpha) = 0$ oder $g(\alpha) = 0$ und damit $(X - \alpha)|f$ oder $(X - \alpha)|g$.
- $\mathbb{R}[X]$ ist ein faktorieller Ring.

  Die Argumentation verläuft im Wesentlichen analog zum vorherigen Fall.
- $\mathbb{Z}[\sqrt{-5}]$ ist *kein* faktorieller Ring.

  Wäre dieser Ring faktoriell, so müssten die Faktoren der im Beispiel 1.8 angegebenen Faktorisierungen für das Element 9 nach Feststellung 1.14 und Satz 1.12 zueinander assoziiert sein. Wie im Beispiel bewiesen, ist dies nicht der Fall.

Abschließend behandeln wir noch das technische Problem die Primfaktorisierung in einem faktoriellen Ring eindeutig zu machen - Satz 1.12 liefert nur die Eindeutigkeit bis auf Assoziierte.

DEFINITION 1.15: *Sei R ein faktorieller Ring. Eine Teilmenge $P \subset R$ von Primelementen heißt repräsentativ, falls sie die folgenden beiden Eigenschaften besitzt:*

- *Zu jedem Primelement $q \in R$ gibt es ein Primelement $p \in P$ mit $p \sim q$.*
- *Für je zwei verschiedene $p_1, p_2 \in P$ gilt $p_1 \not\sim p_2$.*

Es ist klar, dass in einem faktoriellen Ring R stets eine repräsentative Menge P von Primelementen existiert.

Ist $q \in R$ ein Primelement, so gibt es *genau ein* $p \in P$ mit $q \sim p$: Gäbe es zwei verschiedene zu q assoziierte Primelemente $p_1, p_2 \in P$, so hätte man $p_1 \sim q \sim p_2$ im Widerspruch zur Eigenschaft 2 einer repräsentativen Menge.

SATZ 1.16: *Sei R ein faktorieller Ring und $P \subset R$ eine repräsentative Menge von Primelementen. Dann gibt es zu jeder Nichteinheit $r \neq 0$ eindeutig bestimmte Primelemente $p_1, \ldots, p_m$ und natürliche Zahlen $e_1, \ldots, e_m$ sowie eine eindeutig bestimmte Einheit $u \in R^\times$ für welche*

$$r = u \prod_{i=1}^{m} p_i^{e_i}$$

gilt.

BEWEIS: Nach Annahme besitzt eine Nichteinheit $r \neq 0$ eine Primfaktorisierung

$$r = \prod_{i=1}^{m} q_i^{e_i},$$

in der die Primelemente $q_1, \ldots, q_m$ bis auf Assoziierte und die Exponenten $e_1, \ldots, e_m$ eindeutig sind. Zu jedem q_i existiert genau ein $p_i \in P$ mit $p_i \sim q_i$ also $q_i = u_i p_i$ mit einer durch q_i und p_i eindeutig bestimmten Einheit $u_i \in R^\times$. Es folgt

$$r = \prod_{i=1}^{m} (u_i p_i)^{e_i} = \prod_{i=1}^{m} u_i^{e_i} \prod_{i=1}^{m} p_i^{e_i}.$$

Das Produkt

$$u := \prod_{i=1}^{m} u_i^{e_i}$$

ist eine Einheit, da $R^\times$ eine Gruppe ist. □

Beispiel 1.17: Die Primelemente in dem faktoriellen Ring $\mathbb{R}[X]$ sind die Polynome

$$a_1X + a_0,\ a_0 \in \mathbb{R}, a_1 \in \mathbb{R} \setminus 0,$$

sowie die quadratischen Polynome

$$a_2X^2 + a_1X + a_0,\ a_0, a_1 \in \mathbb{R}, a_2 \in \mathbb{R} \setminus 0$$

ohne reelle Nullstellen. Da $\mathbb{R}[X]^\times = \mathbb{R} \setminus 0$ gilt, ist eine repräsentative Menge von Primelementen durch die Polynome

$$X + a_0,\ a_0 \in \mathbb{R},$$

sowie die quadratischen Polynome

$$X^2 + a_1X + a_0,\ a_0, a_1 \in \mathbb{R}$$

ohne reelle Nullstellen gegeben. ◇

2 Euklidische Ringe

Wir haben bereits gesehen, dass die Existenz einer bezüglich Teilbarkeit streng monotonen Funktion $\delta : R \setminus 0 \to \mathbb{N}_0$ die Existenz von Faktorisierungen in irreduzible Elemente nach sich zieht. Mit etwas anderen Anforderungen an δ kann man erreichen, dass der Ring R sogar faktoriell ist. Diese Anforderungen ergeben sich aus einer Verallgemeinerung der Division mit Rest für ganze Zahlen.

Definition 2.1: *Ein euklidischer Ring ist ein Paar (R, δ) bestehend aus einem Integritätsbereich R und einer Abbildung*

$$\delta : R \setminus 0 \to \mathbb{N}_0$$

mit folgender Eigenschaft (»Division mit Rest bezüglich δ«):

$$\forall s \in R, d \in R \setminus 0\ \ \exists q, r \in R \quad s = qd + r \wedge (r = 0 \vee \delta(r) < \delta(d)).$$

Beispiele euklidischer Ringe

- $(\mathbb{Z}, |\cdot|)$: Division mit Rest.
- $(K[X], \deg)$, K ein Körper: Polynomdivision.
- $(\mathbb{Z}[i], N)$: Die Elemente des Rings $\mathbb{Z}[i]$ sind geometrisch betrachtet die Punkte der Ebene $\mathbb{R}^2$ mit ganzzahligen Koordinaten. Für die zugehörige Funktion N (siehe Beispiel 1.6) gilt $N(s) = |s|^2$.

  Zu $s \in \mathbb{Z}[i]$ und $d \in \mathbb{Z}[i] \setminus 0$ betrachte man die komplexe Zahl $\frac{s}{d} = x + iy$. Ab- oder aufrunden von x und y liefert insgesamt vier Elemente von $\mathbb{Z}[i]$, die die Ecken eines Quadrats der Seitenlänge 1 bilden. Für mindestens einem solchen Eckpunkt $q \in \mathbb{Z}[i]$ gilt also

  $$|\frac{s}{d} - q| \leq \frac{1}{2}\sqrt{2}.$$

  Es folgt

  $$|s - qd|^2 \leq \frac{1}{2}|d|^2,$$

  womit man $r := s - qd$ setzen kann.

Lemma 2.2: *Die Folge $(d_i)_{i\in\mathbb{N}}$ in dem euklidischen Ring (R, δ) besitze die Eigenschaften*

- $\forall i \in \mathbb{N}\ d_i \neq 0 \wedge d_i \notin R^\times$,
- $\forall i \in \mathbb{N}\ d_{i+1}$ *ist Teiler von* d_i.

Dann gibt es ein $k \in \mathbb{N}$ mit der Eigenschaft

$$\forall i \geq k \quad d_i \sim d_k.$$

Beweis: Es sei $(d_i)_{i\in\mathbb{N}}$ eine Folge mit den angegebenen Eigenschaften. Da d_{i+1} Teiler von d_i ist, gilt

$$Rd_i \subseteq Rd_{i+1} \tag{8}$$

für alle $i \in \mathbb{N}$. Man betrachtet nun die Menge

$$I := (\bigcup_{i\in\mathbb{N}} Rd_i) \setminus 0.$$

Die Menge $\delta(I)$ besitzt ein minimales Element $\delta(d_0)$. Nach Definition gilt $d_0 \in Rd_k$ für ein $k \in \mathbb{N}$. Für ein beliebiges $t \in I$ liefert die Division mit Rest $t = qd_0 + r$. Wäre $r \neq 0$, so hätte man $\delta(r) < \delta(d_0)$. Andererseits gilt aber $t \in Rd_\ell$ für ein $\ell \in \mathbb{N}$ und damit $d_0, t \in Rd_{\max(k,\ell)}$. Es folgt

$$r = t - qd_0 \in Rd_{\max(k,\ell)} \subseteq I,$$

was zu einem Widerspruch zur Minimalität von $\delta(d_0)$ führt.

Aus $r = 0$ folgt $t \in Rd_0$ und damit $I = Rd_0 \subseteq Rd_k$ also $Rd_i = Rd_k$ für alle $i \geq k$. Letzteres liefert

$$d_i = rd_k = rsd_i$$

also $rs = 1$ und damit $d_i \sim d_k$. □

Satz 2.3: *Jeder euklidische Ring ist faktoriell.*

Beweis: Es sei $s \neq 0$ eine Nichteinheit des euklidischen Rings (R, δ). Man zeigt, dass sich s als Produkt $q_1 \cdot \ldots \cdot q_n$ irreduzibler Elemente darstellen lässt. Wäre dem nicht so, so wäre s nicht irreduzibel und ließe sich daher als Produkt $s = d_1 q_1$ schreiben. Nach Voraussetzung über s lässt sich dann mindestens eines der Elemente d_1 und q_1 nicht als Produkt irreduzibler Elemente schreiben; ohne Einschränkung sei dies d_1. Derselbe Schluss angewandt auf d_1 führt zu einem Element d_2, das sich nicht als Produkt irreduzibler Elemente schreiben lässt. Insgesamt führt die Argumentation zu einer Folge $(d_i)_{i\in\mathbb{N}}$ mit der Eigenschaft d_{i+1} ist echter Teiler von d_i. Eine solche Folge kann nach Lemma 2.2 in einem euklidischen Ring nicht existieren.

Um die Aussage des Satzes zu beweisen genügt es nun zu zeigen, dass in einem euklidischen Ring jedes irreduzible Element ein Primelement ist. Es sei $p \in R$ irreduzibel und es gelte $p|(ab)$. Man nimmt weiter an, dass p kein Teiler von a ist. Man betrachtet die Teilmenge

$$J := \{ra + sp : r, s \in R\};$$

die Menge $\delta(J \setminus 0)$ besitzt ein minimales Element $\delta(t)$. Man kann p mit Rest durch t dividieren und erhält $p = qt + r$ mit $r = 0$ oder $\delta(r) < \delta(t)$. Ist $r \neq 0$, so gilt $r = p - qt \in J \setminus 0$ und es ergibt sich ein Widerspruch zur Minimalität von $\delta(t)$. Also ist $r = 0$ und damit $p = qt$.

Dasselbe Argument kann man mit a anstelle von p durchführen und erhält $a = q't$.

Da p keine echten Teiler besitzt und p kein Teiler von a ist, muss $t \in R^\times$ gelten. Man erhält also

$$1 = t^{-1}(r_1 a + s_1 p)$$

mit gewissen $r_1, s_1 \in R$. Multiplikation dieser Gleichung mit b liefert

$$b = t^{-1}(r_1 ab + s_1 bp);$$

da nach Voraussetzung $p|(ab)$ gilt, folgt $p|b$ und man hat gezeigt, dass p tatsächlich ein Primelement ist. □

Als wesentliche Folgerung aus dem letzten Satz halten wir fest:

KOROLLAR 2.4: *Der Polynomring $K[X]$ der Polynome in einer Unbestimmten mit Koeffizienten in einem Körper K ist faktoriell und seine Primelemente sind genau die irreduziblen Polynome.*

BEISPIEL 2.5: Wir betrachten den für die Kodierungstheorie wichtigen Körper $\mathbb{F}_2 = \{0, 1\}$. Die Polynome $f \in \mathbb{F}_2[X]$ besitzen die Gestalt

$$f = \sum_{i=1}^{m} X^{k_i}$$

mit $k_1 < \ldots < k_m$. Ist m gerade, so gilt $f(1) = 0$, womit f nicht irreduzibel ist. Weiter muss für jedes irreduzible Polynom $k_1 = 0$ gelten. Unter Zuhilfenahme dieser Informationen kann man die irreduziblen und damit Primpolynome geordnet nach ihrem Grad aufzählen:

- Grad 1: $X, X + 1$.
- Grad 2: $X^2 + X + 1$.
- Grad 3: Ein reduzibles Polynom dritten Grades muss ein Polynom vom Grad 1 als Teiler also eine Nullstelle besitzen. Die Kandidaten (gemäß obiger Beobachtutngen) irreduzibler Polynome sind

  $$X^3 + X^2 + 1, X^3 + X + 1.$$

  Da diese keine Nullstellen in $\mathbb{F}_2$ besitzen, sind sie irreduzibel.

- Grad 4: Als Kandidaten kommen in Frage:

$$X^4 + X^3 + X^2 + X + 1, X^4 + X + 1, X^4 + X^2 + 1, X^4 + X^3 + 1.$$

  Da diese keine Nullstellen besitzen, ist genau einer dieser Kandidaten reduzibel, nämlich derjenige, der durch das einzige quadratische irreduzible Polynom $X^2 + X + 1$ teilbar ist:

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1.$$

- Grad 5: Die reduziblen Polynome ohne Nullstellen lassen sich leicht als

$$\begin{aligned}(X^2 + X + 1)(X^3 + X^2 + 1) &= X^5 + X + 1\\ (X^2 + X + 1)(X^3 + X + 1) &= X^5 + X^4 + 1\end{aligned}$$

  angeben. Alle anderen der Kandidaten ohne Nullstellen sind damit irreduzibel.

$\diamond$

3 Polynome über faktoriellen Ringen

Die Diskussion nach Beispiel 1.7 zeigt, dass man im Polynomring $K[X_1, \ldots, X_n]$ in n Unbestimmten über einem Körper K jedes Element $f \notin K$ als Produkt von irreduziblen Elementen schreiben kann. Man verwendet dabei die totale Gradfunktion deg als Funktion δ. Leider gilt aber:

FESTSTELLUNG 3.1: *Der Polynomring $K[X_1, \ldots, X_n]$ in $n \geq 2$ Unbestimmten über einem Körper K ist kein euklidischer Ring.*

BEWEIS: Der Beweis wird nur für den Fall $n = 2$ gegeben, kann aber auf den Fall $n > 2$ verallgemeinert werden.

