Die Vermutung von Casas-Alvero

Bachelorarbeit
in der Studienrichtung Technische Mathematik

Johanna Lercher

verfasst im Rahmen der Lehrveranstaltung
Seminar mit Bachelorarbeit, SE 2

Betreuer:
Univ.-Prof. Dr. Tim Netzer

Universität Innsbruck

8. September 2016

Inhaltsverzeichnis

Einleitung

Im Jahr 2001 äußerte *Eduardo Casas-Alvero* eine Vermutung über das Aussehen bestimmter Polynome, deren Koeffizienten in einem Körper $\mathbb{K}$ liegen. Er vertrat die Ansicht, dass ein Polynom $f \in \mathbb{K}[X]$ vom Grad d genau dann mit all seinen Ableitungen einen nichttrivialen Faktor gemeinsam hat, wenn es nur eine einzige Nullstelle von Vielfachheit d besitzt. Diese Behauptung wurde bis heute weder bewiesen noch vollständig widerlegt. Einzig und allein in Polynomringen über Körpern mit positiver Charakteristik wurden Gegenbeispiele gefunden. Aus diesem Grund nennt man *Casas-Alveros* Annahme heute auch die *Vermutung von Casas-Alvero*.

Im Laufe der Jahre haben sich einige Mathematiker mit der *Vermutung von Casas-Alvero* beschäftigt. So ist es beispielsweise *Gema Diaz-Toca* und *Laureano Gonzalez-Vega* im Jahr 2005 gelungen, die Vermutung für Polynome bis Grad 7 zu beweisen, deren Koeffizienten in Körpern der Charakteristik 0 liegen.
Der wohl wichtigste Fortschritt im Zusammenhang mit der Vermutung gelang den vier Mathematikern *Hans-Christian Graf von Bothmer*, *Oliver Labs*, *Josef Schicho* und *Christiaan van de Woestijne* im Jahr 2006. Sie wiesen nach, dass die Vermutung für Polynome mit Koeffizienten in Körpern der Charakteristik 0 gilt, falls der Grad der betrachteten Polynome eine Primzahlpotenz beziehungsweise das Doppelte einer Primzahlpotenz ist. Der Beweis dafür erfolgte unter Zuhilfenahme von *projektiven Schemata*, eines Begriffs aus der *algebraischen Geometrie*. Zudem gelang es ihnen zu beweisen, dass die Behauptung für diese Grade dann auch bis auf endlich viele Primzahlen p in Polynomringen über Körpern mit Primzahlcharakteristik p gilt.
Schlussendlich fanden *Jan Draisma* und *Johan P. de Jong* im Jahr 2011 einen ähnlichen Beweis, der die Gültigkeit der Vermutung für Polynome $f \in \mathbb{C}[X]$ auch noch für das Dreifache (im Fall $p > 3$) beziehungsweise Vierfache (im Fall $p > 4$ und $p \neq 7$) einer Primzahlpotenz p^k, $k \in \mathbb{N}$, zeigte. Anstelle von *projektiven Schemata*

verwendeten sie *Bewertungstheorie*.

In der vorliegenden Arbeit sollen dem Leser die wichtigsten Ideen im Zusammenhang mit der *Vermutung von Casas-Alvero* nähergebracht und außerdem aufgezeigt werden, welch interessante mathematische Konzepte hinter der scheinbar einfachen Aussage stecken. Vorrangig orientiert sich die Arbeit am Artikel *The Casas-Alvero Conjecture for infinitely many degrees* [**GvBL+07**] von *H.-C. Graf von Bothmer et al*. Hauptziel der Arbeit soll es sein, den Inhalt des Artikels nachzuvollziehen und dessen wichtigste Ideen genauer zu beschreiben. Jedoch wird der Begriff eines *projektiven Schemas* hier außen vor gelassen und ein alternativer Zugang gewählt.

Im ersten Kapitel wird die *Vermutung von Casas-Alvero* genauer erläutert. Es wird aufgezeigt, welche vereinfachenden Annahmen getroffen werden können, sodass die Voraussetzung für die Vermutung immer noch gilt. Im zweiten Teil des Kapitels wird die Vermutung unter Zuhilfenahme der *Resultante* zweier Polynome etwas umformuliert.

Im zweiten Kapitel der Arbeit wird ein wichtiger Satz formuliert und bewiesen, der den Grundstein für die weiteren Beweisschritte legt. Falls die *Vermutung von Casas-Alvero* für einen festen Grad d und eine beliebige Primzahl l für Polynome mit Koeffizienten im Körper $\overline{\mathbb{F}}_l$ stimmt, so garantiert der Satz zudem die Gültigkeit der Vermutung für Polynome desselben Grades mit Koeffizienten in algebraisch abgeschlossenen Körpern der Charakteristik 0 und bis auf endlich viele Primzahlen p in algebraisch abgeschlossenen Körpern mit Primzahlcharakteristik p.
Um den Beweis dieses Satzes führen zu können, sind einige Vorbereitungen notwendig. Deshalb wird in einem eigenen Kapitel genauer auf *Hilberts Nullstellensatz* und den Begriff eines *graduierten Ringes* eingegangen. Des Weiteren wird beschrieben, auf welche Weise das sogenannte *Ultraprodukt der Körper* $\overline{\mathbb{F}}_p$ gebildet werden kann und weshalb dieses *Ultraprodukt* für den Beweis des Satzes wichtig ist. Unter Zuhilfenahme dieses *Ultraprodukts* wird schlussendlich der Hauptsatz des Kapitels gezeigt.

Im dritten Kapitel wird die *Vermutung von Casas-Alvero* in Anlehnung an [**GvBL+07**] und unter Zuhilfenahme des Hauptsatzes des zweiten Kapitels für Polynome mit

Koeffizienten in Körpern der Charakteristik 0, deren Grad eine Primzahlpotenz oder das Doppelte einer Primzahlpotenz ist, bewiesen. Der Hauptsatz garantiert zudem die Gültigkeit der Vermutung bis auf endlich viele Primzahlen p für Polynome desselben Grades in algebraisch abgeschlossenen Körpern der Charakteristik p.

In einem letzten Kapitel der Arbeit wird aufgezeigt, dass für jeden Körper $\mathbb{K}$ mit $\mathrm{char}(\mathbb{K}) \neq 0$ Polynome $f \in \mathbb{K}[X]$ existieren, für die die *Vermutung von Casas-Alvero* nicht stimmt. In Körpern der Charakteristik 0 wurden solche Polynome bis heute nicht gefunden.

An dieser Stelle sei erwähnt, dass die Kapitel 1, 3 und 4 dieser Arbeit dem Artikel [**GvBL+07**] folgen. Die wichtigsten Ideen und Sätze der erwähnten Kapitel sind diesem zuzuschreiben, werden in der vorliegenden Bachelorarbeit genauer erläutert und oft mithilfe von Beispielen untermauert. Auch jener wichtige Satz, der im zweiten Kapitel der Arbeit gezeigt wird, wurde erstmals in [**GvBL+07**] formuliert und bewiesen. Die vorliegende Arbeit illustriert aber eine etwas andere Möglichkeit, den Satz zu beweisen.

An dieser Stelle möchte ich meinem Betreuer, Herrn Univ.-Prof. Dr. Tim Netzer, für seine maßgebliche Unterstützung zum Gelingen dieser Bachelorarbeit danken.

KAPITEL 1

Die Vermutung von Casas-Alvero

Die *Vermutung von Casas-Alvero* lautet wie folgt:

> Sei $\mathbb{K}$ ein Körper und $\mathbb{K}[X]$ der univariate Polynomring über $\mathbb{K}$. Weiters sei $f \in \mathbb{K}[X]$ ein Polynom vom Grad $d \geqslant 1$ und $f^{(i)}$ dessen i-te formale Ableitung. Dann sind folgende Aussagen äquivalent:
>
> $$\begin{aligned} &(1) \quad \forall i \in \{1, \ldots, d-1\} : \mathrm{ggT}(f, f^{(i)}) \neq 1 \\ &(2) \quad f = c(X-a)^d \quad \text{für } c, a \in \mathbb{K},\ c \neq 0 \end{aligned} \tag{1.1}$$

Man kann schnell zeigen, dass die Implikationsrichtung (2) $\Rightarrow$ (1) stimmt. Denn besitzt ein Polynom $f \in \mathbb{K}[X]$ das Aussehen $f = c(X-a)^d$, so gilt:

$$\begin{aligned} f' &= c \cdot d \cdot (X-a)^{d-1} \\ f'' &= c \cdot d \cdot (d-1) \cdot (X-a)^{d-2} \\ &\vdots \\ f^{(d-1)} &= c \cdot d \cdot (d-1) \cdot \ldots \cdot 2 \cdot (X-a) \end{aligned}$$

Falls nun $\mathrm{char}(\mathbb{K}) = 0$ oder $\mathrm{char}(\mathbb{K}) = p > d$ gilt, so teilt das Polynom f mit all seinen Ableitungen den gemeinsamen Faktor $(X-a)$.

Im Falle $\mathrm{char}(\mathbb{K}) = p$ für eine Primzahl $p \leqslant d$ werden die formalen Ableitungen ab einem gewissen Index konstant 0. Für diese Ableitungen gilt $\mathrm{ggT}(f, 0) = c^{-1} f$. Die restlichen Ableitungen besitzen mit f den gemeinsamen Faktor $(X-a)$.

Dadurch ist die Implikation (2) $\Rightarrow$ (1) bewiesen. Deshalb wird im Folgenden nur noch die andere Implikationsrichtung betrachtet.

VEREINFACHENDE ANNAHMEN

Sei nun $f = a_dX^d + \ldots + a_1X + a_0 \in \mathbb{K}[X]$ ein Polynom, das die Bedingung (1) der *Casas-Alvero Vermutung* (1.1) erfüllt. Folgende vereinfachende Annahmen können getroffen werden (vgl. dazu z.B. [**GvBL+07**], S. 225 f.):

(1) Da zu jedem Körper $\mathbb{K}$ ein algebraisch abgeschlossener Erweiterungskörper existiert, kann man annehmen, dass es sich bei $\mathbb{K}$ um einen algebraisch abgeschlossenen Körper handelt. Weil f über einem solchen Körper in Linearfaktoren zerfallen muss, wird die Aussage $\mathrm{ggT}(f, f^{(i)}) \neq 0$ $\forall i \in \{1, \ldots, d-1\}$ durch die Bedingung ersetzt, dass f mit all seinen Ableitungen eine gemeinsame Nullstelle besitzt.