Man nimmt an $(K[X_1, X_2], \delta)$ sei ein euklidischer Ring und betrachtet die Menge

$$J := \{f \cdot X_1 + g \cdot X_2 : f, g \in K[X_1, X_2]\} \setminus 0.$$

Dann besitzt die Menge $\delta(J)$ ein minimales Element $\delta(h)$.

Division mit Rest liefert die Gleichung

$$X_1 = q_1 \cdot h + r.$$

Wäre $r \neq 0$, so hätte man einerseits $\delta(r) < \delta(h)$ und andererseits $r = X_1 - q \cdot h \in I$ – ein Widerspruch zur Minimalität von $\delta(h)$. Folglich gilt $X_1 = q_1 \cdot h$ und damit $\deg_{X_2}(q_1) + \deg_{X_2}(h) = 0$ und $\deg_{X_1}(q_1) + \deg_{X_1}(h) = 1$. Hieraus folgt $q_1 \in K \setminus 0$.

Ein analoges Argument mit X_2 anstelle von X_1 zeigt $X_2 = q_2 \cdot h$ mit $q_2 \in K \setminus 0$. Es folgt $X_2 = q_2 \cdot q_1^{-1} \cdot X_1$, ein Widerspruch. □

Wir können also den Satz 2.3 nicht verwenden um die durch Korollar 2.4 erweckte Hoffnung, dass die Polynomringe $K[X_1, \ldots, X_n]$ faktoriell sind, zu beweisen. Andererseits ist $K[X_1, X_2] = K[X_1][X_2]$ ein Polynomring in einer Unbestimmten über einem faktoriellen Ring. Diese Tatsache soll im Weiteren genutzt werden: Wir betrachten einen faktoriellen Ring R und den Ring $R[X]$ der Polynome in einer Unbestimmten mit Koeffizienten in R. Ist K der Quotientenkörper von R, dann gilt

$$R[X] \subseteq K[X].$$

Dies ist bemerkenswert, weil $K[X]$ ein faktorieller Ring ist.

Wir beginnen die Untersuchung der Situation mit der Frage, ob Primelemente von R auch Primelemente von $R[X]$ sind. Es ist also zu prüfen, ob aus $p|(fg)$ für Polynome $f, g \in R[X]$ eine der Relationen $p|f$ oder $p|g$ folgt.

LEMMA 3.2: *Es sei p ein Primelement des Integritätsbereichs $R[X]$. Gilt dann $p|(fg)$ für $f, g \in R[X]$, so folgt $p|f$ oder $p|g$.*

BEWEIS: Es seien $f = \sum_{i=0}^{m} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$ Polynome deren Koeffizienten *nicht* sämtlich durch p teilbar sind. Es seien k und ℓ die kleinsten Indizes, für die der Koeffizient a_k von f und b_ℓ von g nicht durch p teilbar ist. Für den Koeffizienten $c_{k+\ell}$ von fg gilt dann:

$$c_{k+\ell} = a_0 b_{k+\ell} + \ldots + a_{k-1} b_{\ell+1} + a_k b_\ell + a_{k+1} b_{\ell-1} + \ldots + a_{k+\ell} b_0.$$

In dieser Summe sind nach Definition der Indizes k und ℓ alle Summanden außer $a_k b_\ell$ durch p teilbar. Folglich ist $c_{k+\ell}$ nicht durch p teilbar, womit p kein Teiler von fg ist. □

Aufgrund des gerade bewiesenen Lemmas wissen wir nun, dass alle Primelemente von R auch Primelemente von $R[X]$ sind und müssen jetzt die Primelemente $f \in R[X] \setminus R$ ermitteln. Ein solches muss irreduzibel sein, insbesondere darf es kein Primelement $p \in R$ geben, das alle Koeffizienten von f teilt. Dies motiviert die im Folgenden eingeführten Begriffe.

DEFINITION 3.3: *Ein gemeinsamer Teiler der Elemente $r_1, \ldots, r_m$ eines Integritätsbereichs R ist ein Element $d \in R$ mit der Eigenschaften:*

$$\forall i \in \{1, \ldots, m\} \quad d | r_i.$$

Ein größter gemeinsamer Teiler der Elemente $r_1, \ldots, r_m$ ist ein gemeinsamer Teiler d dieser Elemente mit der zusätzlichen Eigenschaft: Ist d' ein beliebiger gemeinsamer Teiler dieser Elemente, so gilt $d'|d$.

BEMERKUNGEN:

1. Aus der Definition folgt unmittelbar, dass zwei größte gemeinsame Teiler der Elemente $r_1, \ldots, r_m$ stets zueinander assoziiert sind. Obwohl es also verschiedene größte gemeinsame Teiler gibt, ist die Verwendung des Symbols $\mathrm{ggT}(r_1, \ldots, r_m)$ sinnvoll, da nur die Teilbarkeitseigenschaft des Elements wichtig ist.

2. In einem faktoriellen Ring R lässt sich der größte gemeinsame Teiler von Elementen aus deren Primfaktorisierungen ermitteln. Im Folgenden wird dies für den Fall zweier Elemente r_1, r_2 erläutert: Es sei $P \subset R$ eine repräsentative Menge von Primelementen von R und $p_1, \ldots, p_m \in P$ seien diejenigen Primelemente, die in den Primfaktorisierungen *beider* Elemente vorkommen. Sind dann $e_1, \ldots, e_m$ und $f_1, \ldots, f_m$ die Exponenten, mit denen diese Primelemente in der jeweiligen Faktorisierung vorkommen, so gilt

   $$\mathrm{ggT}(r_1, r_2) = \prod_{i=1}^{m} p_i^{\min(e_i, f_i)}.$$

   Besitzen r_1 und r_2 keine gemeinsamen Primfaktoren, so ist nach Definition $\mathrm{ggT}(r_1, r_2) = 1$.

DEFINITION 3.4: *Für ein Polynom*

$$f = a_d X^d + \ldots + a_0 \in R[X] \setminus 0$$

bezeichnet man das bis auf Assoziierte eindeutig bestimmte Element

$$I(f) := \mathrm{ggT}(a_n, \ldots, a_0)$$

als Inhalt von f.

Ein Polynom $f \in R[X] \setminus 0$ mit der Eigenschaft $I(f) \in R^\times$ wird als primitives Polynom bezeichnet.

Der Inhalt von Polynomen über faktoriellen Ringen ist eine multiplikative Größe:

SATZ 3.5: *Sei R ein faktorieller Ring. Für Polynome $f, g \in R[X] \setminus 0$ gilt dann $I(fg) = I(f)I(g)$. Insbesondere ist das Produkt primitiver Polynome ein primitives Polynom.*

BEWEIS: Nach Definition des Inhalts gilt für jedes Polynom $h \in R[X] \setminus 0$

$$h = I(h)\tilde{h},$$

wobei das Polynom $\tilde{h}$ primitiv ist. Folglich ist einerseits

$$fg = I(f)I(g)\tilde{f}\tilde{g}$$

und andererseits

$$fg = I(fg)\widetilde{fg}.$$

Kann man zeigen, dass $\tilde{f}\tilde{g}$ primitiv ist, so folgt die Behauptung.

Wäre $\tilde{f}\tilde{g}$ nicht primitiv, so gäbe es ein Primelement $p \in R$ mit der Eigenschaft $p|(\tilde{f}\tilde{g})$. Lemma 3.2 liefert dann $p|\tilde{f}$ oder $p|\tilde{g}$ im Widerspruch zur Primitivität dieser Polynome. □

Wir bringen nun den Quotientenkörper K von R ins Spiel: Da R ein Teilring von K ist, ist auch $R[X]$ ein Teilring von $K[X]$. Es bietet sich daher an ein Polynom $f \in R[X]$ im euklidischen Ring $K[X]$ zu faktorisieren um Rückschlüsse auf eine Faktorisierung in $R[X]$ zu ziehen.

SATZ 3.6: *Es sei $f \in R[X]$ primitiv und $f = gh$ eine Zerlegung von f in nicht konstante Polynome in $K[X]$. Dann gibt es Elemente $c_g, c_h \in K$ mit den Eigenschaften*

- *$c_g g$ und $c_h h$ sind primitive Polynome in $R[X]$,*
- *$f = (c_g g)(c_h h)$.*

Insbesondere bleibt jedes irreduzible Polynom $f \in R[X] \setminus R$ in $K[X]$ irreduzibel.

BEWEIS: Es seien $r_g, r_h \in R$ die Hauptnenner der Koeffizienten der Polynome g und h. Dann gilt $r_g g, r_h h \in R[X]$ und man erhält die Gleichung

$$r_g r_h f = I(r_g g)I(r_h h)\widetilde{r_g g}\widetilde{r_h h}$$

mit den primitiven Polynomen $\widetilde{r_g g}$ und $\widetilde{r_h h}$. Da f primitiv ist, folgt aus Satz 3.5

$$r_g r_h \sim I(r_g g) I(r_h h),$$

womit die Behauptung des Satzes für die Elemente $c_g := \frac{I(r_g g)}{r_g}$ und $c_h := \frac{I(r_h h)}{r_h}$ bewiesen ist. □

SATZ 3.7 (C.F. Gauß): *Der Polynomring $R[X]$ über einem faktoriellen Ring R ist selbst faktoriell. Die Primelemente von $R[X]$ sind:*

- *die Primelemente von R,*
- *die primitiven Polynome $f \in R[X]$, die in $K[X]$ irreduzibel sind.*

BEWEIS: Wir zeigen zunächst, dass jedes primitive irreduzible Polynom $q \in R[X]$ ein Primelement ist: Gilt $q|(fg)$ für Polynome $f, g \in R[X]$, so gilt diese Teilbarkeitsrelation auch in $K[X]$. Nach Satz 3.6 ist q in $K[X]$ irreduzibel also ein Primelement, da $K[X]$ faktoriell ist. Ohne Einschränkung der Allgemeinheit gilt also $q|f$ in $K[X]$, woraus sich

$$rf = qh$$

für $r \in R$ und primitives $h \in R[X]$ ergibt. Nach Satz 3.5 ist dann $r \in R^\times$, was die Behauptung beweist.

Sei nun $f \in R[X]$ ein beliebiges Element. Ist $f \in R$, so besitzt f nach Voraussetzung eine Primfaktorisierung in R und diese ist auch eine Primfaktorisierung in $R[X]$. Man kann also $\deg(f) > 0$ und wegen $f = I(f)\tilde{f}$ auch die Primitivität von f annehmen. Nach Satz 3.6 liefert die Primfaktorisierung

$$f = \prod_{i=1}^{m} p_i^{e_i}$$

von f in $K[X]$ eine Faktorisierung

$$f = \prod_{i=1}^{m} (c_i p_i)^{e_i},$$

mit $c_i \in K$ derart, dass die Polynome $c_i p_i$ primitiv sind. Nach Satz 3.6 sind diese Polynome irreduzibel und damit nach dem bereits Bewiesenen Primelemente. □

KOROLLAR 3.8: *Die Polynomringe* $\mathbb{Z}[X_1, \ldots, X_n]$ *und* $K[X_1, \ldots, X_n]$, K *ein Körper, sind für alle* $n \in \mathbb{N}$ *faktoriell.*

BEWEIS: Die Ringe $\mathbb{Z}$ und $K[X]$ sind euklidisch also faktoriell. Die Rekursionsgleichungen

$$\mathbb{Z}[X_1, \ldots, X_n] = \mathbb{Z}[X_1, \ldots, X_{n-1}][X_n],\ K[X_1, \ldots, X_n] = K[X_1, \ldots, X_{n-1}][X_n]$$

liefern in Kombination mit Satz 3.7 die Behauptung. □

BEMERKUNG: Man beachte, dass im Fall des Rings $K[X_1, \ldots, X_n]$ die Zerlegung eines Polynoms in irreduzible Faktoren identisch ist mit der Primfaktorzerlegung.

4 Homogene Polynome

In diesem Abschnitt werden spezielle Polynome $f \in K[X_1, \ldots, X_n]$ in einem Polynomring in $n \geq 2$ Unbestimmten mit Koeffizienten in einem Körper K betrachtet: Es ist naheliegend die in einem Polynom f vorkommenden Monome nach ihrem totalen Grad zusammenzufassen. So würde man etwa die Monome des Polynoms

$$f = X_1^3 - X_1X_2 + X_2^5 - X_1^2X_2 - X_1^2X_2^3 + X_2^2$$

wie folgt ordnen

$$f = (X_2^2 - X_1X_2) + (X_1^3 - X_1^2X_2) + (X_2^5 - X_1^2X_2^3),$$

wobei die Reihenfolge des Auftretens der Monome gleichen Grades in der Summe beliebig ist. Die in Klammern stehenden Summanden besitzen die Eigenschaft, dass alle ihre Monome denselben totalen Grad haben.

Im Allgemeinen gilt: *Jedes* $f \in K[X_1, \ldots, X_n]$ *lässt sich in der Form*

$$f = \sum_{i=0}^{d} f_i \tag{9}$$

darstellen, wobei die im Polynom f_i *vorkommenden Monome den totalen Grad* i *besitzen.*

DEFINITION 4.1: *Die in der Darstellung (9) auftretenden Polynome f_i nennt man die homogenen Komponenten des Polynoms f.*

Ein Polynom $f \in K[X_1, \ldots, X_n] \setminus 0$ heißt homogen (vom Grad d), wenn es genau eine homogene Komponente besitzt (und diese den Grad d hat).

Das Nullpolynom ist per Definition homogen von jedem Grad d.

Die grundlegenden algebraischen Eigenschaften homogener Polynome sind im Folgenden zusammengefasst:

FESTSTELLUNG 4.2: *Für jedes $d \in \mathbb{N}_0$ bezeichne $K[X_1, \ldots, X_n]_d$ die Menge der homogenen Polynome vom Grad d.*

1. *$K[X_1, \ldots, X_n]_d$ bildet zusammen mit der Polynomaddition und der Multiplikation mit Elementen aus K einen Vektorraum. Die Menge der Monome vom Grad d bildet eine Basis dieses Vektorraums; die Anzahl solcher Monome ist $\binom{n+d-1}{d}$.*

2. *Für alle $d, d' \in \mathbb{N}_0$ gilt*

$$K[X_1, \ldots, X_n]_d \cdot K[X_1, \ldots, X_n]_{d'} = K[X_1, \ldots, X_n]_{d+d'}.$$

BEWEIS: Der Beweis der Feststellung ist bis auf die Aussage über die Anzahl verschiedener Monome vom Grad d Routine.

Die Monomanzahl lässt sich ermitteln, indem man ein Monom vom Grad d in n Unbestimmten als Folge von zwei Symbolen wie etwa $*$ und $|$ angibt, wobei in der Folge d Symbole $*$ und $n-1$ Symbole $|$ auftreten müssen. Dabei steht das Symbol $*$ für einen Faktor X_i, wobei der Index i durch die Anzahl der Symbole $|$ links des betrachteten Symbols $*$ bestimmt ist. Ein Beispiel macht klar, wie dies gemeint ist: Die Folge $(***\,|\,**\,||)$ steht für ein Monom vom Grad 5 in 4 Unbestimmten und zwar für $X_1^3 X_2^2 X_3^0 X_4^0$.

Die beschriebenen Folgen stehen in Bijektion mit den Monomen. Eine Folge ist durch die Positionen der Symbole $|$ eindeutig festgelegt. Für die Wahl dieser Positionen gibt es $\binom{n+d-1}{n-1} = \binom{n+d-1}{d}$ Möglichkeiten $\square$

Homogene Polynome besitzen die folgende im Hinblick auf ihre Verwendung in der algebraischen Geometrie zentrale Eigenschaft: Für jedes $f \in K[X_1, \ldots, X_n]_d$ gilt

$$\forall (a_1, \ldots, a_n) \in K^n, \lambda \in K \quad f(\lambda a_1, \ldots, \lambda a_n) = \lambda^d f(a_1, \ldots, a_n). \tag{10}$$

Offenbar genügt es diese Eigenschaft für Monome zu zeigen. Hier gilt für ein Monom $f = \prod_{k=1}^{n} X_k^{i_k}$ vom Grad $d = \sum_{k=1}^{n} i_k$:

$$f(\lambda a_1, \ldots, \lambda a_n) = \prod_{i=1}^{n} (\lambda a_k)^{i_k} = \prod_{i=1}^{n} \lambda^{i_k} \prod_{i=1}^{n} a_k^{i_k} = \lambda^d f(a_1, \ldots, a_n).$$

Diese Abbildungseigenschaft homogener Polynome lässt sich allerdings nicht zu ihrer Definition verwenden. So hat zum Beispiel *jedes* Polynom $f \in \mathbb{F}_2[X_1, \ldots, X_n]$, dessen konstanter Koeffizient gleich 0 ist, diese Eigenschaft. Man kann jedoch eine Variante des gerade Diskutierten zur Charakterisierung homogener Polynome nutzen: Hierzu sei Y eine von $X_1, \ldots, X_n$ unabhängige Unbestimmte. Man betrachtet dann den Polynomring $K[X_1, \ldots, X_n, Y]$, welcher $K[X_1, \ldots, X_n]$ als Unterring enthält. In dieser Situation gilt:

FESTSTELLUNG 4.3: *Ein Polynom $f \in K[X_1, \ldots, X_n]$ ist genau dann homogen, wenn eine Gleichung der Gestalt*

$$f(YX_1, \ldots, YX_n) = Y^d f(X_1, \ldots, X_n)$$

für ein $d \in \mathbb{N}_0$ besteht.

BEWEIS: Die Implikation $\Rightarrow$ beweist man genauso wie die Eigenschaft (10).

Sei also nun $f \in K[X_1, ..., X_n]$ ein Polynom mit der in der Feststellung genannten Eigenschaft und sei $f = f_0 + \ldots + f_d$ seine Zerlegung in homogene Komponenten. Dann folgt durch Einsetzen die Polynomidentität

$$f_0 + Y f_1 + \ldots + Y^d f_d = Y^d f$$

im Ring $K[X_1, \ldots, X_n, Y] = K[X_1, \ldots, X_n][Y]$. Es muss also $f = f_d$ gelten, was die Behauptung beweist. □

SATZ 4.4: *Jeder Teiler eines homogenen Polynoms f ist homogen. Insbesondere sind alle in der Primfaktorzerlegung von f auftretenden Polynome homogen.*

BEWEIS: Es gelte $f = gh$ und $g = g_0 + ldots + g_m$, $h = h_0 + ldots + h_n$ seien die Zerlegungen der Faktoren in homogene Komponenten. Dann folgt aus Feststellung 4.3 die Polynomidentität

$$Y^d f(X_1, \ldots, Y_n) = (g_0 + Y g_1 + \ldots + Y^m g_m)(h_0 + Y h_1 + \ldots + Y^n h_n)$$

im Ring $K[X_1, \ldots, X_n, Y]$, wobei $d = n + m$ gilt. Es folgt $f = g_m h_n$ und

$$0 = \sum_{i+j=k} g_i h_j$$

für alle $k < d$. Seien i_0 und j_0 die jeweils kleinsten Indizes mit $g_{i_0} \neq 0$ und $h_{j_0} \neq 0$. Dann folgt insbesondere

$$0 = g_{i_0} h_{j_0},$$

ein Widerspruch, da der Polynomring $K[X_1, \ldots, X_n]$ nullteilerfrei ist. □

5 Affine algebraische Hyperflächen

Einleitung

Das Bestreben das Lösungsverhalten linearer Gleichungssysteme

$$\begin{array}{rcl} a_{11}X_1 + \ldots + a_{1n}X_n & = & b_1 \\ a_{21}X_1 + \ldots + a_{2n}X_n & = & b_2 \\ \vdots & = & \vdots \\ a_{m1}X_1 + \ldots + a_{mn}X_n & = & b_m \end{array} \tag{11}$$

mit reellen Koeffizienten und rechten Seiten zu verstehen, hat historisch zur Entwicklung der *linearen Algebra* geführt. Die Lösungsmengen solcher Gleichungssysteme sind affine Unterräume des affinen Raums $\mathbb{R}^n$ und besitzen daher eine geometrische Interpretation als Punkte, Geraden, Ebenen usw. in diesem Raum, was wiederum zur so genannten *analytischen Geometrie* führt. Zur Bestimmung dieser Lösungsmengen kann der Gauß-Algorithmus verwendet werden. Die theoretischen Aussagen zum Lösungsverhalten ändern sich nicht, wenn man anstelle von $\mathbb{R}$ einen beliebigen Körper K betrachtet. Auch der Gauß-Algorithmus kann in den so entstehenden allgemeineren Situationen prinzipiell zur Lösung verwendet werden, wobei natürlich die konkrete Implementierung des Algorithmus' stark von K abhängt.

Eine direkte Verallgemeinerung linearer Gleichungssysteme sind polynomiale Gleichungssysteme

$$\begin{array}{rcl} f_1(X_1, \ldots, X_n) & = & 0 \\ f_2(X_1, \ldots, X_n) & = & 0 \\ \vdots & = & \vdots \\ f_m(X_1, \ldots, X_n) & = & 0 \end{array} \tag{12}$$

mit $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. Auch in diesen Gleichungssystemen treten nur die »Grundrechenarten« auf. Besitzen alle Polynome f_i den Grad 1, so erhält man ein lineares Gleichungssystem. Die Lösungsmengen $A \subseteq K^n$ polynomialer Gleichungssysteme bezeichnet man als *algebraische Teilmengen* des affinen Raums K^n über K. Im Fall $K = \mathbb{R}$ besitzen diese wiederum eine geometrische Interpretation als Punkte, Kurven, Flächen etc. einer bestimmten Art. Der Versuch einer systematischen Untersuchung und Klassifikation algebraischer Teilmengen hat zur *algebraischen Geometrie* geführt. Im Unterschied zu linearen Gleichungssystemen gibt es für Polynomgleichungssysteme kein einfach überprüfbares Kriterium für die Lösbarkeit des Systems. Auch ein allgemeiner Algorithmus zur Angabe der Lösung in parametrisierter Form existiert nicht. Tatsächlich kann man beweisen, dass die Lösungsmengen von Polynomgleichungssystemen häufig überhaupt nicht parametrisierbar sind.

Definition

Im Folgenden sollen Polynomgleichungen

$$f(X_1, \ldots, X_n) = 0 \tag{13}$$

mit $f \in K[X_1, \ldots, X_n]$ für $n \geq 2$ betrachtet werden. Deren Lösungsmengen können sich auch im Fall $K = \mathbb{R}$ entgegen der Intuition verhalten, wie die beiden folgenden Beispiele zeigen:

$$X_1^2 + \ldots + X_n^2 = -1 \quad \text{und} \quad X_1^2 + \ldots + X_n^2 = 0.$$

Man erwartet, dass die Einschränkungen durch eine Gleichung im n-dimensionalen Raum zu einer $n-1$-dimensionalen Lösungsmenge führt, wobei Letzteres noch genau zu definieren ist. Tatsächlich besitzt die erste der beiden obigen Gleichungen keine Lösungen und die zweite ist nur im Punkt $(0, \ldots, 0)$ erfüllt. Um solche »Pathologien« zu vermeiden, arbeitet man in der algebraischen Geometrie mit algebraisch abgeschlossenen Körpern:

Definition 5.1: *Eine über dem Körper K definierte, affine algebraische Hyperfläche ist eine Teilmenge $H \subset \tilde{K}^n$ der Gestalt*

$$H = \{(\alpha_1, \ldots, \alpha_n) \in \tilde{K}^n : f(\alpha_1, \ldots, \alpha_n) = 0\},$$

wobei $\tilde{K}$ den algebraischen Abschluss von K bezeichnet und $f \in K[X_1, \ldots, X_n] \setminus K$ gilt. Man nennt f dann auch ein H definierendes Polynom.

Ist $L \subseteq \tilde{K}$ ein Erweiterungskörper von K, so nennt man die Elemente der Menge

$$H_L := H \cap L^n$$

die L-rationalen Punkte von H.

Bemerkungen:

1. In der algebraischen Geometrie wird das Symbol $Z(f)$ für die durch f definierte Hyperfläche benutzt, was im Folgendem in der Regel ebenfalls getan wird. Der Buchstabe Z steht für »zero set«. Man beachte, dass $Z(f) = Z(g)$ für $f \neq g$ gelten kann. Ein einfaches Beispiel ist durch $g = f^r$ für beliebiges $r \in \mathbb{N}$ gegeben.

2. Im Fall $n = 2$ bezeichnet man die Mengen $Z(f)$ als ebene affine algebraische Kurven. Die durch diese Bezeichnung implizierte Vorstellung von »Eindimensionalität« ist noch zu thematisieren.

3. Im Fall $n = 3$ bezeichnet man die Mengen $Z(f)$ als affine algebraische Flächen. Auch hier ist die Bezugnahme auf die Dimension 2 noch zu begründen.

4. Bezeichnungskonvention: Da im Weiteren keine anderen als affine algebraische Hyperflächen betrachtet werden, werden diese knapp als K-Hyperflächen bzw. ebene K-Kurven bzw. K-Flächen bezeichnet, wobei K der Körper ist über dem sie definiert sind.

5. Im Fall $K = \mathbb{R}$ zahlt man für den Übergang zu $\tilde{\mathbb{R}} = \mathbb{C}$ mit dem Verlust unmittelbarer geometrischer Interpretierbarkeit als Preis. So ist etwa die »komplexe Ebene« $\mathbb{C}^2$ ein 4-dimensionaler reeller Vektorraum wie die folgende bijektive, $\mathbb{R}$-lineare Abbildung zeigt:

$$\phi : \mathbb{C}^2 \to \mathbb{R}^4,\ (u_1 + iu_2, v_1 + iv_2) \mapsto (u_1, v_1, u_2, v_2). \tag{14}$$

Wir halten zunächst fest, dass der Übergang zum algebraischen Abschluss tatsächlich die oben angeführte Pathologie fehlender Lösungen behebt:

Feststellung 5.2: *Eine K-Hyperfläche besitzt unendlich viele Punkte.*

BEWEIS: Die Hyperfläche H werde durch $f \in K[X_1, \ldots, X_n] \setminus K$ definiert. Mindestens eine der Unbestimmten kommt in den Monomen von f vor, sagen wir X_n. Da algebraisch abgeschlossene Körper unendlich viele Elemente besitzen, gibt es unendlich viele Tupel $(\alpha_1, \ldots, \alpha_{n-1}) \in \tilde{K}^{n-1}$. Nach Definition eines algebraisch abgeschlossenen Körpers besitzen die Polynome $f(\alpha_1, \ldots, \alpha_{n-1}, X_n) \in \tilde{K}[X_n]$ eine Nullstelle $\alpha_n \in \tilde{K}$, womit die Behauptung bewiesen ist. □