(2) Zudem bietet es sich an, anstelle der i-ten formalen Ableitung des Polynoms f dessen *i-te Hasse-Ableitung* zu verwenden. Dazu folgende Definition:

Definition 1.1: Sei $f = a_dX^d + \ldots + a_1X + a_0$ ein Polynom in $\mathbb{K}[X]$. Dann heißt

$$f_i := \binom{d}{i} a_dX^{d-i} + \binom{d-1}{i} a_{d-1}X^{d-i-1} + \ldots + \binom{i}{i} a_i$$

die *i-te Hasse-Ableitung* von f.

Man kann leicht zeigen, dass die Beziehung $f_i = \frac{f^{(i)}}{i!}$ gilt. Ersetzt man $f^{(i)}$ in Körpern der Charakteristik 0 also durch die *i-te Hasse-Ableitung* f_i, so ändert das nichts an Bedingung (1) der *Casas-Alvero Vermutung* (1.1). Rechnet man aber in Körpern mit Primzahlcharakteristik, so garantiert die *i-te Hasse-Ableitung* viel bessere Eigenschaften als die formale Ableitung. Denn während die i-ten formalen Ableitungen in Körpern der Charakteristik

p für Polynome vom Grad $d \geqslant p$ ab einem gewissen Index immer verschwinden, muss das bei der i*-ten Hasse-Ableitung* nicht der Fall sein. Das wird aus folgendem Beispiel ersichtlich:

Beispiel 1.2: Sei $f = X^4 + X^3 + 1 \in \overline{\mathbb{F}}_2[X]$. Es gilt:

$$f^{(3)} = 24X + 6 = 0$$
$$f_3 = 4X + 1 \neq 0$$

Aufgrund der Tatsache, dass die Beziehung $f_i = \frac{f^{(i)}}{i!}$ gilt, folgt aus der Existenz gemeinsamer Nullstellen von f mit all seinen *Hasse-Ableitungen* auch die Existenz gemeinsamer Nullstellen von f mit all seinen formalen Ableitungen. Um zu verhindern, dass die Ableitungen ab einem gewissen Index konstant 0 werden, wird die Voraussetzung der *Vermutung von Casas-Alvero* etwas verschärft, indem die formalen Ableitungen durch die *Hasse-Ableitungen* ersetzt werden.

(3) Des Weiteren können ohne Beschränkung der Allgemeinheit $a_d = 1$ und $a_0 = 0$ gesetzt werden. Denn durch Normierung beziehungsweise Verschiebung einer Nullstelle in den Nullpunkt bleibt die Bedingung (1) der *Casas-Alvero Vermutung* (1.1) trotzdem gültig.

All diese Vereinfachungen führen zu folgender Definition:

Definition 1.3: Sei $\mathbb{K}$ ein algebraisch abgeschlossener Körper und $f \in \mathbb{K}[X]$ ein Polynom der Form

$$f = X^d + a_{d-1}X^{d-1} + \ldots + a_1X$$

f heißt *Casas-Alvero Polynom*

$$:\Leftrightarrow \forall i \in \{1, \ldots, d-1\} \exists c_i \in \mathbb{K} : (X - c_i) | f \wedge (X - c_i) | f_i \qquad (1.2)$$

Die Bedingung (1.2) wird auch *Casas-Alvero Bedingung* genannt. Im Folgenden wird die *Casas-Alvero Bedingung* mithilfe der *Resultante von Polynomen* etwas umgeschrieben.

DIE RESULTANTE VON POLYNOMEN

Im Folgenden sei $\mathbb{K}$ immer ein algebraisch abgeschlossener Körper.

Definition 1.4: Seien $f = a_m X^m + \ldots + a_0 \in \mathbb{K}[X]$ und $g = b_n X^n + \ldots + b_0 \in \mathbb{K}[X]$ zwei Polynome mit $\deg(f) = m$ und $\deg(g) = n$. Dann heißt

$$\mathrm{Res}(f,g) := \det \begin{pmatrix} a_m & a_{m-1} & a_{m-2} & \ldots & a_1 & a_0 & 0 & 0 & \ldots & 0 \\ 0 & a_m & a_{m-1} & a_{m-2} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\ 0 & 0 & a_m & a_{m-1} & a_{m-2} & \ldots & a_1 & a_0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & a_m & a_{m-1} & a_{m-2} & \ldots & a_1 & a_0 \\ b_n & b_{n-1} & b_{n-2} & \ldots & b_1 & b_0 & 0 & 0 & \ldots & 0 \\ 0 & b_n & b_{n-1} & b_{n-2} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ 0 & 0 & b_n & b_{n-1} & b_{n-2} & \ldots & b_1 & b_0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & b_n & b_{n-1} & b_{n-2} & \ldots & b_1 & b_0 \end{pmatrix}$$

die *Resultante* von f und g. Es handelt sich dabei um die Determinante einer $(m+n) \times (m+n)$-Matrix. Die ersten n Zeilen der Matrix bestehen aus den Koeffizienten von f, die weiteren m Zeilen aus den Koeffizienten von g. Man nennt die obige Matrix auch *Sylvestermatrix*.

Die *Resultante* zweier Polynome besitzt einige nützliche Eigenschaften. Eine sehr wichtige Eigenschaft sei in folgendem Lemma erwähnt:

Lemma 1.5: Seien $f = a_m X^m + \ldots + a_0$ und $g = b_n X^n + \ldots + b_0$ zwei Polynome in $\mathbb{K}[X]$. Dann gilt:

$$\mathrm{Res}(f,g) \in \mathbb{Z}[a_0,\ldots,a_m,b_0,\ldots,b_n] \tag{1.3}$$

Beweis: Diese Eigenschaft folgt direkt aus der *Leibniz-Formel* für Determinanten. Sei S die Sylvestermatrix von f und g. Dann gilt:

$$\mathrm{Res}(f,g) = \det(S) = \sum_{\sigma \in S_{n+m}} \mathrm{sign}(\sigma) S_{\sigma(1)1} \ldots S_{\sigma(m+n)m+n}$$

Aus $\mathrm{sign}(\sigma) \in \{-1,1\} \subseteq \mathbb{Z}$ und der Tatsache, dass die Einträge von S nur aus Nullen und den Koeffizienten der beiden Polynome bestehen, folgt die Behauptung. □

Es gilt folgender Satz, der für die *Vermutung von Casas-Alvero* von zentraler Bedeutung ist:

Satz 1.6: Seien $f,g \in \mathbb{K}[X]$ zwei Polynome mit $1 \leqslant \deg(f) = m$ und $1 \leqslant \deg(g) = n$. Dann gilt:

$$\mathrm{Res}(f,g) = 0 \Leftrightarrow \mathrm{ggT}(f,g) \neq 1 \Leftrightarrow \text{ } f \text{ und } g \text{ besitzen eine gemeinsame Nullstelle}$$

Beweis: Vgl. z.B. [**Fi11**], S. 297 f. Die zweite Äquivalenz gilt, weil es sich bei $\mathbb{K}$ um einen algebraisch abgeschlossenen Körper handelt. □

Unter Zuhilfenahme der *Resultante* ist es nun möglich, die Voraussetzung (1) der *Casas-Alvero Vermutung* (1.1) wie folgt umzuformulieren (Idee nach [**GvBL+07**], S. 226):

Sei $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X$ ein Polynom. Laut **Satz 1.6** ist f genau dann ein *Casas-Alvero Polynom*, wenn gilt:

$$\forall i \in \{1,\ldots,d-1\} : \mathrm{Res}(f,f_i) = 0 \tag{1.4}$$

Da die Koeffizienten des Polynoms f und seiner i*-ten Hasse-Ableitung* f_i bis auf ganzzahlige Vielfache dieselben sind, gilt wegen **Lemma 1.5** zudem:

$$\forall i \in \{1, \ldots, d-1\} : \mathrm{Res}(f, f_i) \in \mathbb{Z}[a_1, \ldots, a_{d-1}] \tag{1.5}$$

Definition 1.7: Sei $\mathbb{Z}[X_1, \ldots, X_{d-1}]$ der multivariate Polynomring über $\mathbb{Z}$ in $d-1$ Variablen. Für Polynome der Form $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X \in \mathbb{K}[X]$ und $i = 1, \ldots, d-1$ definiere die Polynome $P_i \in \mathbb{Z}[X_1, \ldots, X_{d-1}]$ durch

$$P_i(a_1, \ldots, a_{d-1}) = \mathrm{Res}(f, f_i) \tag{1.6}$$

Mithilfe der Polynome $P_1, \ldots, P_{d-1}$ kann nun ein homogenes polynomiales Gleichungssystem betrachtet werden. Von Interesse für die *Vermutung von Casas-Alvero* sind jene Elemente $(a_1, \ldots, a_{d-1}) \in \mathbb{K}^{d-1}$, die für alle $i \in \{1, \ldots, d-1\}$ die Bedingung $P_i(a_1, \ldots, a_{d-1}) = 0$ erfüllen. Denn diese Elemente sind wegen (1.6) und (1.4) Koeffizienten von *Casas-Alvero Polynomen* vom Grad d. Deshalb betrachte folgende Lösungsmenge:

$$\mathcal{V}(\mathbb{K}, d) = \{(a_1, \ldots, a_{d-1}) \in \mathbb{K}^{d-1} : P_i(a_1, \ldots, a_{d-1}) = 0 \quad \forall i \in \{1, \ldots, d-1\}\} \tag{1.7}$$

Bemerkung 1.8: Will man die *Vermutung von Casas-Alvero* für ein *Casas-Alvero Polynom* $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X$ vom Grad d beweisen, so muss man aufgrund der Tatsache, dass $a_0 = 0$ und $a_d = 1$ gesetzt wurden, nur Folgendes zeigen:

$$f = X^d \quad \text{also:} \quad a_{d-1} = \ldots = a_1 = 0 \tag{1.8}$$

Will man die Gültigkeit der *Vermutung von Casas-Alvero* für alle *Casas-Alvero Polynome* eines festen Grades d überprüfen, so darf in der oben betrachteten Lösungsmenge (1.7) einzig und allein der Nullvektor aus $\mathbb{K}^{d-1}$ enthalten sein. Es muss also gelten:

$$\mathcal{V}(\mathbb{K}, d) = \{(0, \ldots, 0)\} \tag{1.9}$$

Bemerkung 1.9: Die Idee, Koeffizienten von *Casas-Alvero Polynomen* eines festen Grades d als Elemente der Lösungsmenge des oben betrachteten homogenen polynomialen Gleichungssystems zu betrachten, stammt aus [**GvBL+07**], S. 226. Im erwähnten Artikel wurde mit dessen Hilfe ein *gewichtet projektives Schema* konstruiert und gezeigt, dass die *Vermutung von Casas-Alvero* für Polynome eines festen Grades d genau dann erfüllt ist, wenn dieses Schema keine Elemente enthält (vgl. [**GvBL+07**], S. 227, Proposition 2.1). Auf diesen Gedanken basiert **Bemerkung 1.8**.