BEISPIEL 5.3: Die ebene $\mathbb{R}$-Kurve

$$Z(X_1^2 + X_2^2 + 1) := \{(\alpha_1, \alpha_2) \in \mathbb{C}^2 : \alpha_1^2 + \alpha_2^2 = -1\}$$

besitzt, wie bereits festgestellt, keine $\mathbb{R}$-rationalen Punkte. Die Faktorisierung

$$X_1^2 + X_2^2 = (X_1 - iX_2)(X_1 + iX_2)$$

ermöglicht es immerhin eine komplexe Parametrisierung von $Z(X_1^2 + X_2^2 + 1)$ anzugeben: Für einen Punkt $(\alpha_1, \alpha_2) \in Z(X_1^2 + X_2^2 + 1)$ setzt man $\lambda := \alpha_1 + i\alpha_2$. Dann gilt $\alpha_1 - i\alpha_2 = -\frac{1}{\lambda}$. Dies liefert nach einfacher Rechnung

$$Z(X_1^2 + X_2^2 + 1) = \{(\frac{\lambda^2 - 1}{2\lambda}, \frac{\lambda^2 + 1}{2i\lambda}) : \lambda \in \mathbb{C}^*\}.$$

Man erkennt direkt, dass $Z(X_1^2 + X_2^2 + 1)$ überabzählbar unendlich viele Punkte enthält. ◇

BEISPIEL 5.4: Für die ebene $\mathbb{R}$-Kurve

$$Z(X_1^2 + X_2^2) = \{(\alpha_1, \alpha_2) \in \mathbb{C}^2 : \alpha_1^2 + \alpha_2^2 = 0\}$$

gilt

$$Z(X_1^2 + X_2^2)_{\mathbb{R}} = \{(0, 0)\}$$

und die Faktorisierung

$$0 = X_1^2 + X_2^2 = (X_1 - iX_2)(X_1 + iX_2)$$

zeigt

$$Z(X_1^2 + X_2^2) = \{\lambda(i, 1) : \lambda \in \mathbb{C}\} \cup \{\lambda(-i, 1) : \lambda \in \mathbb{C}\},$$

das heißt $Z(X_1^2+X_2^2)$ ist die Vereinigungsmenge zweier komplexer Untervektorräume der Dimension 1 (»komplexe Ursprungsgeraden«) der komplexen Ebene $\mathbb{C}^2$. Die beiden Unterräume schneiden sich nur im Ursprung. Nutzt man die $\mathbb{R}$-lineare Abbildung ϕ (14), so ergibt sich mit $\lambda = a + bi$:

$$\phi(\{\lambda(i,1) : \lambda \in \mathbb{C}\}) = \{(-b,a,a,b) : a,b \in \mathbb{R}\}.$$

Wie erwartet ist das Bild einer komplexen Ursprungsgeraden, also eines komplex 1-dimensionalen und damit reell 2-dimensionalen Vektorraums, eine Ebene im reellen 4-dimensionalen Raum $\mathbb{R}^4$. $\diamond$

Beispiel 5.5: Die $\mathbb{R}$-rationalen Punkte der ebenen $\mathbb{R}$-Kurve $Z(X_1^2 + X_2^2 - 1) \subset \mathbb{C}^2$ bilden bekanntlich den Einheitskreis

$$S^1 := \{(\alpha_1, \alpha_2) \in \mathbb{R}^2 : \alpha_1^2 + \alpha_2^2 = 1\}).$$

Es ist in diesem Fall besonders interessant sich ein Bild von $Z(X_1^2 + X_2^2 - 1)$ zu machen. Die Zerlegung in Real- und Imaginärteil $\alpha_1 = u_1 + iu_2$ und $\alpha_2 = v_1 + iv_2$ liefert für einen Punkt $(\alpha_1, \alpha_2) \in Z(X_1^2+X_2^2-1)$ die Gleichungen

$$\begin{aligned} u_1^2 + v_1^2 - (u_2^2 + v_2^2) &= 1 \\ u_1u_2 + v_1v_2 &= 0 \end{aligned}$$

für das Bild $\phi(Z(X_1^2 + X_2^2 - 1)) \subset \mathbb{R}^4$. Um einen möglichst großen Teil dieser Menge visualisieren zu können, betrachtet man diejenigen Punkte (u_1, v_1, u_2, v_2) mit $v_1 \neq 0$. Dann gilt $v_2 = -\frac{u_1u_2}{v_1}$ und es ergibt sich die definierende Gleichung

$$v_1^4 + (u_1^2 - u_2^2 - 1)v_1^2 - u_1^2u_2^2 = 0$$

für die Menge

$$\phi(Z(X_1^2 + X_2^2 - 1)) \setminus \{(u_1, 0, 0, v_2) : u_1^2 - v_2^2 = 1\}.$$

Die Abbildung 1 zeigt drei Sichten auf diese Menge: Die u_1-Achse des verwendeten Koordinatensystems liegt längs des »Knicks« in der Fläche, die v_1-Achse ist wechselnd orange-farben und blau und die u_2-Achse blau dargestellt. (Diese Darstellungsform ist der Tatsache geschuldet, dass in der verwendeten Software *Surfer* die Darstellung von Koordinatensystemen nicht vorgesehen ist.) In der rechten Grafik ist deutlich der Einheitskreis S^1 in der (u_1, v_1)-Ebene zu sehen. $\diamond$

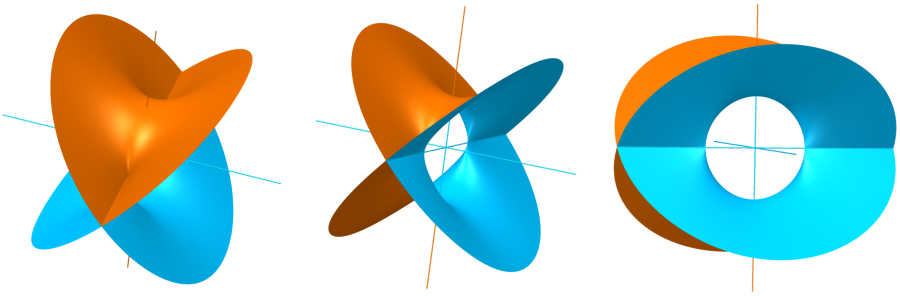


Abbildung 1: Partielle 3-dimensionale Darstellung von $Z(X_1^2 + X_2^2 - 1)$

BEISPIEL 5.6: Das Polynom $X_2^2 - X_1^3 + X_1$ kann man als Element des Polynomrings $K[X_1, X_2]$ über einem beliebigen Körper K interpretieren, da alle von 0 verschiedenen Koeffizienten 1 oder -1 also in jedem Körper existierende Elemente sind. Es handelt sich um ein Beispiel einer sogenannten *elliptischen Kurve*. Diese Kurvenklasse spielt in den aktuell verwendeten Verfahren der Kryptographie eine zentrale Rolle.

$K = \mathbb{F}_7$: Die Menge $Z(X_2^2 - X_1^3 + X_1)_{\mathbb{F}_7}$ der $\mathbb{F}_7$-rationalen Punkte lässt sich vollständig angeben. Ist nämlich $(a_1, a_2) \in \mathbb{F}_7^2$ ein solcher Punkt, so muss die Gleichung

$$a_2^2 = a_1^3 - a_1$$

gelten, das heißt das Element $a_1^3 - a_1 \in \mathbb{F}_3$ muss ein Quadrat in diesem Körper sein. Man tabelliert daher die Werte a^2 und $a^3 - a$ für alle Körperelemente:

a	a^2	a^3	$a^3 - a$
0	0	0	0
1	1	1	0
2	4	1	6
3	2	6	3
4	2	1	4
5	4	6	1
6	1	6	0

Man erhält:

$$Z(X_2^2 - X_1^3 + X_1)_{\mathbb{F}_7} = \{(0,0), (1,0), (6,0), (4,2), (4,5), (5,1), (5,6)\}.$$

$K = \mathbb{R}$: Um sich einen Überblick über die $\mathbb{R}$-rationalen Punkte $Z(X_2^2 - X_1^3 + X_1)_{\mathbb{R}}$ zu verschaffen schreibt man a_2 als Funktion von a_1. Wegen der Zweideutigkeit der Quadratwurzel sind allerdings auch zwei Funktionen notwendig:

$$a_2 = \pm\sqrt{a_1^3 - a_1}.$$

Aus diesen Gleichungen ergibt sich leicht, das in Abbildung 2 dargestellte Bild: Der Graph der Funktion $g(a_1) = a_1^3 - a_1$ ist als durchbrochene Linie zusätzlich dargestellt. ◇

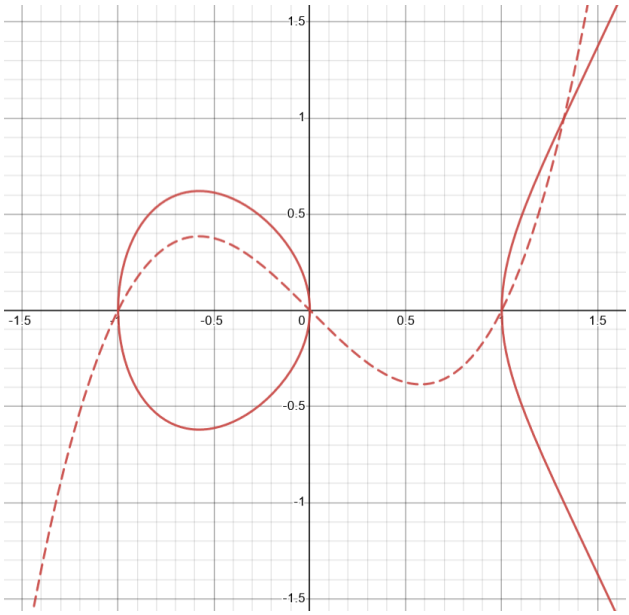


Abbildung 2: $Z(X_2^2 - X_1^3 + X_1)_{\mathbb{R}}$
(rot durchgezogen)

Beispiel 5.7: Die Abbildung 3 zeigt links die Menge

$$Z(X_1^2 + X_2^2 + X_3^4 - X_3^2)_{\mathbb{R}}.$$

Die vorliegende Gestalt kann man auf ähnliche Weise aus der Gleichung ableiten wie im Beispiel 5.6: Man betrachtet zunächst die Funktion $g(a_3) := a_3^2 - a_3^4$

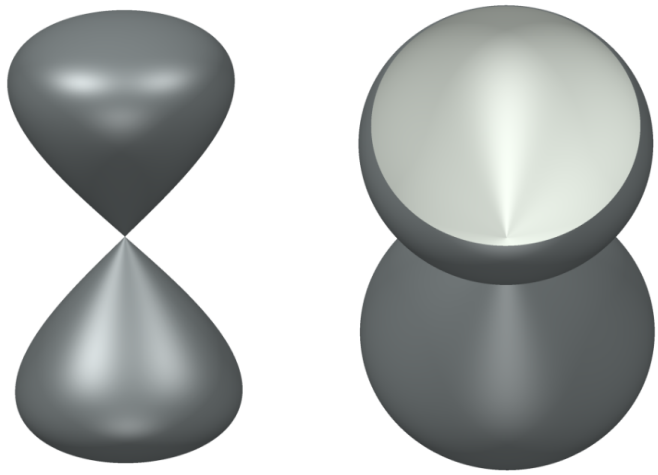


Abbildung 3: »Sanduhr«: $Z(X_1^2 + X_2^2 + X_3^4 - X_3^2)_{\mathbb{R}}$

– ihr Graph ist in Abbildung 4 dargestellt. Da die Größe $a_1^2 + a_2^2$ für einen Punkt $(a_1, a_2, a_3) \in \mathbb{R}^3$ der quadrierte euklidische Abstand von der dritten Koordinatenachse ist, ergibt sich die vorliegende Gestalt nun aus der Gleichung.

Die Menge $Z(X_1^2 + X_2^2 + X_3^4 - X_3^2)_{\mathbb{R}}$ ist »flächenhaft«, das heißt die Punkte im Inneren der sichtbaren »Sanduhr« gehören nicht zur Menge. Die Abbildung 3 rechts zeigt einen Blick ins Innere bei abgeschnittener oberer »Kappe«. ◇

Die Lösungsmengen linearer Gleichhungssysteme mit n Unbestimmten über einem Körper K sind genau die affinen Unterräume des K^n. Es ist naheliegend zu fragen, wodurch affine algebraische Hyperflächen $H \subseteq \tilde{K}^n$ ausgezeichnet sind. Das folgende Ergebnis liefert ein Ausschlusskriterium:

Satz 5.8: *Es sei $H \subseteq \tilde{K}^n$ eine K-Hyperfläche und $G \subset \tilde{K}^n$ eine Gerade. Dann gilt entweder $G \subseteq H$ oder $G \cap H$ ist endlich.*

Bemerkung: Wie der folgende Beweis zeigt, sind die Bedingungen »$G \subseteq H$ oder $G \cap H$ ist endlich« im obigen Satz exklusiv. Der Satz gilt auch für die L-rationalen Punkte H_L und Geraden im affinen Raum L^n für beliebige Erweiterungskörper L von K. Die obige Exklusivität folgt aber nur für unendliche Körper L.

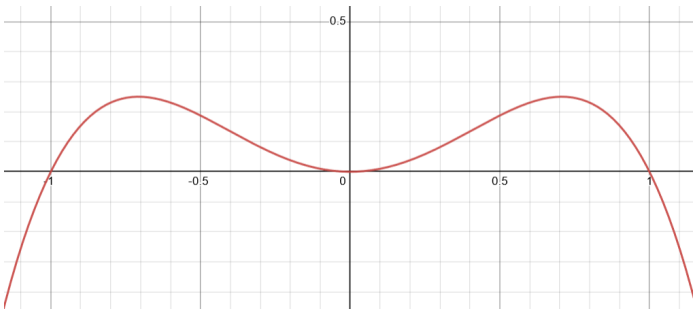


Abbildung 4: Graph von $g(a_3) := a_3^2 - a_3^4$

BEWEIS: Es gelte $H = Z(f)$ für ein $f \in K[X_1, \ldots, X_n]$ und $G = \tilde{K}v$ für ein $v := (v_1, \ldots, v_n)^t \neq 0$. Dann gilt die Gleichung

$$H \cap G = \{t \in \tilde{K} : f(tv_1, \ldots, tv_n) = 0\}.$$

Das Polynom $f(Tv_1, \ldots, Tv_n) \in \tilde{K}[T]$ ist entweder das Nullpolynom oder es besitzt endlich viele Nullstellen in $\tilde{K}$. Dies beweist die Behauptung. □

Der Satz liefert eines der folgenden Ausschlusskriterien:

SATZ 5.9: *Es sei $A \subset \mathbb{R}^n$ eine Menge mit mindestens einer der folgenden Eigenschaften:*

1. *A ist nicht abgeschlossen (bezüglich der durch die euklidische Norm gelieferten Topologie).*

2. *A ist beschränkt und enthält eine konvexe Teilmenge mit mehr als einem Element.*

Dann gibt es keine $\mathbb{R}$-Hyperfläche $H \subseteq \mathbb{C}^n$ mit der Eigenschaft $H_{\mathbb{R}} = A$.