Die *Vermutung von Casas-Alvero* wurde also unter Zuhilfenahme der *Resultante* derart vereinfacht, dass für den Beweis der Vermutung für einen festen Grad d nur die Bedingung (1.9) gezeigt werden muss. Um dieser Tatsache für Polynome, deren Grad eine Primzahlpotenz beziehungsweise das Doppelte einer Primzahlpotenz ist, etwas näherzukommen, bedarf es eines wichtigen Satzes, dem ob seiner bemerkenswerten Aussagekraft ein ganzes Kapitel gewidmet wird.

KAPITEL 2

Einer für (fast) alle

Ein sehr wichtiger Satz im Zusammenhang mit der *Vermutung von Casas-Alvero* lautet wie folgt:

Hauptsatz (nach [**GvBL+07**], S. 226, Proposition 2.2)**:** Sei $d \geqslant 1$ eine positive ganze Zahl. Für eine Primzahl l sei die *Vermutung von Casas-Alvero* für Polynome vom Grad d in $\overline{\mathbb{F}}_l[X]$ erfüllt, das heißt:

$$\mathcal{V}(\overline{\mathbb{F}}_l, d) = \{(0, \ldots, 0)\}$$

Dann gilt die Vermutung für diesen Grad auch für Polynome mit Koeffizienten in algebraisch abgeschlossenen Körpern der Charakteristik 0 und bis auf endlich viele Primzahlen p auch in algebraisch abgeschlossenen Körpern der Charakteristik p.

Bemerkung 2.1: Die Aussagekraft des obigen Satzes ist enorm. Denn will man die *Vermutung von Casas-Alvero* für einen festen Grad d in Charakteristik 0 beweisen, so erlaubt es der Satz, stattdessen für eine beliebige Primzahl l in Charakteristik l zu rechnen. Das Rechnen in positiver Charakteristik bringt einige Vorteile mit sich. Diese werden in Kapitel 3 für die *Vermutung von Casas-Alvero* verdeutlicht.

Im Artikel [**GvBL+07**] wird der **Hauptsatz** mithilfe *projektiver Schemata* bewiesen. Die vorliegende Arbeit illustriert einen alternativen Beweis unter Zuhilfenahme einer Version von *Hilberts Nullstellensatz*.

1. Hilberts Nullstellensatz

Bevor die Aussage von *Hilberts Nullstellensatz* näher erläutert wird, bedarf es noch einiger Vorbereitungen. Dazu sei im Folgenden k ein beliebiger Körper und $\mathbb{K}$ ein algebraisch abgeschlossener Erweiterungskörper von k. Des Weiteren sei $k[X_1, \ldots, X_n]$ der multivariate Polynomring über k in n Variablen.

Alle mathematischen Grundlagen, die für dieses Kapitel notwendig sind, wurden [**Ne16**], Kapitel 1.1 und Kapitel 1.2, entnommen.

Definition 2.1.1: Sei $\mathcal{P} \subseteq k[X_1, \ldots, X_n]$ eine Menge von Polynomen. Dann heißt

$$\mathcal{V}(\mathcal{P}) := \{a \in \mathbb{K}^n : p(a) = 0 \quad \forall p \in \mathcal{P}\} \tag{2.1}$$

die *von $\mathcal{P}$ definierte affine Varietät*. $\mathcal{V}(\mathcal{P})$ beschreibt die Lösungsmenge des von $\mathcal{P}$ definierten polynomialen Gleichungssystems.

Bemerkung 2.1.2: Weil $\mathbb{Z}$ als Teilmenge einer der beiden möglichen Primkörper $k = \mathbb{Q}$ beziehungsweise $k = \mathbb{F}_p$ aufgefasst werden kann, ist auch $\mathcal{V}(\mathbb{K}, d)$ aus (1.7) eine affine Varietät. Sie wird von der Menge $\{P_1, \ldots, P_{d-1}\} \subseteq k[X_1, \ldots, X_{d-1}]$ definiert. Als algebraisch abgeschlossener Erweiterungskörper fungiert gerade jener Körper, für den die *Vermutung von Casas-Alvero* gezeigt werden soll.

Lemma 2.1.3: Sei $\mathcal{P} \subseteq k[X_1, \ldots, X_n]$ und $I = \langle \mathcal{P} \rangle$ das von $\mathcal{P}$ erzeugte Ideal in $k[X_1, \ldots, X_n]$. Dann gilt:

$$\mathcal{V}(\mathcal{P}) = \mathcal{V}(I) \tag{2.2}$$

Beweis: Wegen $\mathcal{P} \subseteq I$ gilt $\mathcal{V}(I) \subseteq \mathcal{V}(\mathcal{P})$. Sei nun $a \in \mathcal{V}(\mathcal{P})$. Dann gilt $\forall p \in \mathcal{P} : p(a) = 0$. Wähle $f \in I$. Dann gibt es Polynome $f_i \in k[X_1, \ldots, X_n]$ und $p_i \in \mathcal{P}$ mit:

$$f = \sum_i f_i p_i \quad \text{und deshalb} \quad f(a) = \sum_i f_i(a) p_i(a) \overset{\forall i:\ p_i(a)=0}{=} 0$$

□

Definition und Satz 2.1.4: Sei $V \subseteq \mathbb{K}^n$ eine beliebige Teilmenge. Die Menge

$$\mathcal{I}(V) := \{p \in k[X_1, \ldots, X_n] : p(a) = 0 \quad \forall a \in V\} \tag{2.3}$$

ist ein Ideal in $k[X_1, \ldots, X_n]$ und heißt das *Verschwindungsideal von* V.

Beweis: Offensichtlich ist das Nullpolynom in der Menge enthalten. Des Weiteren gilt für $f, g \in \mathcal{I}(V)$, $h \in k[X_1, \ldots, X_n]$ und $a \in V$:

$$\begin{aligned}(f+g)(a) &= \underbrace{f(a)}_{=0} + \underbrace{g(a)}_{=0} = 0\\ (h \cdot f)(a) &= h(a) \cdot \underbrace{f(a)}_{=0} = 0\end{aligned}$$

□

Definition und Satz 2.1.5: Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Die Menge

$$\sqrt{I} := \{a \in R : \exists n \in \mathbb{N} : a^n \in I\} \tag{2.4}$$

ist wieder ein Ideal von R und heißt *Radikal* von I.

Beweis: Für den Beweis müssen erneut die drei Eigenschaften eines Ideals nachgewiesen werden:

(1) $\forall n \in \mathbb{N} : 0^n = 0 \in I \Rightarrow 0 \in \sqrt{I}$
(2) Es seien $x, y \in \sqrt{I}$, also $x^r, y^s \in I$ für $r, s \in \mathbb{N}$. Dann gilt:

$$\begin{aligned}(x+y)^{r+s} &= \sum_{i=0}^{r+s} \binom{r+s}{i} x^i y^{r+s-i} =\\ &= \underbrace{\sum_{i=0}^{r-1} \binom{r+s}{i} x^i y^{r+s-i}}_{(*)} + \underbrace{\sum_{i=r}^{r+s} \binom{r+s}{i} x^i y^{r+s-i}}_{(\triangle)}\end{aligned}$$

Für $i \geqslant r$ gilt $x^i = x^{i-r}x^r \in I$ wegen $x^{i-r} \in R$ und $x^r \in I$. Aufgrund der Tatsache, dass I ein Ideal ist, muss dann auch $(\triangle)$ in I liegen.

Für $i < r$ muss mit derselben Argumentation wie oben $y^{r+s-i} = y^{r-i}y^s \in I$ liegen und aufgrund der Tatsache, dass I ein Ideal ist, gilt dann $(*) \in I$.

Anwendung von Eigenschaft (2) eines Ideals liefert dann $(x+y)^{r+s} \in I$ und somit $x + y \in \sqrt{I}$.

(3) Sei nun $a \in R$ und $x \in \sqrt{I}$, also $x^r \in I$ für ein $r \in \mathbb{N}$. Dann gilt:

$$(ax)^r = \underbrace{a^r}_{\in R}\underbrace{x^r}_{\in I} \overset{I \text{ Ideal}}{\in} I$$

Daraus folgt $ax \in \sqrt{I}$.

□

Mithilfe dieser Vorbereitungen kann nun eine Version von *Hilberts Nullstellensatz* formuliert werden:

Satz 2.1.6 (Hilberts Nullstellensatz): Für jedes Ideal $I \subseteq k[X_1, \ldots, X_n]$ gilt:

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} \tag{2.5}$$

Beweis: Vgl. z.B. [**Ne16**], S. 12 f.

Die Nützlichkeit dieses Satzes für die *Vermutung von Casas-Alvero* wird nun kurz beschrieben. Sei ab jetzt k immer einer der möglichen Primkörper und $\mathbb{K}$ ein algebraisch abgeschlossener Körper (inbesondere ein Erweiterungskörper von k). Laut (1.9) gilt die *Vermutung von Casas-Alvero* für Polynome vom Grad d in $\mathbb{K}[X]$ genau dann, wenn

$$\mathcal{V}(\mathbb{K}, d) = \{(0, \ldots, 0)\}$$

Wegen (2.2) gilt für $I = \langle P_1, \ldots, P_{d-1}\rangle \subseteq k[X_1, \ldots, X_{d-1}]$:

$$\mathcal{V}(\mathbb{K}, d) = \mathcal{V}(I) = \{(0, \ldots, 0)\}$$

Das *Verschwindungsideal* dieser Menge sieht nun wie folgt aus:

$$\mathcal{I}(\mathcal{V}(I)) = \{p \in k[X_1, \ldots, X_{d-1}] : p(0, \ldots, 0) = 0\} \tag{2.6}$$

Man sieht sofort, dass die Polynome $X_1, \ldots, X_{d-1}$ im Ideal (2.6) enthalten sein müssen. Also gilt:

$$X_1, \ldots, X_{d-1} \in \mathcal{I}(\mathcal{V}(I)) \overset{\text{Hilberts Nullstellensatz}}{=} \sqrt{I} \tag{2.7}$$

Aufgrund der Definition (2.4) eines *Radikals* bedeutet das:

$$\forall i \in \{1, \ldots, d-1\} \quad \exists n \in \mathbb{N} : X_i^n \in I = \langle P_1, \ldots, P_{d-1} \rangle \tag{2.8}$$

Wegen *Hilberts Nullstellensatz* erhält man also folgende Implikation:

$$\mathcal{V}(\mathbb{K}, d) = \{(0, \ldots, 0)\} \Rightarrow \forall i \in \{1, \ldots, d-1\} \quad \exists n \in \mathbb{N} : X_i^n \in I \tag{2.9}$$

Es ist leicht einzusehen, dass auch die umgekehrte Implikationsrichtung gilt. Sei dazu $i \in \{1, \ldots, d-1\}$ und $n \in \mathbb{N}$ derart, dass $X_i^n \in I$. Für jedes Element $a \in \mathcal{V}(I)$ muss dann gelten: $X_i^n(a) = 0$. Das heißt:

$$X_i^n \equiv 0 \text{ in } \mathcal{V}(I) \overset{\text{Körper nullteilerfrei}}{\Rightarrow} X_i \equiv 0 \text{ in } \mathcal{V}(I)$$

Damit gilt $\forall a = (a_1, \ldots, a_{d-1}) \in \mathcal{V}(I) : X_i(a) = a_i = 0$. Weil diese Tatsache für jedes $i \in \{1, \ldots, d-1\}$ erfüllt ist, folgt $\mathcal{V}(I) = \mathcal{V}(\mathbb{K}, d) = \{(0, \ldots, 0)\}$.