BEWEIS: Gilt $H = Z(f)$ mit einem Polynom $f \in \mathbb{R}[X_1, \ldots, X_n]$, so hat man

$$H_{\mathbb{R}} = F^{-1}(0)$$

für die durch f induzierte Abbildung $F : \mathbb{R}^n \to \mathbb{R}$. Diese ist stetig, weshalb $F^{-1}(0)$ abgeschlossen ist.

Ist $B \subseteq A$ konvex und sind b_1, b_2 verschiedene Punkte von B, so liegt die Verbindungsstrecke dieser beiden Punkte in B also in A. Die durch diese Strecke festgelegte Gerade kann aber nicht Teilmenge von A sein. □

Irreduzible Komponenten von Hyperflächen

Ist $H = Z(f)$ eine durch ein Polynom $f \in K[X_1, \ldots, X_n]$ definierte K-Hyperfläche und ist

$$f = c \prod_{i=1}^{r} p_i^{e_i},\ c \in K^* \tag{15}$$

die Primfaktorisierung von f, so gilt offensichtlich

$$H = H_1 \cup \ldots \cup H_r,\ H_i := Z(p_i) \tag{16}$$

und ebenso für jeden Erweiterungskörper $K \subseteq L \subseteq \tilde{K}$:

$$H_L = (H_1)_L \cup \ldots \cup (H_r)_L \tag{17}$$

Definition 5.10: *Die in Gleichung (16) auftretenden K-Hyperflächen bezeichnet man als irreduzible Komponenten von H. Besitzt H nur eine irreduzible Komponente, so nennt man H selbst irreduzibel.*

Die irreduziblen Komponenten einer K-Hyperfläche H sind durch H und K eindeutig bestimmt, da die Primfaktorisierung (15) bis auf Assoziierte der Polynome p_i eindeutig bestimmt ist. Man beachte: Ist H eine K-Hyperfläche und L ein Erweiterungskörper von K, so ist H auch eine L-Hyperfläche, da $K[X_1, \ldots, X_n] \subseteq L[X_1, \ldots, X_n]$. Die irreduziblen Faktoren von f in $L[X_1, \ldots, X_n]$ können jedoch andere sein als in $K[X_1, \ldots, X_n]$.

Beispiel 5.11: In Abbildung 5 sind links die ähnlich aussehenden Mengen der $\mathbb{R}$-rationalen Punkte zweier ebener $\mathbb{R}$-Kurven zu sehen, nämlich die durch

$$L_1 := Z(\left(X_1^2 + X_2^2\right)^2 - \left(X_1^2 - X_2^2\right))$$

gegebene *Lemniskate von Bernoulli* (orange-farben) und die blau dargestellte Menge

$$L_2 := Z(X_2^4 + 2 \cdot X_1^4 \cdot X_2^2 - \left(1 - X_1^2\right) \cdot X_1^6)).$$

Die $\mathbb{R}$-Kurve L_1 ist irreduzibel: In einer Faktorisierung

$$\left(X_1^2 + X_2^2\right)^2 - \left(X_1^2 - X_2^2\right) = g \cdot h$$

muss ohne Einschränkung der Allgemeinheit entweder $\deg(g) = 1$ oder $\deg(g) = \deg(h) = 2$ gelten. Im ersten Fall wäre $Z(g)_{\mathbb{R}}$ eine Gerade mit

$Z(g)_{\mathbb{R}} \subseteq (L_1)_{\mathbb{R}}$, was offensichtlich nicht der Fall ist. Im zweiten Fall betrachtet man die homogenen Komponenten der Faktoren: $g = g_2 + g_1 + g_0$, $h = h_2 + h_1 + h_0$. Ist $g_0 \neq 0$, so muss $h_0 = h_1 = 0$ gelten, da gh nur homogene Komponenten vom Grad 2 und 4 besitzt. Es folgt $g_1 = 0$ aus demselben Grund. Die dann sich ergebende Gleichung

$$g_0 h_2 = g_0 h = (gh)_2 = -\left(X_1^2 - X_2^2\right)$$

steht im Widerspruch zu

$$g_2 h_2 = g_2 h = \left(X_1^2 + X_2^2\right)^2,$$

da die linke Seite durch $X_1 - X_2$ teilbar ist, die rechte aber nicht.

Es verbleibt der Fall $g_0 = h_0 = 0$, womit $g_1 h_1 = -(X_1^2 - X_2^2)$ und daher ohne Einschränkung der Allgemeinheit $g_1 = -(X_1 - X_2)$ und $h_1 = X_1 + X_2$ gilt. Es folgt

$$(X_1 - X_2)h_2 = (X_1 + X_2)g_2,$$

was nicht möglich ist, da $g_2 = h_2 = X_1^2 + X_2^2$ gilt.
Die $\mathbb{R}$-Kurve L_2 ist reduzibel, denn man hat die Faktorisierung

$$X_2^4 + 2 \cdot X_1^4 \cdot X_2^2 - \left(1 - X_1^2\right) \cdot X_1^6 = \left(X_2^2 - X_1^3 \cdot (1 - X_1)\right) \cdot \left(X_2^2 + X_1^3 \cdot (1 + X_1)\right).$$

Die auftretenden Faktoren sind irreduzibel: Man fasst $X_2^2 - X_1^3 \cdot (1 - X_1)$ als Element von $\mathbb{R}[X_1][X_2]$ auf. Als solches ist es primitiv, womit es nach Satz 3.6 genügt seine Irreduzibilität in $\mathbb{R}(X_1)[X_2]$ zu zeigen. Reduzibilität hätte aber die Existenz einer Nullstelle in $\mathbb{R}(X_1)$ zur Folge, was unmöglich ist, da $X_1^3 \cdot (1 - X_1)$ kein Quadrat ist. Die Irreduzibilität des zweiten Faktors wird analog bewiesen.

Insgesamt folgt

$$L_2 = Z(X_2^2 - X_1^3 \cdot (1 - X_1)) \cup Z(X_2^2 + X_1^3 \cdot (1 + X_1))$$

und die beiden $\mathbb{R}$-Kurven auf der rechten Seite der Gleichung sind die irreduziblen Komponenten von L_2. Sie werden *Quartiken von Longchamps* genannt; ihre $\mathbb{R}$-rationalen Punkte sind in Abbildung 5 rechts in blauer und roter Farbe dargestellt. $\diamond$

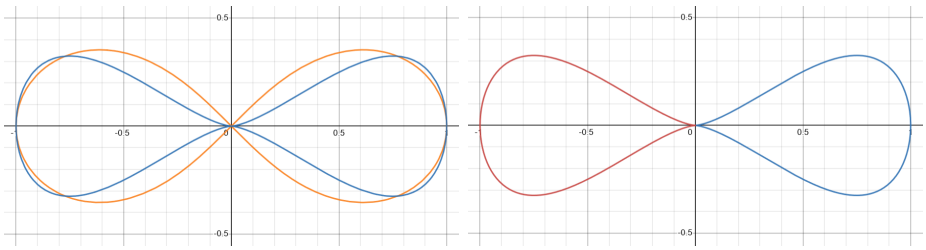


Abbildung 5: Lemniskate von Bernoulli (orange-farben) und Quartiken von Longchamps (blau / blau und rot)

Das Beispiel 5.11 zeigt, dass sich die irreduziblen Komponenten einer K-Hyperfläche schneiden können, weswegen man unter anderem(!) aus der Gestalt etwa der Menge der $\mathbb{R}$-rationalen Punkte nicht auf Reduzibilität schließen kann. Die Situation ist noch deutlich unschöner: Selbst wenn die Menge $H_{\mathbb{R}}$ einer $\mathbb{R}$-Hyperfläche in zwei oder mehr *disjunkte und abgeschlossene* Teilmengen zerfällt, kann H dennoch irreduzibel sein. Die im Beispiel 5.6 betrachtete elliptische Kurve ist irreduzibel, obwohl die Menge ihrer $\mathbb{R}$-rationalen Punkte in zwei disjunkte und abgeschlossene Teilmengen zerfällt. Die Abbildung 6 zeigt ein weiteres solches Beispiel, in diesem Fall im Raum: Die Menge $Z(X_1X_2X_3 - 1)_{\mathbb{R}} \subseteq \mathbb{R}^3$ ist die Vereinigung von vier abgeschlossenen, disjunkten Teilmengen, während $Z(X_1X_2X_3 - 1)$ selbst irreduzibel ist, wie man leicht nachprüft.

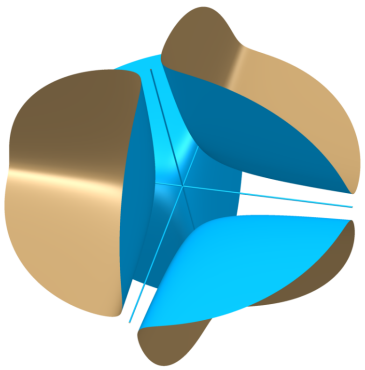


Abbildung 6: $Z(X_1X_2X_3 - 1)_{\mathbb{R}}$

Lokale Gestalt der Mengen $Z(f)_{\mathbb{R}}$

Um die geometrische Gestalt der $\mathbb{R}$-rationalen Punkte einer $\mathbb{R}$-Hyperfläche $Z(f) \subseteq \mathbb{C}^n$ zu ermitteln, kann man diese zunächst in »kleinen« Umgebungen jedes Punktes $P := (a_1, \ldots, a_n) \in Z(f)_{\mathbb{R}}$ untersuchen. Das Adjektiv »klein« bezieht sich dabei auf den euklidischen Abstand in $\mathbb{R}^n$.

Es genügt den Fall $P = 0$ zu betrachten, da man diesen durch eine affine Koordinatentransformation stets erzeugen kann:

$$\begin{aligned} f(X_1, \ldots, X_n) &= \sum_{(i_1,\ldots,i_n)\in E} a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \\ &= \sum_{(i_1,\ldots,i_n)\in E} a_{(i_1,\ldots,i_n)} (X_1 - a_1 + a_1)^{i_1} \cdot \ldots \cdot (X_n - a_n + a_n)^{i_n} \\ &= \sum_{(j_1,\ldots,j_n)\in F} b_{(j_1,\ldots,j_n)} (X_1 - a_1)^{j_1} \cdot \ldots \cdot (X_n - a_n)^{j_n} \\ &=: f_P(X_1 - a_1, \ldots, X_n - a_n), \end{aligned} \tag{18}$$

wobei sich die Koeffizienten $b_{(j_1,\ldots,j_n)} \in \mathbb{R}$ aus dem binomischen Satz

$$(X_k - a_k + a_k)^{i_k} = \sum_{\ell=0}^{i_k} \binom{i_k}{\ell} (X_k - a_k)^{\ell} a_k^{i_k - \ell},$$

dem Ausmultiplizieren der Summen in den einzelnen Monomen und dem Zusammenfassen nach Monomen gleichen Grades ergeben. Definiert man nun

$$Y_i := X_i - a_i,$$

so ist $f_P \in \mathbb{R}[Y_1, \ldots, Y_n]$ und es gilt $0 \in Z(f_P)$. Man überzeugt sich leicht, dass die gerade beschriebene Koordinatentransformation für jeden Körper K anstelle von $\mathbb{R}$ durchführbar ist. Die durchgeführte Rechnung zeigt folglich:

Feststellung 5.12: *Es sei $f \in K[X_1, \ldots, X_n] \setminus K$ und $P \in Z(f)_K$. Dann gibt es ein Polynom $f_P \in K[Y_1, \ldots, Y_n]$ mit der Eigenschaft*

$$f = f_P(X_1 - a_1, \ldots, X_n - a_n).$$

Insbesondere gilt $0 \in Z(f_P)$.