Unter Zuhilfenahme von *Hilberts Nullstellensatz* wurde gezeigt:

Die *Vermutung von Casas-Alvero gilt für Polynome vom Grad* d

$$\begin{aligned} &\Leftrightarrow \mathcal{V}(\mathbb{K}, d) = \{(0, \ldots, 0)\} \\ &\Leftrightarrow \forall i \in \{1, \ldots, d-1\} \quad \exists n \in \mathbb{N} : X_i^n \in \langle P_1, \ldots, P_{d-1} \rangle \end{aligned} \tag{2.10}$$

Bemerkung 2.1.7: Bei genauerer Betrachtung der rechten Seite der Äquivalenz wird klar, dass diese nicht vom algebraisch abgeschlossenen Oberkörper abhängt, über dem die Varietät definiert wurde. Diese Eigenschaft erlaubt folgenden Rückschluss: Möchte man die *Vermutung von Casas-Alvero* für Polynome eines festen Grades d mit Koeffizienten in einem algebraisch abgeschlossenen Körper $\mathbb{K}$ beweisen, so kann stattdessen auch ein anderer algebraisch abgeschlossener Körper derselben Charakteristik betrachtet werden. Denn diesem Körper liegt derselbe Primkörper zugrunde.
Diese Tatsache bringt einen enormen Nutzen mit sich. Denn falls es gelingt, die *Vermutung von Casas-Alvero* für Polynome eines festen Grades d mit Koeffizienten in einem beliebigen algebraisch abgeschlossenen Körper $\mathbb{K}$ zu beweisen, so folgt daraus die Gültigkeit der Vermutung für Polynome desselben Grades, deren Koeffizienten in einem anderen algebraisch abgeschlossenen Körper derselben Charakteristik liegen.

Für den Beweis des **Hauptsatzes** wird im Folgenden noch der Begriff eines *graduierten Ringes* eingeführt.

2. Graduierte Ringe

Alle mathematischen Grundlagen, die für dieses Kapitel notwendig sind, wurden [**Ne16**], Kapitel 2.2, entnommen.

Sei $(G, +, 0)$ eine abelsche Gruppe.

Definition 2.2.1: Ein Ring R zusammen mit einer additiven Untergruppe $R_g \subseteq R$ für jedes $g \in G$ heißt *G-graduierter Ring*

$$:\Leftrightarrow \quad R = \bigoplus_{g \in G} R_g \quad \text{und} \quad \forall g, h \in G : R_g \cdot R_h \subseteq R_{g+h} \tag{2.11}$$

Ein Element $a \in R$ heißt *homogen*, falls $a \in R_g$ für ein $g \in G$ gilt. Falls $a \neq 0$ ist, nennt man in diesem Fall $\deg(a) = g$ den *Grad* von a. Man setzt $\deg(0) = -\infty$.

Bemerkung 2.2.2: Jedes $a \in R$ besitzt die eindeutige Darstellung

$$a = \sum_{g \in G} a_g$$

mit homogenen Elementen $a_g \in R$ vom *Grad* g und $a_g = 0$ bis auf endlich viele $g \in G$. a_g heißt die *homogene Komponente vom Grad g von a*.

Beispiel 2.2.3 (Standardgraduierung): Sei k ein Körper und $R = k[X_1, \ldots, X_n]$. Für $d \in \mathbb{Z}$ mit $d \geqslant 0$ definiere

$$R_d := \{ \sum_{\alpha_1 + \ldots + \alpha_n = d} p_{\alpha_1 \ldots \alpha_n} X_1^{\alpha_1} \ldots X_n^{\alpha_n} : \quad p_{\alpha_1 \ldots \alpha_n} \in k \}$$

Für $d < 0$ setze $R_d := 0$. Diese $\mathbb{Z}$-Graduierung heißt *Standardgraduierung* von $k[X_1, \ldots, X_n]$.

Beispiel 2.2.4 (Gewichtete Grad-Graduierung): Sei wie oben k ein Körper und $R = k[X_1, \ldots, X_n]$. Für $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}^n$ und $d \in \mathbb{Z}$ mit $d \geqslant 0$ definiere

$$R_d := \{ \sum_{\alpha_1 \gamma_1 + \ldots + \alpha_n \gamma_n = d} p_{\alpha_1 \ldots \alpha_n} X_1^{\alpha_1} \ldots X_n^{\alpha_n} : \quad p_{\alpha_1 \ldots \alpha_n} \in k \}$$

Wie vorher setze $R_d := 0$ für $d < 0$. Diese $\mathbb{Z}$-Graduierung heißt *gewichtete Grad-Graduierung* von $k[X_1, \ldots, X_n]$. Man sieht gut, dass $\deg(X_i) = \gamma_i$ gilt. Die Zahlen γ_i werden oft als *Gewichte* bezeichnet.

Beispiel 2.2.5: Sei $f = 7X^3Y^3 + X^2Y^6 + X^4 \in \mathbb{Q}[X, Y]$. Versieht man $\mathbb{Q}[X, Y]$ für $\gamma = (3, 1)$ mit der *gewichteten Grad-Graduierung*, so ist f homogen vom *Grad* $\deg(f) = 12$.

Bemerkung 2.2.6: Für $\gamma = (\gamma_1, \ldots, \gamma_n)$ sei $k[X_1, \ldots, X_n]$ mit der *gewichteten Grad-Graduierung* versehen. Zudem seien $f \in k[X_1, \ldots, X_n]$ und $\mathbb{K}$ ein algebraisch abgeschlossener Erweiterungskörper von k. Man kann zeigen, dass f genau dann homogen vom Grad d ist, wenn für alle $x \in \mathbb{K}^n$ und für alle $\lambda \in \mathbb{K}$ gilt:

$$f(\lambda^{\gamma_1} x_1, \ldots, \lambda^{\gamma_n} x_n) = \lambda^d f(x_1, \ldots, x_n) = \lambda^d f(\underline{x}) \tag{2.12}$$

Folgender Satz ist für den Beweis des **Hauptsatzes** von zentraler Bedeutung:

Satz 2.2.7: Sei k einer der möglichen Primkörper. Für $\gamma = (d-1, \ldots, 1)$ versehe $k[X_1, \ldots, X_{d-1}]$ mit der *gewichteten Grad-Graduierung*. Damit gilt: $\deg(X_i) = d - i$.

Dann ist $P_i \in k[X_1, \ldots, X_{d-1}]$ homogen vom Grad $d(d-i)$.

Beweis:

Für ein $\lambda \in \mathbb{K}$ muss laut **Bemerkung 2.2.6** Folgendes gezeigt werden:

$$P_i(\lambda^{d-1} a_1, \ldots, \lambda a_{d-1}) = \lambda^{d(d-i)} P_i(a_1, \ldots, a_{d-1}) \tag{2.13}$$

Für die beiden Polynome

$$f = X^d + a_{d-1} X^{d-1} + \ldots + a_1 X$$

und

$$\tilde{f} = X^d + \lambda a_{d-1} X^{d-1} + \ldots + \lambda^{d-1} a_1 X$$

gilt $P_i(a_1, \ldots, a_{d-1}) = \mathrm{Res}(f, f_i)$ und $P_i(\lambda^{d-1} a_1, \ldots, \lambda a_{d-1}) = \mathrm{Res}(\tilde{f}, \tilde{f}_i)$. Also muss man laut (2.13) zeigen:

$$\mathrm{Res}(\tilde{f}, \tilde{f}_i) = \lambda^{d(d-i)} \mathrm{Res}(f, f_i)$$

Betrachtet man nun die Resultante der Polynome $\tilde{f}$ und $\tilde{f}_i$, so unterscheidet sich deren Sylvestermatrix $\tilde{S}$ von der Sylvestermatrix S der Polynome f und f_i nur durch Potenzen von λ. Die Sylvestermatrix S sieht wie folgt aus:

$$\begin{pmatrix}
1 & a_{d-1} & \dots & a_1 & 0 & 0 & 0 & \dots & 0 \\
0 & 1 & a_{d-1} & \dots & a_1 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & a_{d-1} & \dots & a_1 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
0 & 0 & \dots & 0 & 1 & a_{d-1} & \dots & a_1 & 0 \\
\binom{d}{i} & \binom{d-1}{i}a_{d-1} & \dots & \binom{i+1}{i}a_{i+1} & \binom{i}{i}a_i & 0 & 0 & \dots & 0 \\
0 & \binom{d}{i} & \binom{d-1}{i}a_{d-1} & \dots & \binom{i+1}{i}a_{i+1} & \binom{i}{i}a_i & 0 & \dots & 0 \\
0 & 0 & \binom{d}{i} & \binom{d-1}{i}a_{d-1} & \dots & \binom{i+1}{i}a_{i+1} & \binom{i}{i}a_i & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
0 & 0 & \dots & 0 & \binom{d}{i} & \binom{d-1}{i}a_{d-1} & \dots & \binom{i+1}{i}a_{i+1} & \binom{i}{i}a_i
\end{pmatrix}$$

Folgende Matrix soll verdeutlichen, an welchen Stellen sich $\tilde{S}$ von S durch Potenzen von λ unterscheidet.