Sei nun also $0 \in Z(f)$ und

$$f = f_{k_1} + f_{k_2} + \ldots + f_{k_r},\ k_1 < k_2 < \ldots < k_r$$

die Darstellung von f als Summe von 0 verschiedener homogener Komponenten. Aus dieser ergibt sich die Ungleichung

$$|f(x_1, \ldots, x_n) - f_{k_1}(x_1, \ldots, x_n)| \leq |f_{k_2}(x_1, \ldots, x_n)| + \ldots + |f_{k_r}(x_1, \ldots, x_n)|$$

für beliebige $x_1, \ldots, x_n \in \mathbb{C}$. Kombiniert man diese mit der Monomungleichung

$$\begin{aligned} |a_{(i_1,\ldots,i_n)} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}| &= |a_{(i_1,\ldots,i_n)}|\,|x_1|^{i_1} \cdot \ldots \cdot |x_n|^{i_n} \\ &\leq |a_{(i_1,\ldots,i_n)}|\,\|(x_1,\ldots,x_n)\|_2^{i_1+\ldots+i_n}, \end{aligned}$$

wobei $\|\cdot\|_2$ die euklidische Norm des $\mathbb{C}^n$ bezeichnet, so ergibt sich für alle $(x_1, \ldots, x_n) \in \mathbb{C}^n$ mit $\|(x_1, \ldots, x_n)\|_2 < 1$:

$$\begin{aligned} |f(x_1,\ldots,x_n) - f_{k_1}(x_1,\ldots,x_n)| &\leq \sum_{j=2}^{r} a_j s_j \|(x_1,\ldots,x_n)\|_2^{k_j} \\ &\leq (r-1)\max(a_j s_j : j \in \{2,\ldots r\})\|(x_1,\ldots,x_n)\|_2^{k_2}, \end{aligned}$$

wobei a_j der maximale Betrag der Koeffizienten von f_{k_j} und s_j die Anzahl der Monome in f_{k_j} ist. Folglich existiert eine nur von f abhängende Konstante $C > 0$ mit der Eigenschaft

$$\|(x_1,\ldots,x_n)\|_2 < 1 \Rightarrow |f(x_1,\ldots,x_n) - f_{k_1}(x_1,\ldots,x_n)| \leq C\|(x_1,\ldots,x_n)\|_2^{k_2}. \qquad (19)$$

Aus dieser Ungleichung ergibt sich:

Satz 5.13: *Sei $f \in \mathbb{R}[X_1, \ldots, X_n] \setminus \mathbb{R}$ ein Polynom mit der Eigenschaft $0 \in Z(f)$. Dann gilt für seine homogene Komponente minimalen Grades f_ℓ:*

$$\forall \epsilon \in (0,1)\ \exists \delta > 0\ \|(x_1,\ldots,x_n)\|_2 < \delta \Rightarrow |f(x_1,\ldots,x_n) - f_\ell(x_1,\ldots,x_n)| \leq \epsilon.$$

Bemerkung: Salopp gesprochen haben $Z(f)_\mathbb{R}$ und $Z(f_\ell)_\mathbb{R}$ nahe des Nullpunkts ähnliche Gestalt.

Beweis: Zu gegebenem ϵ setzt man $\delta := (C^{-1}\epsilon)^{\frac{1}{k_2}}$ mit der Konstanten C aus Ungleichung (19) und k_2 dem zweitgrößten Grad einer von 0 verschiedenen homogenen Komponente von f. □

Der gerade bewiesene Satz motiviert die

Definition 5.14: *Es sei $f \in K[X_1, \ldots, X_n] \setminus K$ und $P \in Z(f)_K$. Dann bezeichnet man die homogene Komponente $L(f, P)$ niedrigsten Grades des Polynoms f_P aus Feststellung 5.12 als Leitform von f im Punkt P.*

Beispiel 5.15: Wir betrachten die als »Newton'scher Knoten« bezeichnete ebene $\mathbb{R}$-Kurve

$$C := Z(X_1^2 - X_2^2 + X_1^3 - X_2^3 + X_1^2 X_2).$$

Die definierende Gleichung besitzt homogene Komponenten der Grade 2 und 3. Folglich gilt für $f := X_1^2 - X_2^2 + X_1^3 - X_2^3 + X_1^2 X_2$ die Gleichung

$$L(f,0) = X_1^2 - X_2^2$$

und $C_{\mathbb{R}}$ besitzt nahe bei 0 ähnliche Gestalt wie die Menge

$$Z(L(f,0))_{\mathbb{R}} = Z(X_1^2 - X_2^2)_{\mathbb{R}} = Z((X_1 - X_2)(X_1 + X_2))_{\mathbb{R}}.$$

Nun ist aber offensichtlich

$$Z((X_1 - X_2)(X_1 + X_2))_{\mathbb{R}} = Z(X_1 - X_2)_{\mathbb{R}} \cup Z(X_1 + X_2)_{\mathbb{R}},$$

wobei die beiden rechts stehenden Mengen Ursprungsgeraden sind. Es ergibt sich die in Abbildung 7 dargestellte Situation.

Will man die lokale Gestalt in der Nähe beispielsweise des Punktes $(0,-1) \in C$ ermitteln, so führt man zunächst die Koordinatentransformation (18) durch:

$$\begin{aligned} f &= X_1^2 - (X_2+1-1)^2 + X_1^3 - (X_2+1-1)^3 + X_1^2(X_2+1-1) \\ &= X_1^2 - (X_2+1)^2 + 2(X_2+1) - 1 + X_1^3 - (X_2+1)^3 + 3(X_2+1)^2 \\ &\quad -3(X_2+1) + 1 + X_1^2(X_2+1) - X_1^2 \\ &= Y_1^2 - Y_2^2 + 2Y_2 - 1 + Y_1^3 - Y_2^3 + 3Y_2^2 - 3Y_2 + 1 + Y_1^2 Y_2 - Y_1^2 \\ &= -Y_2 + 2Y_2^2 + Y_1^3 - Y_2^3 + Y_1^2 Y_2 \\ &= f_{(0,-1)}. \end{aligned}$$

Damit gleicht die Gestalt von $Z(f)_{\mathbb{R}}$ nahe $(0,-1)$ der Gestalt von

$$Z(-Y_2 + 2Y_2^2 + Y_1^3 - Y_2^3 + Y_1^2 Y_2)_{\mathbb{R}}$$

nahe $(0,0)$ und die Letztere wiederum ähnelt

$$Z(L(f_{(0,-1)},0))_{\mathbb{R}} = Z(-Y_2)_{\mathbb{R}}$$

also einer horizontalen Geraden. ◇

Beispiel 5.16: Das definierende Polynom f der $\mathbb{R}$-Fläche aus Beispiel 5.7 besitzt homogene Komponenten der Grade 2 und 4. Die Menge

$$Z(L(f,0))_{\mathbb{R}} = Z(X_1^2 + X_2^2 - X_3^2)_{\mathbb{R}}$$

ist die Mantelfläche eines unendlich ausgedehnten Doppelkegels, der symmetrisch zur X_3-Achse liegt. Ein Ausschnitt von $Z(L(f,0))_{\mathbb{R}}$ zusammen mit der Menge $Z(f)_{\mathbb{R}}$ ist in Abbildung 8 dargestellt. ◇

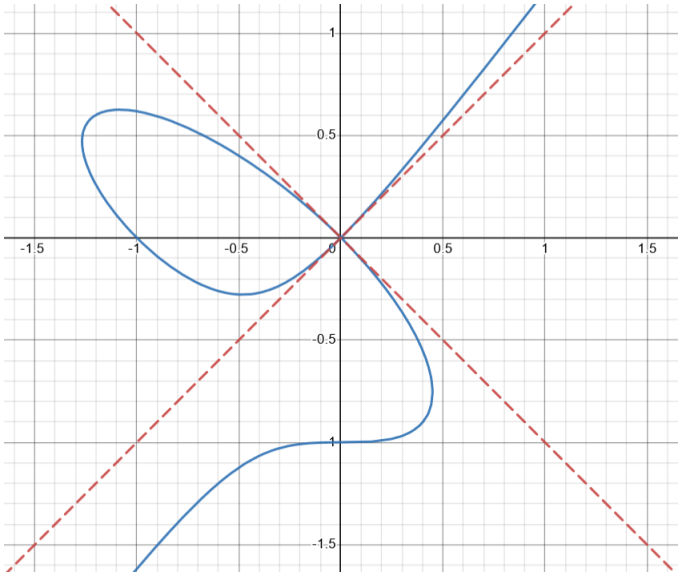


Abbildung 7: $Z(X_1^2 - X_2^2 + X_1^3 - X_2^3 + X_1^2 X_2)_{\mathbb{R}}$ (blau), $Z(X_1^2 - X_2^2)_{\mathbb{R}}$ (rot)

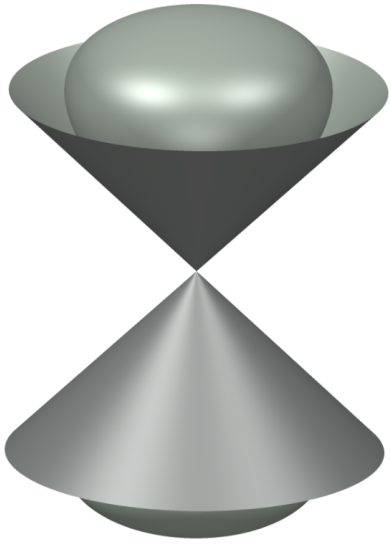


Abbildung 8: $Z(X_1^2 + X_2^2 + X_3^4 - X_3^2)_{\mathbb{R}}$ und $Z(X_1^2 + X_2^2 - X_3^2)_{\mathbb{R}}$

BEISPIEL 5.17: In der Abbildung 9 sind drei Ansichten der Menge

$$Z(X_1^3 + X_1^2X_3^2 + X_1^2 - X_2^2)_{\mathbb{R}}$$

dargestellt: aus der X_2-X_3-Koordinatenebene (links), von einem Raumpunkt außerhalb aller drei Koordinatenebenen (Mitte) und aus Richtung der X_3-Achse (rechts).

Die Leitform $L(f, 0)$ des definierenden Polynoms f ist

$$X_1^2 - X_2^2 = (X_1 - X_2)(X_1 + X_2).$$

Die Gleichungen $X_1 \pm X_2 = 0$ besitzen Ursprungsebenen in $\mathbb{C}^3$ beziehungsweise $\mathbb{R}^3$ als Lösungsmengen. Die betrachtete $\mathbb{R}$-Fläche verhält sich also nahe des Koordinatenursprungs wie zwei sich schneidende Ursprungsebenenen – siehe Abbildung 9 rechts. ◇

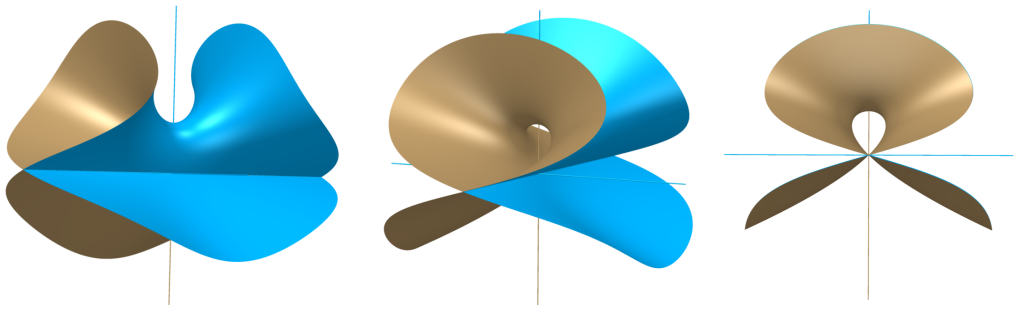


Abbildung 9: Ansichten von $Z(X_1^3 + X_1^2X_3^2 + X_1^2 - X_2^2)_{\mathbb{R}}$

Satz 5.13 zeigt, dass es lohnenswert ist einen genaueren Blick auf die durch homogene Polynome definierten affinen algebraischen Hyperflächen zu werfen.

SATZ 5.18: *Für die durch ein homogenes Polynom $h \in K[X_1, \ldots, X_n]$ vom Grad $d > 0$ definierte K-Hyperfläche $Z(h)$ gilt: Ist $x \in Z(h) \setminus 0$, so liegt die Ursprungsgerade $\tilde{K} \cdot x \subset \tilde{K}^n$ vollständig in $Z(h)$. Insbesondere liegt für jedes $x \in Z(h)_K \setminus 0$ die Ursprungsgerade $K \cdot x \subset K^n$ vollständig in $Z(h)_K$.*

BEWEIS: Es seien $(x_1, \ldots, x_n) \in Z(h) \setminus 0$ und $\lambda \in \tilde{K}$. Dann gilt

$$h(\lambda x_1, \ldots, \lambda x_n) = \lambda^d h(x_1, \ldots, x_n) = \lambda^d \cdot 0.$$

Die verbleibende Aussage ergibt sich aus der Inklusion $K \cdot x \subseteq \tilde{K} \cdot x$ sowie der Identität $\tilde{K} \cdot x \cap K^n = K \cdot x$, falls $x \in K^n$. □

Die Beispiele 5.16 und 5.17 demonstrieren den Satz 5.18: In einem Doppelkegel $D \subset \mathbb{R}^3$ mit Spitze im Ursprung verläuft offensichtlich jede Gerade durch einen Punkt $P \in D \setminus 0$ und den Ursprung vollständig innerhalb von D. Im anderen Beispiel ist die Menge $Z(L(f,0))_{\mathbb{R}}$ eine Vereinigung zweier Ursprungsebenen. Eine Gerade durch den Ursprung und einen Punkt $P \in Z(L(f,0))_{\mathbb{R}} \setminus 0$ verläuft dann innerhalb einer der beiden Ebenen.
Im Fall von ebenen $\mathbb{R}$-Kurven besitzt Satz 5.18 eine besondere Ausprägung:

SATZ 5.19: *Für ein homogenes Polynom $h \in K[X_1, X_2]$ vom Grad $d > 0$ gilt:*

1. *Genau dann ist $(b_1, b_2) \in Z(h) \setminus 0$, wenn $b_2X_1 - b_1X_2$ ein irreduzibler Faktor von h ist.*

2. *Die Primfaktorisierung von h im Ring $\tilde{K}[X_1, X_2]$ besitzt die Form*

$$h = \prod_{i=1}^{m} (a_{i,1}X_1 + a_{i,2}X_2)^{e_i}.$$

BEMERKUNG: Satz 5.19 lässt sich nicht auf den Fall $n > 2$ verallgemeinern, da ein homogenes Polynom dann auch über dem algebraischen Abschluss betrachtet irreduzible Faktoren vom Grad größer als 1 besitzen kann. Ein Beispiel ist das irreduzible homogene Polynom $X_1^2 + X_2^2 - X_3^2 \in \mathbb{C}[X_1, X_2, X_3]$ – siehe Beispiel 6.3.

BEWEIS: 1. Die Implikation $\Leftarrow$ ist klar.

$\Rightarrow$: Eine der beiden Koordinaten b_1 und b_2 ist nicht 0 - ohne Einschränkung sei dies b_2. Polynomdivision von h durch $b_2X_1 - b_1X_2$ im Polynomring $\tilde{K}[X_2][X_1]$ liefert

$$h = q(b_2X_1 - b_1X_2) + r$$

mit einem Restpolynom r, welches entweder 0 ist oder $\deg_{X_1}(r) = 0$ erfüllt. Im ersten Fall ist die Behauptung bewiesen. Im zweiten Fall gilt für alle $\lambda \in \tilde{K}$:

$$r(\lambda b_2) = h(\lambda b_1, \lambda b_2) - q(\lambda b_1, \lambda b_2)(b_2b_1 - b_1b_2) = 0,$$

womit $r \in \tilde{K}[X_2]$ unendlich viele Nullstellen besitzt – ein Widerspruch.

2. Man führt eine Induktion nach d durch.

Der Induktionsanfang bei $d = 1$ ist offensichtlich richtig.

Sei nun $d > 1$ und $x_1 \in \tilde{K} \setminus 0$. Da Polynom $h(x_1, X_2) \in \tilde{K}[X_2]$ besitzt dann eine Nullstelle x_2, womit $h(x_1, x_2) = 0$ gilt. Nach Punkt 1 gilt dann

$$h = h_1(x_2 X_1 - x_1 X_2)$$

mit einem Polynom h_1 vom Grad $d - 1$, das nach Satz 4.4 homogen ist. □

Als unmittelbare Folgerung aus Satz 5.19 erhält man:

KOROLLAR 5.20: *Für jeden Punkt P einer ebenen K-Kurve $Z(f)$ gilt*

$$Z(L(f, P)) = T_1 \cup \ldots \cup T_m,$$

wobei $T_i \subset \tilde{K}^2$ paarweise verschiedene Geraden mit $P \in T_i$ sind.

Die geometrische Interpretation dieses Korollars im Fall $K = \mathbb{R}$ motiviert die

DEFINITION 5.21: *Es sei $C := Z(f)$ eine ebene K-Kurve und $P \in C$. Die im Korollar 5.20 auftretenden Geraden $T_1, \ldots, T_m$ bezeichnet man als Tangenten an C im Punkt P.*

Den Exponenten mit dem das definierende Polynom einer Tangente T in P in der Faktorisierung der Leitform $L(f, p)$ auftritt (siehei Punkt 2 von Satz 5.19) nennt man auch die Vielfachheit der Tangente T.

Mit Hilfe der Tangenten und ihrer Vielfachheiten kann man eine allerdings unvollständige geometrisch motivierte Klassifikation der Punkte einer ebenen K-Kurve
$C = Z(f) \subset K^2$ vornehmen: Es sei $P = (p_1, p_2) \in C$ und

$$L(f, P) = \prod_{i=1}^{m} (a_{i,1}(X_1 - p_1) + a_{i,2}(X_2 - p_2))^{e_i}$$

die Primfaktorisierung der Leitform $L(f, P)$ gemäß Satz 5.19. Dann bezeichnet man P als

- *einfachen oder regulären Punkt*, falls $m = 1$ und $e_1 = 1$ gilt;
- *gewöhnlichen m-fach Punkt*, falls $m > 1$ und $e_1 = \ldots = e_m = 1$ gilt;
- *Spitze*, falls $m = 1$ und $e_1 > 1$ gilt.

Die in dieser Klassifikation nicht auftretenden Fälle müssen mit subtileren Mitteln klassifiziert werden.

Die nicht einfachen Punkte der Kurve C werden als *Singularitäten von C* bezeichnet.

Beispiel 5.22: Die Abbildung 10 zeigt zwei ebene $\mathbb{R}$-Kurven mit einem gewöhnlichen Mehrfachpunkt bei $P = 0$: Links sind die $\mathbb{R}$-rationalen Punkte der Bernoullischen Lemniskate

$$C_1 := Z(\left(X_1^2 + X_2^2\right)^2 - \left(X_1^2 - X_2^2\right)) \subset \mathbb{C}^2$$

aus Beispiel 5.11 dargestellt. Die Primfaktorisierung der Leitform in $= 0$ ist

$$L(C_1, 0) = \left(X_1^2 - X_2^2\right) = (X_1 - X_2)(X_1 + X_2).$$

Insbesondere findet diese Faktorisierung bereits im Ring $\mathbb{R}[X_1, X_2]$ statt, mit der Konsequenz, dass für die beiden Tangenten im Punkt 0 die Gleichung

$$Z(L(C_1, 0))_{\mathbb{R}} = Z(X_1 - X_2)_{\mathbb{R}} \cup Z(X_1 + X_2)_{\mathbb{R}}$$

gilt – siehe Abbildung 10 links.

Die Abbildung 10 ist rechts das so genannte *Trifolium*

$$C_2 := Z(\left(X_1^2 + X_2^2\right)^2 - 3 \cdot X_1^2 \cdot X_2 + X_2^3) \subset \mathbb{C}^2$$

dargestellt, jedenfalls seine $\mathbb{R}$-rationalen Punkte. Die Leitform im Punkt $P = 0$ faktorisiert wie im Fall der Lemniskate bereits in $\mathbb{R}[X_1, X_2]$ vollständig in lineare Polynome:

$$L(C_2, 0) = -3 \cdot X_1^2 \cdot X_2 + X_2^3 = X_2(X_2 - \sqrt{3}X_1)(X_2 + \sqrt{3}X_1),$$

es handelt sich bei 0 also um einen gewöhnlichen 3-fach Punkt. ◇

Beispiel 5.23: Die Abbildung 11 zeigt ebene $\mathbb{R}$-Kurven mit Spitzen: Links sind die $\mathbb{R}$-rationalen Punkte der durch

$$C_1 := Z(X_2^2 - X_1^3)$$

definierten *Neile'schen Parabel* zu sehen. Ihre Leitform im Punkt 0 ist

$$L(f, 0) = X_2^2,$$

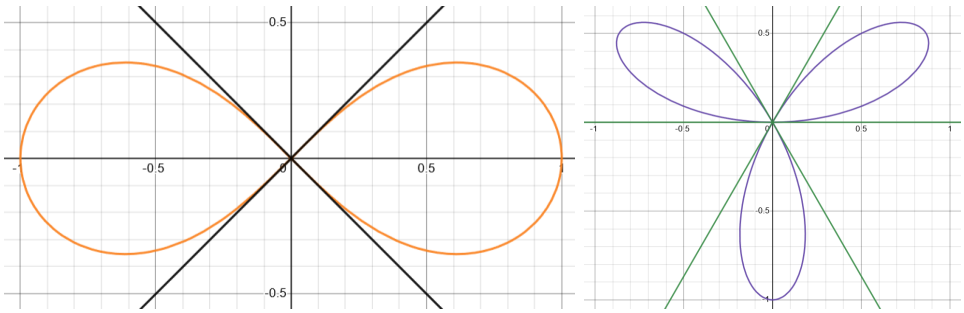


Abbildung 10: Bernoulli's Lemniskate (links) und Trifolium (rechts)

womit C_1 dort nur die X_1-Achse als Tangente besitzt, diese allerdings mit der Vielfachheit 2.

In Abbildung 11 ist rechts das so genannte *Bicorn* zu sehen, es ist durch

$$C_2 := Z(X_2^2(1 - X_1^2) - (X_1^2 + 2X_2 - 1)^2)$$

gegeben und besitzt offensichtlich mindestens zwei Singularitäten - man beachte, dass Singularitäten mit nicht-reellen Koordinaten existieren könnten. Um die Natur des Punktes $P := (-1, 0)$ zu ermitteln, berechnet man das Polynom f_P:

$$\begin{aligned} X_2^2(1 - X_1^2) - (X_1^2 + 2X_2 - 1)^2 &= X_2^2(1 - (X_1 + 1 - 1)^2) - ((X_1 + 1 - 1)^2 + 2X_2 - 1)^2 \\ &= X_2^2(-(X_1 + 1)^2 + 2(X_1 + 1)) - ((X_1 + 1)^2 - 2(X_1 + 1) + 2X_2)^2 \\ &= -(X_1 + 1)^4 - 4(X_1 + 1)^2 - 4X_2^2 + 4(X_1 + 1)^3 \\ &\quad -4X_2(X_1 + 1)^2 + 8X_2(X_1 + 1) \\ &\quad -X_2^2(X_1 + 1)^2 + 2X_2^2(X_1 + 1) \\ &= -Y_1^4 - Y_2^2Y_1^2 + 4Y_1^3 - 4Y_2Y_1^2 + 2Y_2^2Y_1 - 4Y_1^2 - 4Y_2^2 + 8Y_2Y_1. \end{aligned}$$

Als Leitform im Punkt P ergibt sich damit

$$\begin{aligned} L(f, P) &= -4Y_1^2 - 4Y_2^2 + 8Y_2Y_1 \\ &= -4(Y_1 - Y_2)^2 = -4((X_1 + 1) - X_2)^2. \end{aligned}$$

Der Punkt P ist also eine Spitze mit der doppelten Tangente $Z((X_1 + 1) - X_2)$. ◇

Abbildung 11: Neile'sche Parabel (links) und Bicorn (rechts)

6 Irreduzibilität

Nachdem durch die Ausführungen des vorigen Abschnitts klar geworden ist, dass die Bestimmung irreduzibler Faktoren eines Polynoms $f \in K[X_1, \ldots, X_n]$ nützlich ist, stellen sich die beiden eng miteinander verbundenen Probleme Irreduzibilität zu erkennen und die Zerlegung von f in irreduzible Faktoren zu ermitteln. Wie im Fall der Frage nach der Existenz der Primfaktorisierung in $K[X_1, \ldots, X_n]$ ist es auch für die beiden vorliegenden Probleme gewinnbringend den Polynomring in der Form $K[X_1, \ldots, X_{n-1}][X_n]$ zu betrachten, also als Polynomring in einer Unbestimmten über einem faktoriellen Ring. Man beachte dabei, dass anstelle der Unbestimmten X_n auch jede andere der n Unbestimmten gewählt werden kann. Diese Wahlmöglichkeit erweist sich etwa bei der Ermittlung der Irreduzibilität konkreter Polynome als sehr nützlich.

Satz 6.1 (Eisenstein-Kriterium): *Es sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R$ ein Primelement. Für das Polynom*

$$f = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_1 X + a_0 \in R[X]$$

gelte: $p \nmid a_d$, $\forall i < d\ p \mid a_i$, $p^2 \nmid a_0$.

Dann ist f irreduzibel in $K[X]$. Insbesondere gibt es keine Zerlegung $f = gh$, $g, h \in R[X]$, $\deg(g) > 0$, $\deg(h) > 0$.

Bemerkung: Das Polynom f im Satz kann durchaus reduzibel in $R[X]$ sein, wobei dann die Zerlegung vom Typ $f = r \cdot g$ mit $r \in R$ ist.

Beweis: Die Gleichung $f = I(f)\tilde{f}$ zeigt, dass man sich auf den Fall eines primitiven Polynoms f beschränken kann. Wäre f in $K[X]$ reduzibel, so

gäbe es nach Satz 3.6 auch eine Zerlegung $f = gh$ mit primitiven Polynomen $g, h \in R[X]$.

Es seien a_k, b_k und c_k die Koeffizienten von g, h und f. Es gilt dann $c_0 = a_0 b_0$, woraus wegen $p^2 \nmid c_0$ ohne Einschränkung der Allgemeinheit $p \mid a_0$ und $p \nmid b_0$ folgt. Der Leitkoeffizient von f ist $a_m b_n$, wobei a_m und b_n die Leitkoeffizienten von g und h sind. Da p nach Voraussetzung $a_m b_n$ nicht teilt, gilt $p \nmid a_m$. Sei k der kleinste Index mit der Eigenschaft $p \nmid a_k$. Dann gilt also $k > 0$ und $k < m$. Man betrachtet jetzt

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0.$$

Nach Voraussetzung über f und Wahl von k sind c_k und alle Terme $a_i b_{k-i}$, $i \in \{0, \ldots, k-1\}$ durch p teilbar, also auch $a_k b_0$ – ein Widerspruch. □

Beispiel 6.2: Das Polynom $f = X_2^2 - X_1^3 + X_1 \in K[X_1, X_2]$ aus Beispiel 5.6 ist irreduzibel: Man betrachtet es als Element von $K[X_1][X_2]$ und wählt $p = X_1$. Das Eisenstein-Kriterium ist anwendbar und liefert die Irreduzibilität im Polynomring $K(X_1)[X_2]$. Da f aber primitiv ist, folgt damit die Irreduzibilität im Polynomring $K[X_1][X_2]$ aus Satz 3.6. ◇

Beispiel 6.3: Das Polynom $f = X_1^2 + X_2^2 - X_3^2 \in K[X_1, X_2, X_3]$ aus Beispiel 5.16 kann für jeden Körper K betrachtet werden. Ob es irreduzibel ist oder nicht hängt vom Körper K ab:

$K = \mathbb{R}$: Man fasst f als Element von $K[X_1, X_2][X_3]$ auf. Das Polynom $X_1^2 + X_2^2 \in \mathbb{R}[X_1, X_2]$ ist irreduzibel also ein Primelement. Wäre es keines, so läge eine Faktorisierung in Polynome von totalem Grad 1 vor. Diese besitzen unendlich viele Nullstellen in $\mathbb{R}^2$, wogegen f dort nur die Nullstelle $(0, 0)$ vorweist.

Nun kann man das Eisenstein-Kriterium mit $p = X_1^2 + X_2^2$ anwenden und erhält in Kombination mit Satz 3.6 die Irreduzibilität in $\mathbb{R}[X_1, X_2][X_3]$.