$$\begin{pmatrix}
- & \lambda & \dots & \lambda^{d-1} & - & - & - & \dots & - \\
- & - & \lambda & \dots & \lambda^{d-1} & - & - & \dots & - \\
- & - & - & \lambda & \dots & \lambda^{d-1} & - & \dots & - \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
- & - & \dots & - & - & \lambda & \dots & \lambda^{d-1} & - \\
- & \lambda & \dots & \lambda^{d-(i+1)} & \lambda^{d-i} & - & - & - & - \\
- & - & \lambda & \dots & \lambda^{d-(i+1)} & \lambda^{d-i} & - & \dots & - \\
- & - & - & \lambda & \dots & \lambda^{d-(i+1)} & \lambda^{d-i} & \dots & - \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
- & - & \dots & - & - & \lambda & \dots & \lambda^{d-(i+1)} & \lambda^{d-i}
\end{pmatrix}$$

Führe nun folgende Zeilenumformungen an $\tilde{S}$ durch:

$$\tilde{S}_{neu} = A \cdot \tilde{S}$$

wobei

$$A = \mathrm{Diag}(\lambda, \lambda^2, \ldots, \lambda^{d-i}, \lambda, \lambda^2, \ldots, \lambda^d)$$

Wieder soll die folgende Matrix verdeutlichen, wie sich das auf die Potenzen von λ auswirkt:

$$\begin{pmatrix}
\lambda & \lambda^2 & \ldots & \lambda^d & - & - & - & \ldots & - \\
- & \lambda^2 & \lambda^3 & \ldots & \lambda^{d+1} & - & - & \ldots & - \\
- & - & \lambda^3 & \lambda^4 & \ldots & \lambda^{d+2} & - & \ldots & - \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
- & - & \ldots & - & \lambda^{d-i} & \lambda^{d-i+1} & \ldots & \lambda^{2d-i-1} & - \\
\lambda & \lambda^2 & \ldots & \lambda^{d-i} & \lambda^{d-i+1} & - & - & - & - \\
- & \lambda^2 & \lambda^3 & \ldots & \lambda^{d-i+1} & \lambda^{d-i+2} & - & \ldots & - \\
- & - & \lambda^3 & \lambda^4 & \ldots & \lambda^{d-i+2} & \lambda^{d-i+3} & \ldots & - \\
\vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
- & - & \ldots & - & \lambda^d & \lambda^{d+1} & \ldots & \lambda^{2d-i-1} & \lambda^{2d-i}
\end{pmatrix}$$

Dasselbe Ergebnis erreicht man, wenn man an der ursprünglichen Sylvestermatrix S folgende Spaltenumformungen durchführt:

$$S_{neu} = S \cdot B$$

wobei

$$B = \mathrm{Diag}(\lambda, \lambda^2, \ldots, \lambda^{2d-i})$$

Nun gilt:

$$A \cdot \tilde{S} = S \cdot B \Rightarrow \det(A \cdot \tilde{S}) = \det(S \cdot B) \Rightarrow \det(A) \cdot \det(\tilde{S}) = \det(S) \cdot \det(B)$$

Für $\mu := (1 + 2 + \ldots + (d - i)) + (1 + 2 + \ldots + d)$ und $\nu := 1 + 2 + \ldots + 2d - i$ gilt

$$\det(A) = \lambda^\mu \text{ bzw. } \det(B) = \lambda^\nu$$

Das bedeutet:

$$\lambda^{\mu} \cdot \mathrm{Res}(\tilde{f}, \tilde{f}_i) = \lambda^{\nu} \cdot \mathrm{Res}(f, f_i) \Rightarrow \mathrm{Res}(\tilde{f}, \tilde{f}_i) = \lambda^{\nu-\mu}\mathrm{Res}(f, f_i)$$

Wegen $\nu - \mu = d(d-i)$ folgt unmittelbar die Behauptung.

Ein ausführlicher Beweis zu einem ähnlichen Thema findet sich auch in [**Bo06**], S. 300 f.

□

Bemerkung 2.2.8: Das Resultat von **Satz 2.2.7** wurde im Artikel [**GvBL+07**] zur Konstruktion des in Kapitel 1 erwähnten *gewichtet projektiven Schemas* verwendet. Auch für den alternativen Beweis des Hauptsatzes, der in dieser Arbeit geführt wird, ist der obige Satz äußerst nützlich. Denn nun ist es möglich, die Polynome $P_i,\ i = 1, \ldots, d-1,$ als homogene Elemente eines graduierten Ringes anzusehen. Graduierte Ringe bringen einige nützliche Eigenschaften mit sich. Eine oft verwendete Eigenschaft sei in folgendem **Lemma** kurz erwähnt:

Lemma 2.2.9 (nach [**Ne16**], S. 36, Bemerkung 2.2.4)**:** Sei R ein graduierter Ring. Ein Element $a \in R$ besitze die Darstellung

$$a = \sum_i b_i c_i \tag{2.14}$$

Zudem seien a und alle c_i *homogen*. Dann können auch alle b_i als *homogen* angenommen werden, mit

$$\deg(b_i) = \deg(a) - \deg(c_i) \tag{2.15}$$

Beweis: Ersetze alle b_i durch ihre homogenen Summanden vom Grad $\deg(a) - \deg(c_i)$. Wegen

$$R_{\deg(c_i)} \cdot R_{\deg(\mathrm{a})-\deg(c_i)} \subseteq R_{\deg(c_i)+(\deg(a)-\deg(c_i))} = R_{\deg(a)}$$

gilt dann: $c_i b_i \in R_{\deg(a)}$. Dann gilt auch $\sum_i c_i b_i \in R_{\deg(a)}$. Weil a homogen vom Grad $\deg(a)$ ist, muss Gleichung (2.14) auch für die homogenen Summanden gültig bleiben. Das folgt aus der Eindeutigkeit der Darstellung von Elementen eines graduierten Ringes als direkte Summe homogener Elemente.

□

Nun wurden alle Vorbereitungen getroffen, um den **Hauptsatz** des Kapitels beweisen zu können.

3. Beweis des Hauptsatzes

Im Folgenden sei für jeden Primkörper k der Polynomring $k[X_1, \ldots, X_{d-1}]$ mit der Graduierung aus **Satz 2.2.7** versehen.

Sei $d \in \mathbb{N}$ fest gewählt. Laut Voraussetzung des **Hauptsatzes** gibt es eine Primzahl $l \in \mathbb{N}$, sodass die *Vermutung von Casas-Alvero* für Polynome vom Grad d in $\overline{\mathbb{F}}_l[X]$ erfüllt ist.

Um unnötige Schreibarbeit zu vermeiden, wird folgende Abkürzung verwendet: Gilt die *Vermutung von Casas-Alvero* für einen festen Grad d im Polynomring $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$, so wird in Zukunft „CA_d gilt in $\mathbb{K}$“ geschrieben.

Der Beweis des **Hauptsatzes** wird in zwei Schritte unterteilt:

SCHRITT 1: CA_d GILT BIS AUF ENDLICH VIELE PRIMZAHLEN p IN ALGEBRAISCH ABGESCHLOSSENEN KÖRPERN DER CHARAKTERISTIK p.

Dazu betrachte die folgende Menge:

$$\{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\} \tag{2.16}$$

$\mathbb{P}$ bezeichne hier gerade die Menge aller Primzahlen. Es gilt zu zeigen, dass es sich hierbei um eine *koendliche* Menge handelt. In den vorigen Kapiteln wurden genügend Vorbereitungen getroffen, um (2.16) genauer zu analysieren.

$$\{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\} =$$
$$\overset{(1.9)}{=} \{p \in \mathbb{P} : \mathcal{V}(\overline{\mathbb{F}}_p, d) = \{(0, \ldots, 0)\}\}$$
$$\overset{(2.10)}{=} \{p \in \mathbb{P} : \forall i \in \{1, \ldots, d-1\} \quad \exists n \in \mathbb{N} : X_i^n \in \langle P_1, \ldots, P_{d-1}\rangle \text{ in } \mathbb{F}_p[X_1, \ldots, X_{d-1}]\} =$$
$$\overset{(*)}{=} \{p \in \mathbb{P} : \exists n \in \mathbb{N} \quad \forall i \in \{1, \ldots, d-1\} : X_i^n \in \langle P_1, \ldots, P_{d-1}\rangle \text{ in } \mathbb{F}_p[X_1, \ldots, X_{d-1}]\} = (\triangle)$$

Bemerkung 2.3.1: Die Umformung $(*)$ ist aufgrund der Tatsache, dass es sich bei $\langle P_1, \ldots, P_{d-1}\rangle$ um ein Ideal in $\mathbb{F}_p[X_1, \ldots, X_{d-1}]$ handelt, ohne Weiteres möglich.

Nun wird $(\triangle)$ weiter umgeschrieben:

$$(\triangle) = \bigcup_{n \geqslant 1} \{p \in \mathbb{P} : \forall i \in \{1, \ldots, d-1\} : X_i^n \in \langle P_1, \ldots, P_{d-1}\rangle \text{ in } \mathbb{F}_p[X_1, \ldots, X_{d-1}]\}$$
$$= \bigcup_{n \geqslant 1} \{p \in \mathbb{P} : \forall i \in \{1, \ldots, d-1\} : X_i^n = \sum_{j=1}^{d-1} H_{ij} P_j \quad \text{mit } H_{ij} \in \mathbb{F}_p[X_1, \ldots, X_{d-1}]\} = (\triangle)$$

Bemerkung 2.3.2: In **Satz 2.2.7** wurde gezeigt, dass es sich bei allen P_j, $j = 1, \ldots, d-1$, um *homogene* Polynome handelt. Auch X_i^n ist *homogen* vom Grad $(d-i)n$. Wegen **Lemma 2.2.9** können deshalb auch alle $H_{ij},\ j = 1, \ldots, d-1$, als *homogen* vom Grad

$$(d-i)n - \deg(P_j)$$

angenommen werden.

Die Idee besteht nun darin, für beliebiges n

$$\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n} \quad \text{mit } q_n = \sum_{i=1}^{d-1} in$$

zu betrachten. Wegen der oben gewählten Graduierung kann $\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n}$ wie folgt als Vektorraum über $\mathbb{F}_p$ aufgefasst werden:

$$\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n} = {}_{\mathbb{F}_p}\langle X_1^{\alpha_1} \cdot \ldots \cdot X_{d-1}^{\alpha_{d-1}} : (d-1)\alpha_1 + \ldots + 1\alpha_{d-1} = q_n \rangle \quad (2.17)$$

Sei nun p in der Menge (2.16) enthalten. Dann gilt folgende Aussage:

$$\begin{aligned} &\exists n \geqslant 1 : \forall i \in \{1, \ldots, d-1\} : X_i^n = \sum_{j=1}^{d-1} H_{ij} P_j \\ &\text{mit } H_{ij} \in \mathbb{F}_p[X_1, \ldots, X_{d-1}] \textit{ homogen} \text{ vom Grad } (d-i)n - \deg(P_j). \end{aligned} \quad (2.18)$$

Im Folgenden sei ohne Einschränkung der Allgemeinheit

$$(d-1)! \mid n \quad (2.19)$$

erfüllt. Denn falls das nicht gilt, so folgt aus $X_i^n \in \langle P_1, \ldots, P_{d-1} \rangle$ auch $(X_i^n)^{(d-1)!} \in \langle P_1, \ldots, P_{d-1} \rangle$. Hierbei wurde verwendet, dass es sich bei $\langle P_1, \ldots, P_{d-1} \rangle$ um ein Ideal handelt. Damit kann $X_i^{n \cdot (d-1)!}$ wie in (2.18) dargestellt werden. Für $\tilde{n} = n \cdot (d-1)!$ ist $(d-1)! \mid \tilde{n}$ mit Sicherheit erfüllt.

Sei nun $X_1^{\alpha_1} \cdot \ldots \cdot X_{d-1}^{\alpha_{d-1}}$ ein Erzeugendes von $\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n}$. Das bedeutet:

$$\sum_{i=1}^{d-1} (d-i)\alpha_i = q_n = \sum_{i=1}^{d-1} in \quad (2.20)$$

Dann gibt es ein $i \in \{1, \ldots, d-1\}$ mit $\alpha_i \geqslant n$. Denn sonst würde

$$\sum_{i=1}^{d-1} (d-i)\alpha_i < \sum_{i=1}^{d-1} (d-i)n = \sum_{i=1}^{d-1} in$$

gelten, was im Widerspruch zu (2.20) steht. Wähle also $i \in \{1, \ldots, d-1\}$ mit $\alpha_i \geqslant n$. Dann gilt wegen (2.18):

$$X_1^{\alpha_1} \cdot \ldots \cdot X_{d-1}^{\alpha_{d-1}} = \sum_{j=1}^{d-1} X_1^{\alpha_1} \cdot \ldots \cdot X_{i-1}^{\alpha_{i-1}} \cdot X_i^{\alpha_i - n} \cdot X_{i+1}^{\alpha_{i+1}} \cdot \ldots \cdot X_{d-1}^{\alpha_{d-1}} \cdot H_{ij} \cdot P_j$$

Weil es sich bei $X_1^{\alpha_1} \cdot \ldots \cdot X_{d-1}^{\alpha_{d-1}}$ um ein homogenes Polynom vom Grad q_n handelt, können für $j = 1, \ldots, d-1$ die Polynome

$$X_1^{\alpha_1} \cdot \ldots \cdot X_{i-1}^{\alpha_{i-1}} \cdot X_i^{\alpha_i - n} \cdot X_{i+1}^{\alpha_{i+1}} \cdot \ldots \cdot X_{d-1}^{\alpha_{d-1}} \cdot H_{ij}$$

nach erneuter Anwendung von **Lemma 2.2.9** als homogen vom Grad $q_n - \deg(P_j)$ angenommen werden. Das bedeutet nun:

$$\begin{aligned} &\exists n \geqslant 1, (d-1)! \mid n : \mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n} = \\ &= {}_{\mathbb{F}_p}\langle X_1^{\beta_1} \cdot \ldots \cdot X_{d-1}^{\beta_{d-1}} \cdot P_j : j = 1, \ldots, d-1, \sum_{i=1}^{d-1} (d-i)\beta_i = q_n - \deg(P_j) \rangle \end{aligned} \tag{2.21}$$

Sei nun umgekehrt die Bedingung (2.21) erfüllt.

Aus $(d-1)! \mid n$ folgt auch $(d-1)! \mid q_n$. Weil $\forall i \in \{1, \ldots, d-1\}$ klarerweise $(d-i) \mid (d-1)!$ erfüllt ist, gilt auch: $(d-i) \mid q_n$. Das bedeutet:

$$(d-i) \mid q_n \Rightarrow \exists r_i \in \mathbb{N} : q_n = r_i(d-i) \Rightarrow \exists r_i \in \mathbb{N} : X_i^{r_i} \in \mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n}$$

Wegen Eigenschaft (2.21) bedeutet das, dass $X_i^{r_i}$ in folgender Form geschrieben werden kann:

$$X_i^{r_i} = \sum_{j=1}^{d-1} H_{ij} P_j$$

Die H_{ij} entstehen dabei aus Linearkombinationen von homogenen Polynomen der Form $X_1^{\beta_1} \cdot \ldots \cdot X_{d-1}^{\beta_{d-1}}$ vom Grad $q_n - \deg(P_j) = \deg(X_i^{r_i}) - \deg(P_j)$. Das bedeutet,

dass es sich auch bei H_{ij} um homogene Polynome desselben Grades handelt.

Setze nun $\tilde{n} = q$. Wegen $r_i \leqslant \tilde{n}$ gilt $\tilde{n} = r_i + m_i$ mit $m_i \in \mathbb{N}_0$. Daraus folgt:

$$X_i^{\tilde{n}} = X_i^{m_i} X_i^{r_i} = X_i^{m_i} \sum_{j=1}^{d-1} H_{ij} P_j = \sum_{j=1}^{d-1} (X_i^{m_i} H_{ij}) P_j \tag{2.22}$$

Bemerkung 2.3.3: $X_i^{m_i}$ ist homogen vom Grad $(d-i)m_i$ und H_{ij} ist homogen vom Grad $(d-i)r_i - \deg(P_j)$. Setze nun $\tilde{H}_{ij} = X_i^{m_i} H_{ij}$. Aufgrund der Eigenschaften graduierter Ringe ist auch $\tilde{H}_{ij}$ homogen vom Grad

$$\begin{aligned}(d-i)m_i + (d-i)r_i - \deg P_j = (d-i)(m_i + r_i) - \deg(P_j) = \\ = (d-i)\tilde{n} - \deg(P_j)\end{aligned}$$

Aus (2.22) und **Bemerkung 2.3.3** folgt nun, dass $\tilde{n}$ die Bedingung (2.18) erfüllt.

Insgesamt wurde also gezeigt, dass die in (2.18) und (2.21) formulierten Bedingungen äquivalent sind. Aufgrund dieser Tatsache kann $(\triangle)$ weiter umgeschrieben werden. Der Übersicht wegen wird im Folgenden für $\sum_{i=1}^{d-1} in$ immer q_n geschrieben.

$$\begin{aligned}(\triangle) = \bigcup_{n \geqslant 1} \{p \in \mathbb{P} : \mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n} = \\ = {}_{\mathbb{F}_p}\langle X_1^{\beta_1} \cdot \ldots \cdot X_{d-1}^{\beta_{d-1}} \cdot P_j : j = 1, \ldots, d-1, \sum_{i=1}^{d-1} (d-i)\beta_i = q_n - \deg(P_j) \rangle\}\end{aligned} \tag{2.23}$$

Bemerkung 2.3.4: Für $n \geqslant 1$ kann die Bedingung $\sum_{i=1}^{d-1}(d-i)\beta_i = q_n - \deg(P_j)$ nur von endlich vielen Polynomen der Form $X_1^{\beta_1} \cdot \ldots \cdot X_{d-1}^{\beta_{d-1}}$ erfüllt werden. Deshalb besteht das Erzeugendensystem des Vektorraums $\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n}$ aus (2.23) aus nur endlich vielen Polynomen.

Im Folgenden werden für jedes $n \geqslant 1$ die erzeugenden Vektoren aus (2.23) mit $(v_{1_n}, \ldots, v_{m_n})$ bezeichnet. Wähle nun für $n \geqslant 1$ unabhängig von den Primzahlen

$p \in \mathbb{P}$ eine Basis $(u_{1_n}, \ldots, u_{r_n})$ von $\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n}$. Eine Möglichkeit hierfür wären die erzeugenden Monome aus (2.17). Die Matrix M_n sei jene Matrix, deren Spalten $(M_n)_{-i}$ die Koordinatenspalten von v_{i_n} bezüglich der Basis $(u_{1_n}, \ldots, u_{r_n})$ bilden. Es handelt sich dabei also um eine $(r_n \times m_n)$-Matrix. Für jene Primzahlen $p \in \mathbb{P}$, für die CA_d in $\overline{\mathbb{F}}_p$ gilt, besitzt diese Matrix vollen Rang. Denn für diese Primzahlen kann aus dem Erzeugendensystem aus (2.23) eine Basis von $\mathbb{F}_p[X_1, \ldots, X_{d-1}]_{q_n}$ ausgesondert werden. Dasselbe gilt für die entsprechenden Koordinatenspalten. Damit gilt:

$$
\begin{aligned}
(\triangle) &= \bigcup_{n \geqslant 1} \{p \in \mathbb{P} : M_n \text{ besitzt über } \mathbb{F}_p \text{ vollen Rang}\} = \\
&= \bigcup_{n \geqslant 1} \{p \in \mathbb{P} : \text{ eine der größten Unterdeterminanten von } M_n \text{ ist nicht } 0 \text{ in } \mathbb{F}_p\} = \\
&= \bigcup_{n \geqslant 1} \underbrace{\{p \in \mathbb{P} : p \nmid \text{ eine der größten Unterdeterminanten von } M_n \text{ in } \mathbb{Z}\}}_{=:A_n}
\end{aligned}
$$

Beachte: Es existiert ein $n' \geqslant 1$, für das $A_{n'} \neq \emptyset$ gilt, denn laut Voraussetzung des **Hauptsatzes** gilt CA_d für eine Primzahl l in $\overline{\mathbb{F}}_l$. Also:

$$\exists n' \in \mathbb{N}\ \exists p \in \mathbb{P} : p \nmid \text{ eine der größten Unterdeterminanten von } M_{n'} \text{ in } \mathbb{Z}$$

Das bedeutet insbesondere, dass diese Unterdeterminante in $\mathbb{Z}$ nicht 0 ist. Die Menge $A_{n'}$ enthält bereits alle bis auf endlich viele Primzahlen. Denn die obige Unterdeterminante kann in $\mathbb{N}\backslash\{0\}$ als Produkt endlich vieler Primzahlen dargestellt werden. Nur diese Primzahlen teilen die Unterdeterminante in $\mathbb{Z}$.