$K = \mathbb{C}$: Es gilt $X_1^2 + X_2^2 = (X_1 - iX_2)(X_1 + iX_2)$, wobei die beiden Faktoren auf der rechten Seite Primelemente in $\mathbb{C}[X_1, X_2]$ sind, da sie den Grad 1 besitzen. Man kann nun das Eisenstein-Kriterium mit $p = X_1 - iX_2$ oder $p = X_1 + iX_2$ anwenden um wie im Fall $K = \mathbb{R}$ die Irreduzibilität in $\mathbb{C}[X_1, X_2][X_3]$ nachzuweisen.

K mit der Eigenschaft $1 + 1 = 0$: Ein solcher Körper ist zum Beispiel der Körper $\mathbb{F}_2$ mit zwei Elementen, aber auch der Körper $\mathbb{F}_2(X)$ der rationalen

Funktionen in einer Unbestimmten X. In jedem solchen Körper gilt

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$$

für beliebige $a, b \in K$. Es folgt

$$f = X_1^2 + X_2^2 - X_3^2 = X_1^2 + X_2^2 + X_3^2 = (X_1 + X_2 + X_3)^2,$$

womit f reduzibel ist. $\diamond$

Beispiel 6.4: Das Polynom $f \in K[X_1, \ldots, X_n]$ ist genau dann irreduzibel, wenn das durch affine Koordinatentransformation entstehende Polynom $f_P \in K[Y_1, \ldots, Y_n]$ (siehe (18)) für einen frei wählbaren Punkt $P = (a_1, \ldots, a_n) \in K^n$ irreduzibel ist: Nach Definition gilt

$$f = f_P(X_1 - a_1, \ldots, X_n - a_n),$$

womit aus $f_P = \bar{g}\bar{h}$ die Gleichung

$$f = \bar{g}(X_1 - a_1, \ldots, X_n - a_n)\bar{h}(X_1 - a_1, \ldots, X_n - a_n) = gh$$

folgt.

Wir wenden dies auf das Polynom $f = X_1^2 - X_2^2 + X_1^3 - X_2^3 + X_1^2 X_2$ aus Beispiel 5.15: Um das Eisenstein-Kriterium mit X_1 als Unbestimmte anzuwenden, muss wegen des Monoms $X_1^2 X_2$ das Primelement $p = X_2$ gewählt werden. Dann ist aber das Kriterium wegen des Monoms X_1^2 nicht anwendbar. Ein analoge Situation ergibt sich bei Wahl von X_2 als Unbestimmte.

Das Eisenstein-Kriterium ist hier nicht direkt anwendbar. Für das Polynom

$$f_{(0,-1)} = -Y_2 + 2Y_2^2 + Y_1^3 - Y_2^3 + Y_1^2 Y_2 \in K[Y_2][Y_1]$$

kann man das Kriterium mit $p = Y_2$ anwenden und erhält die Irreduzibilität von f. $\diamond$

Satz 6.5 (Reduktionskriterium): *Es seien R und S Integritätsbereiche mit den Quotientenkörpern K und L. Es sei $\phi : R \to S$ ein Ringhomomorphismus. Dann ist durch die Abbildung*

$$\Phi : R[X] \to S[X], a_d X^d + \ldots + a_0 \mapsto \phi(a_d)X^d + \ldots + \phi(a_0)$$

ein Ringhomomorphismus gegeben.

Es sei $f \in R[X]$ ein Polynom mit der Eigenschaft $\deg(f) = \deg(\Phi(f))$. Ist dann $\Phi(f)$ irreduzibel in $L[X]$, so gibt es keine Zerlegung $f = gh$, $g, h \in R[X]$, $\deg(g) > 0$, $\deg(h) > 0$.

BEWEIS: Der Beweis der Aussage, dass es sich bei Φ um einen Ringhomomorphismus handelt, ist Routine.

Das Polynom $f \in A[X]$ erfülle die Gradvoraussetzung und $f = gh$, $g, h \in R[X]$, $\deg(g) > 0$, $\deg(h) > 0$. Dann gilt $\Phi(f) = \Phi(g)\Phi(h)$ und

$$\deg(\Phi(f)) = \deg(\Phi(g)) + \deg(\Phi(h)) \leq \deg(g) + \deg(h) = \deg(f) = \deg(\Phi(f)).$$

Es folgt $\deg(\Phi(g)) = \deg(g) > 1$ und $\deg(\Phi(h)) = \deg(h) > 1$ im Widerspruch zur Irreduzibilität von $\Phi(f)$. □

BEISPIEL 6.6: Wir betrachten das Polynom

$$f = X_1^3 + X_1^2 X_3^2 + X_1^2 - X_2^2 \in \mathbb{R}[X_1, X_2, X_3] = \mathbb{R}[X_2, X_3][X_1]$$

aus Beispiel 5.17 und den Ringhomomorphismus

$$\phi : \mathbb{R}[X_2, X_3] \to \mathbb{R}[X_3], h \mapsto h(1, X_3).$$

Es gilt $\deg_{X_1}(f) = 3$ und $\deg_{X_1}(\Phi(f)) = \deg_{X_1}(X_1^3 + X_1^2 X_3^2 + X_1^2 - 1) = 3$. Wäre $X_1^3 + X_1^2 X_3^2 + X_1^2 - 1$ reduzibel in $\mathbb{R}(X_3)[X_1]$, so besäße es aus Gradgründen eine Nullstelle

$$\alpha = \frac{z}{n},\ z, n \in \mathbb{R}[X_3] \text{ teilerfremd.}$$

Man beachte, dass dieses Argument nur für Polynome dritten Grades mit Koeffizienten in einem *Körper* anwendbar ist, weswegen man das in Frage stehende Polynom zunächst im Polynomring $\mathbb{R}(X_3)[X_1] \supset \mathbb{R}[X_3][X_1]$ betrachten muss.

Es folgt

$$0 = z^3 + z^2 n X_3^2 + z^2 n - n^3,$$

womit z^3 durch n teilbar ist, im Widerspruch zur Teilerfremdheit von z und n. Das Reduktionskriterium zeigt nun, dass f nur in der Form gh mit $g \in \mathbb{R}[X_2, X_3]$ und $h \in \mathbb{R}[X_2, X_3][X_1]$ zerlegbar ist. Dies ist jedoch unmöglich, da f als Element von $\mathbb{R}[X_2, X_3][X_1]$ betrachtet primitiv ist. Folglich ist f ein irreduzibles Polynom. ◇

Beispiel 6.7: Mit Hilfe des Reduktionskriteriums lassen sich massenweise irreduzible Polynome im Ring $\mathbb{Z}[X]$ finden, indem man den Ringhomomorphismus

$$\phi : \mathbb{Z} \to \mathbb{F}_p,\ z \mapsto \overline{z}$$

nutzt, der jeder ganzen Zahl ihren Rest modulo einer Primzahl p zuweist. So ist beispielsweise das Polynom $X^3 + X^2 + 2 \in \mathbb{F}_3[X]$ irreduzibel, weil es in $\mathbb{F}_3$ keine Nullstelle besitzt. Folglich sind alle Polynome der Form

$$X^3 + (3a+1)X^2 + 3bX + (3c+2),\ a, b, c \in \mathbb{Z}$$

irreduzibel in $\mathbb{Z}[X]$. ◇

Wir wollen abschließend auch das zweite eingangs formulierte Problem, nämlich die Faktorisierung in irreduzible Polynome, addressieren.

Der Algorithmus von Kronecker

Die Grundlagen des hier dargestellten Verfahrens sind in jedem unendlichen Integritätsbereich verfügbar.

Satz 6.8 (Interpolation nach Lagrange): *Es seien $x_1, \ldots, x_{d+1}$ paarweise verschiedene und $y_1, \ldots, y_{d+1}$ beliebige Elemente eines Integritätsbereichs R. Dann existiert höchstens ein Polynom $f \in R[X]$ vom Grad d mit der Eigenschaft $f(x_i) = y_i$ für alle $i \in \{1, \ldots, d+1\}$.*

Ist R ein Körper, so existiert ein Polynom $f \in R[X]$ mit den angegebenen Eigenschaften.

Bemerkungen:

1. Das im Satz betrachtete Polynom f wird als Interpolationspolynom vom Grad d zu den Daten $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ bezeichnet.

2. Das Beispiel $R = \mathbb{Z}$, $x_1 = 0$, $x_2 = 3$, $y_1 = 0$ und $y_2 = 1$ zeigt, dass ein Interpolationspolynom zum Grad d nicht existieren muss.

Beweis: Es seien $f_1, f_2 \in R[X]$ Polynome, die die im Satz angegebenen Bedingungen erfüllen. Dann besitzt das Polynom $f_1 - f_2$ einen Grad kleiner gleich d und $d+1$ verschiedene Nullstellen. Dies ist für Polynome mit Koeffizienten in einem Integritätsbereich nur für das Nullpolynom möglich.

Im Fall eines Körpers R kann man das gesuchte Polynom konkret angeben: Für jedes $k \in \{1, \ldots, d+1\}$ sei

$$L_k := \prod_{i \neq k} \frac{X - x_i}{x_k - x_i}.$$

Für diese so genannten *Lagrange-Polynome* gilt offensichtlich

$$\forall i \neq k \; L_k(x_i) = 0, \; L_k(x_k) = 1.$$

Daher besitzt das Polynom

$$L := \sum_{i=1}^{d+1} y_i L_i \in R[X] \tag{20}$$

die gewünschte Eigenschaft. □

Das Verfahren von Kronecker beruht auf der einfachen

Beobachtung: Ist $g \in R[X]$ ein Teiler des Polynoms $f \in R[X]$, so ist für jedes $x \in R$ auch $g(x)$ ein Teiler von $f(x)$.

Damit lässt sich das folgende Verfahren zur Faktorisierung eines Polynoms $f \in R[X]$ vom Grad $n > 0$ formulieren:

1. Initialisierung: Wähle ein $x_1 \in R$ derart, dass $f(x_1)$ möglichst wenige Teiler besitzt (oder wähle x_1 beliebig), setze $d = 0$ (Grad der betrachteten irreduziblen Faktoren), $I = \{x_1\}$ (Liste der Interpolationspunkte) und $F = \emptyset$ (Liste der Faktoren und ihrer Vielfachheit).

2. Hinzufügen eines Interpolationspunktes: Setze $d := d + 1$ und wähle ein $x_{d+1} \in R \setminus I$ derart, dass $f(x_{d+1})$ möglichst wenige Teiler besitzt (oder wähle x_{d+1} beliebig).

3. Kandidaten testen: Ermittle alle Polynome $g \in R[X]$ vom Grad d mit den Eigenschaften

   $$g(x_1) = y_1, \ldots, g(x_{d+1}) = y_{d+1},$$

   wobei y_i bis auf Assoziierte alle Teiler von $f(x_i)$ durchläuft.

   Teste mittels Polynomdivision in $K[X]$, K der Quotientenkörper von R, für jedes solche g, ob es f teilt. Ist dies der Fall ermittle durch Polynomdivision die maximale Zahl $e \in \mathbb{N}$ für die $f = g^e h$ in $R[X]$ gilt.

   Setze gegebenenfalls $F := F \cup \{(g, e)\}$ und $f := h$.

4. Abbruchbedingung: Ist $\deg(f) = 0$, beende das Verfahren.

   Andernfalls setze mit Schritt 2 fort.

Bemerkungen:

1. Man beachte, dass Teiler g von f, die im Schritt 2 ermittelt werden, irreduzibel sind. Andernfalls besäße ein solcher Teiler einen Teiler h, der dann auch Teiler von f wäre. Als solcher wäre er bereits in einem früheren Verfahrensschritt bestimmt worden.

2. Das Verfahren ist nur dann implementierbar, wenn die Anzahl der Teiler jedes Elements $r \in R$ bis auf Assoziierte endlich ist. Weiter muss für den Ring R ein implementierbares Verfahren zur Ermittlung dieser Teiler existieren. Dies ist zum Beispiel der Fall für

   - $R = \mathbb{Z}$: Hier gilt für alle Teiler s einer Zahl r die Ungleichung $|s| \leq |r|$ und es gibt nur endlich viele Teiler.
   - $R = \mathbb{F}_q[Y]$: Hier gilt für jeden Teiler s eines Polynoms r die Ungleichung $\deg(s) \leq \deg(r)$ und es gibt nur endlich viele Teiler.

   Mit dem Kronecker-Verfahren lassen sich also rekursiv Polynome in $\mathbb{Z}[X_1, \ldots, X_n]$ und in $\mathbb{F}_q[X_1, \ldots, X_n]$ faktorisieren.

3. Der Rechenaufwand des Kronecker-Verfahrens ist abhängig vom Grad sehr hoch. Es handelt sich im Fall eines konkreten Integritätsbereichs R eher um das schlechteste vorhandene Verfahren. Insbesondere gibt es für die Faktorisierung von Polynomen mit ganzzahligen Koeffizienten oder solchen in endlichen Körpern weit bessere Verfahren.

Literatur

[Gau] C.F. Gauß: *Disquisitiones Arithmeticae*, Leipzig 1801.

[H-P-S] J. Hoffstein, J. Pipher, J. H. Silverman: *An Introduction to Mathematical Cryptography*, Springer 2008.

[K-M] C. Karpfinger, K. Meyberg, *Algebra: Gruppen – Ringe – Körper*, Springer-Spektrum 2013.

[Mac] F. J. MacWilliams: *The Theory of Error-Correcting Codes*, North Holland 1988.

[BHA] S. Bai, M. R. Hansen, T. O. Andersen: *Modelling of a special class of spherical parallel manipulators with Euler parameters*, Robotica Volume 27 (2009), 161–170.