Insgesamt wurde also gezeigt, dass es sich bei $\{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\}$ um eine *koendliche Menge* handelt, sofern CA_d für eine beliebige Primzahl l in $\overline{\mathbb{F}}_l$ erfüllt ist. Wegen **Bemerkung 2.1.7** kann daraus gefolgert werden, dass CA_d unter dieser Voraussetzung auch bis auf endlich viele Primzahlen p in algebraisch abgeschlossenen Körpern mit Primzahlcharakteristik p gilt.

SCHRITT 2: CA_d GILT IN $\overline{\mathbb{F}}_p$ BIS AUF ENDLICH VIELE PRIMZAHLEN $p \Rightarrow \mathrm{CA}_d$ GILT IN ALGEBRAISCH ABGESCHLOSSENEN KÖRPERN DER CHARAKTERISTIK 0.

Dazu betrachte folgende Menge:

$$R = \prod_{p \in \mathbb{P}} \overline{\mathbb{F}}_p = \{(a_p)_{p \in \mathbb{P}} : a_p \in \overline{\mathbb{F}}_p\} \tag{2.24}$$

Bemerkung 2.3.5: Diese Menge bildet zusammen mit der komponentenweisen Addition und Multiplikation einen Ring. Die Körpereigenschaft ist nicht garantiert, da beispielsweise für $a = (1, 0, 1, 0 \ldots)$ und $b = (0, 1, 0, 1, \ldots)$

$$a \cdot b = (0, \ldots, 0)$$

gilt. R ist also nicht *nullteilerfrei*.

Um weiterrechnen zu können, bedarf es einiger Definitionen aus der *Topologie*.

Definition 2.3.6: Sei $X \neq \emptyset$ eine Menge. Ein *Filter $\mathcal{F}$ auf X* ist eine Teilmenge $\mathcal{F} \subseteq \mathcal{P}(X)$ mit folgenden Eigenschaften:

(1) $X \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$
(2) Für $A, B \in \mathcal{F} : A \cap B \in \mathcal{F}$
(3) Für $A \in \mathcal{F}, B \subseteq X$ mit $A \subseteq B$ gilt: $B \in \mathcal{F}$

Definition 2.3.7: Ein Filter $\mathcal{F}$ auf X heißt *Ultrafilter*

$$:\Leftrightarrow \forall A \subseteq X : (A \in \mathcal{F} \text{ oder } A^c \in \mathcal{F}) \tag{2.25}$$

Bemerkung 2.3.8: Mithilfe des *Lemmas von Zorn* kann man zeigen, dass zu jedem Filter $\mathcal{F}$ auf X ein Ultrafilter $\mathcal{G}$ mit $\mathcal{F} \subseteq \mathcal{G}$ existiert.

Sei nun $\mathcal{F}$ ein vorgegebener *Ultrafilter* auf der Menge aller Primzahlen $\mathbb{P}$. Definiere $m_{\mathcal{F}}$ wie folgt:

$$m_{\mathcal{F}} = \{(a_p)_{p \in \mathbb{P}} : \{p \in \mathbb{P} : a_p = 0\} \in \mathcal{F}\} \tag{2.26}$$

Behauptung: $m_{\mathcal{F}}$ ist ein maximales Ideal in R.

Beweis: In einem ersten Schritt werden die Eigenschaften eines Ideals nachgewiesen:

- Zeige: $(0,0,0,\ldots) \in m_{\mathcal{F}}$

  $$(0,0,0,\ldots) \in m_{\mathcal{F}} \Leftrightarrow \mathbb{P} \in \mathcal{F}$$

  Wegen Eigenschaft (1) eines Filters ist das erfüllt.

- Es seien $(a_p)_{p\in\mathbb{P}}$ und $(b_p)_{p\in\mathbb{P}} \in m_{\mathcal{F}}$.
  Zeige: $(a_p)_{p\in\mathbb{P}} + (b_p)_{p\in\mathbb{P}} = (a_p + b_p)_{p\in\mathbb{P}} \in m_{\mathcal{F}}$

  $$(a_p + b_p)_{p\in\mathbb{P}} \in m_{\mathcal{F}} \Leftrightarrow \{p \in \mathbb{P} : a_p + b_p = 0\} \in \mathcal{F}$$

  Nun gilt: $\{p \in \mathbb{P} : a_p = 0\} \in \mathcal{F}$ und $\{p \in \mathbb{P} : b_p = 0\} \in \mathcal{F}$.

  $$\overset{\text{Filtereigenschaft (2)}}{\Rightarrow} \{p \in \mathbb{P} : a_p = 0\} \cap \{p \in \mathbb{P} : b_p = 0\} = \{p \in \mathbb{P} : a_p = 0 \ \wedge \ b_p = 0\} \in \mathcal{F}$$

  Zudem gilt:

  $$\{p \in \mathbb{P} : a_p + b_p = 0\} \supseteq \{p \in \mathbb{P} : a_p = 0 \ \wedge \ b_p = 0\}$$

  und deshalb folgt aus Filtereigenschaft (3) die Behauptung.

- Es seien $(r_p)_{p\in\mathbb{P}} \in R$ und $(a_p)_{p\in\mathbb{P}} \in m_{\mathcal{F}}$.
  Zu zeigen: $(r_p)_{p\in\mathbb{P}} \cdot (a_p)_{p\in\mathbb{P}} = (r_p \cdot a_p)_{p\in\mathbb{P}} \in m_{\mathcal{F}}$

$$\{p \in \mathbb{P} : r_p \cdot a_p = 0\} = \{p \in \mathbb{P} : r_p = 0\} \cup \{p \in \mathbb{P} : a_p = 0\} \supseteq \{p \in \mathbb{P} : a_p = 0\}$$

Wegen $\{p \in \mathbb{P} : a_p = 0\} \in \mathcal{F}$ folgt aus Filtereigenschaft (3) auch $\{p \in \mathbb{P} : r_p \cdot a_p = 0\} \in \mathcal{F}$.

Nun gilt es noch zu zeigen, dass das Ideal $m_{\mathcal{F}}$ maximal ist.

Annahme: $m_{\mathcal{F}}$ ist nicht maximal

$$\Rightarrow \exists I \text{ Ideal in } R \ : m_{\mathcal{F}} \subsetneq I \subsetneq R \tag{2.27}$$

Wähle deshalb $a = (a_p)_{p\in\mathbb{P}} \in I \setminus m_{\mathcal{F}}$. Dann gilt:

$$\{p \in \mathbb{P} : a_p = 0\} \notin \mathcal{F} \overset{\mathcal{F} \text{ Ultrafilter}}{\Longrightarrow} A := \{p \in \mathbb{P} : a_p \neq 0\} \in \mathcal{F} \tag{2.28}$$

Wähle nun $r \in R$. Dann gibt es $b = (b_p)_{p\in\mathbb{P}}$ und $s = (s_p)_{p\in\mathbb{P}} \in R$, sodass

$$r = sa + b,$$

wobei $s_p := r_p \cdot a_p^{-1}$ für $a_p \neq 0$ und $s_p = 0$ sonst und $b_p = 0 \quad \forall p \in A$ und $b_p = r_p$ sonst. Nun gilt:

$$\{p \in \mathbb{P} : b_p = 0\} \supseteq \{p \in \mathbb{P} : a_p \neq 0\} \overset{(2.28)}{\in} \mathcal{F} \Rightarrow b \in m_{\mathcal{F}} \subseteq I$$
$$a \in I \overset{I \text{ Ideal}}{\Longrightarrow} sa \in I$$

Insgesamt gilt also: $b \in I$ und $sa \in I \overset{I \text{ Ideal}}{\Longrightarrow} r = sa + b \in I$. Weil $r \in R$ beliebig war, folgt $R = I$, was im Widerspruch zu (2.27) steht.

□

Bemerkung 2.3.9: Weil das Ideal $m_{\mathcal{F}}$ maximal ist, wird durch den Restklassenring $K_{\text{ult}} := R/m_{\mathcal{F}} = \prod_{p\in\mathbb{P}} \overline{\mathbb{F}}_p/m_{\mathcal{F}}$ ein Körper definiert. Dieser Körper heißt *Ultraprodukt* der Körper $\overline{\mathbb{F}}_p$. Die Erklärung dafür, weshalb man dieses *Ultraprodukt* betrachtet, liefert der folgende Satz:

Satz 2.3.10: Sei $\mathcal{F}$ ein Ultrafilter und K_{ult} das zugehörige Ultraprodukt der Körper $\overline{\mathbb{F}}_p$. Dann gilt:

$$\{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\} \in \mathcal{F} \Leftrightarrow \mathrm{CA}_d \text{ gilt in } K_{\mathrm{ult}}$$

Beweis: $\Rightarrow$: Es gelte:

$$X := \{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\} \in \mathcal{F}$$

Seien nun $a = (\overline{(a_p^1)_{p\in\mathbb{P}}}, \ldots, \overline{(a_p^{d-1})_{p\in\mathbb{P}}}) \in K_{\mathrm{ult}}^{d-1}$ die Koeffizienten eines beliebigen *Casas-Alvero Polynoms* $f \in K_{\mathrm{ult}}[X]$. Will man die Gültigkeit der *Vermutung von Casas-Alvero* nachweisen, so muss man Folgendes zeigen:

$$(\overline{(a_p^1)_{p\in\mathbb{P}}}, \ldots, \overline{(a_p^{d-1})_{p\in\mathbb{P}}}) = 0 \Leftrightarrow \underbrace{\{p \in \mathbb{P} : a_p^1 = \ldots = a_p^{d-1} = 0\}}_{=:Z} \in \mathcal{F} \tag{2.29}$$

Wie bereits im ersten Kapitel dieser Arbeit erläutert, müssen die obigen Koeffizienten für alle $i \in \{1, \ldots, d-1\}$ die Bedingung

$$P_i(a) = P_i(\overline{(a_p^1)_{p\in\mathbb{P}}}, \ldots, \overline{(a_p^{d-1})_{p\in\mathbb{P}}}) = \overline{(P_i(a_p^1, \ldots, a_p^{d-1}))_{p\in\mathbb{P}}} = 0 \tag{2.30}$$

erfüllen. Die Polynome $P_i,\ i \in \{1, \ldots, d-1\}$, wurden dabei wie in **Definition 1.7** gewählt. Die Bedingung (2.30) ist genau dann erfüllt, wenn $(P_i(a_p^1, \ldots, a_p^{d-1}))_{p\in\mathbb{P}}$ im Ideal $m_{\mathcal{F}}$ enthalten ist. Damit folgt aus der Definition von $m_{\mathcal{F}}$:

$$Y := \{p \in \mathbb{P} : P_i(a_p^1, \ldots, a_p^{d-1}) = 0\} \in \mathcal{F}$$

Die zweite Filtereigenschaft garantiert nun $X \cap Y \in \mathcal{F}$.

Sei $p \in X \cap Y$. Das bedeutet:

$$p \in Y \Rightarrow \forall i \in \{1, \ldots, d-1\} : P_i(a_p^1, \ldots, a_p^{d-1}) = 0 \overset{p\in X}{\Rightarrow} a_p^1 = \ldots = a_p^{d-1} = 0$$

Damit gilt insbesondere $X \cap Y \subseteq Z$ und weil Obermengen von Filtermengen wieder im Filter liegen müssen, bedeutet das $Z \in \mathcal{F}$, was zu zeigen war.

$\Leftarrow$: Die zweite Implikationsrichtung wird mittels Kontraposition gezeigt. Sei also

$$\{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\} \notin \mathcal{F} \tag{2.31}$$

Es bleibt zu zeigen, dass CA_d dann auch nicht im Ultraprodukt K_{ult} gültig sein kann.

Weil $\mathcal{F}$ ein Ultrafilter ist, folgt wegen (2.31):

$$X := \{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt nicht in } \overline{\mathbb{F}}_p\} \in \mathcal{F}$$

Die Idee besteht nun darin, ein *Casas-Alvero Polynom* in $K_{\mathrm{ult}}[X]$ zu konstruieren, das die *Vermutung von Casas-Alvero* nicht erfüllt. Dazu wähle für $p \in X$

$$0 \neq (a_p^1, \ldots, a_p^{d-1}) \in \overline{\mathbb{F}}_p^{d-1} \text{ mit } \forall i \in \{1, \ldots, d-1\} : P_i(a_p^1, \ldots, a_p^{d-1}) = 0$$

Solche Tupel existieren, da CA_d in $\overline{\mathbb{F}}_p$ nicht erfüllt ist. Für $p \notin X$ wähle irgendein $(d-1)$-Tupel, das die Bedingung

$$(a_p^1, \ldots, a_p^{d-1}) \neq 0$$

erfüllt. Weil für ein solches p die *Vermutung von Casas-Alvero* gelten muss, folgt daraus unmittelbar

$$\forall i \in \{1, \ldots, d-1\} : P_i(a_p^1, \ldots, a_p^{d-1}) \neq 0$$

Definiere nun durch $a = (\overline{(a_p^1)_{p\in\mathbb{P}}}, \ldots, \overline{(a_p^{d-1})_{p\in\mathbb{P}}})$ die Koeffizienten eines Polynoms f_{ult}. Dieses Polynom ist ein *Casas-Alvero Polynom*, denn für alle $i \in \{1, \ldots, d-1\}$ gilt:

$$P_i(a) = \overline{(P_i(a_p^1, \ldots, a_p^{d-1}))_{p\in\mathbb{P}}} = 0, \text{ weil } \{p \in \mathbb{P} : P_i(a_p^1, \ldots, a_p^{d-1}) = 0\} = X \in \mathcal{F}$$

Nach Konstruktion muss aber $a \neq 0$ sein. Denn wäre $a = 0$, so würde das bedeuten:

$$\{p \in \mathbb{P} : (a_p^1, \ldots, a_p^{d-1}) = 0\} \overset{\text{nach Konstruktion}}{=} \emptyset \in \mathcal{F}$$

Da die leere Menge in keinem Filter enthalten sein darf, muss $a \neq 0$ gelten und somit ist CA_d in K_{ult} nicht erfüllt. □

Anstelle irgendeines Ultrafilters auf $\mathbb{P}$ wird nun ein ganz bestimmter Filter verwendet.

Satz und Definition 2.3.11: Sei X eine unendliche Menge.

$$\mathcal{F} = \{A \subseteq X : A^c \text{ endlich}\} \subseteq \mathcal{P}(X)$$

ist ein Filter auf X und heißt *Filter der koendlichen Teilmengen von* X.

Beweis:

(1) $X^c = \emptyset$ ist endlich, $\emptyset^c = X$ ist nicht endlich $\Rightarrow X \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$

(2) Seien $A, B \in \mathcal{F} \Rightarrow A^c, B^c$ endlich $\Rightarrow A^c \cup B^c \overset{\text{De Morgan}}{=} (A \cap B)^c$ endlich

$$\Rightarrow A \cap B \in \mathcal{F}$$

(3) Sei $A \in \mathcal{F}$ und $B \subseteq X$ mit $B \supseteq A$. Dann gilt $B^c \subseteq A^c$ endlich $\Rightarrow B \in \mathcal{F}$

□

Sei nun $\mathcal{U}$ der *Filter der koendlichen Teilmengen* von $\mathbb{P}$. Sei $\mathcal{F}$ ein Ultrafilter, der $\mathcal{U}$ enthält. Ein solcher Ultrafilter existiert wegen **Bemerkung 2.3.8**.

Im ersten Schritt des Beweises des Hauptsatzes wurde bereits Folgendes gezeigt:

$$\mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_l \Rightarrow \underbrace{\{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt nicht in } \overline{\mathbb{F}}_p\}}_{=:A} \text{ ist endlich}$$

Weil es sich bei A um eine endliche Menge handelt und der Filter $\mathcal{F}$ alle koendlichen Teilmengen enthält, gilt:

$$A^c = \{p \in \mathbb{P} : \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p\} \in \mathcal{F}$$

Aus **Satz 2.3.10** folgt dann aber, dass die *Vermutung von Casas-Alvero* auch im Ultraprodukt der Körper $\overline{\mathbb{F}}_p$ stimmt. Folgender Satz ist wichtig für die Vollendung des Beweises:

Satz 2.3.12: Sei $\mathcal{F}$ wie oben jener Ultrafilter, der den Filter der koendlichen Teilmengen enthält. Dann ist K_{ult} algebraisch abgeschlossen mit Charakteristik 0.

Beweis: Das Einselement des Körpers K_{ult} sieht wie folgt aus:

$$1_{\text{ult}} = \overline{(1_p)_{p\in\mathbb{P}}}$$

Annahme: $\exists n \in \mathbb{N}\backslash\{0\} : n \cdot \overline{(1_p)_{p\in\mathbb{P}}} = 0$. Das bedeutet aber:

$$n \cdot \overline{(1_p)_{p\in\mathbb{P}}} \in m_{\mathcal{F}} \Leftrightarrow \{p \in \mathbb{P} : n \cdot 1_p = 0 \text{ in } \overline{\mathbb{F}}_p\} \in \mathcal{F} \Leftrightarrow \{p \in \mathbb{P} : p \mid n\} \in \mathcal{F}$$

Da jede natürliche Zahl $n \in \mathbb{N}\backslash\{0\}$ als Produkt endlich vieler Primzahlen dargestellt werden kann, handelt es sich bei $\{p \in \mathbb{P} : p \mid n\}$ um eine endliche Menge. Weil ihr Komplement unendlich ist, kann diese Menge nicht im Filter der koendlichen Teilmengen enthalten sein. Die Annahme führt auf einen Widerspruch.

Es bleibt zu zeigen, dass es sich bei K_{ult} um einen algebraisch abgeschlossenen Körper handelt. Sei dazu

$$f = \overline{(a_p^d)_{p\in\mathbb{P}}}X^d + \ldots + \overline{(a_p^1)_{p\in\mathbb{P}}}X + \overline{(a_p^0)_{p\in\mathbb{P}}} \in K_{\text{ult}}[X]$$

Des Weiteren konstruiere aus f für jede Primzahl p ein Polynom $f_p \in \overline{\mathbb{F}}_p[X]$ wie folgt:

$$f_p = a_p^d X^d + \ldots + a_p^1 X + a_p^0 \in \overline{\mathbb{F}}_p[X]$$

Weil $\overline{\mathbb{F}}_p$ algebraisch abgeschlossen ist, zerfällt f über $\overline{\mathbb{F}}_p$ in Linearfaktoren. Seien deshalb $x_p^1, \ldots, x_p^d \in \overline{\mathbb{F}}_p$ die Nullstellen von f_p, wobei diese nicht unbedingt verschieden sein müssen. Betrachte

$$\overline{(x_p^1)_{p\in\mathbb{P}}}, \ldots, \overline{(x_p^d)_{p\in\mathbb{P}}} \in K_{\mathrm{ult}} \tag{2.32}$$

Dann gilt für alle $i \in \{1, \ldots, d\}$:

$$f(\overline{(x_p^i)_{p\in\mathbb{P}}}) = 0 \Leftrightarrow \underbrace{\{p \in \mathbb{P} : f_p(x_p^i) = 0\}}_{=\mathbb{P}} \in \mathcal{F}$$

Weil $\mathcal{F}$ ein Filter ist, ist das sicherlich erfüllt. Also zerfällt auch f über K_{ult} in Linearfaktoren. Damit ist K_{ult} algebraisch abgeschlossen.

□

Bemerkung 2.3.13: In diesem Kapitel wurde gezeigt, dass das *Ultraprodukt* der Körper $\overline{\mathbb{F}}_p$ ein algebraisch abgeschlossener Körper der Charakteristik 0 ist, in dem die *Vermutung von Casas-Alvero* für Polynome $f \in K_{\mathrm{ult}}[X]$ eines festen Grades d gilt, sofern CA_d für eine Primzahl l im Körper $\overline{\mathbb{F}}_l$ erfüllt ist. **Bemerkung 2.1.7** garantiert nun auch die Gültigkeit von CA_d in allen algebraisch abgeschlossenen Körpern der Charakteristik 0.

KAPITEL 3

Beweis der Vermutung für unendlich viele Grade

In diesem Kapitel wird in Anlehnung an [**GvBL+07**] gezeigt, dass CA_d in einem algebraisch abgeschlossenen Körper $\mathbb{K}$ der Charakteristik 0 gilt, falls der Grad d eine Primzahlpotenz beziehungsweise das Doppelte einer Primzahlpotenz ist. Die nachfolgenden Sätze und Beweise sind dem Artikel [**GvBL+07**] entnommen, werden hier aber detailliert ausgeführt. Die Beweisidee besteht darin, für alle Zahlen $d = p^k$ beziehungsweise $d = 2p^k$, $p \in \mathbb{P}$ und $k \in \mathbb{N}$, eine Primzahl $l \in \mathbb{P}$ zu suchen, sodass die *Vermutung von Casas-Alvero* für alle Polynome vom Grad d in $\overline{\mathbb{F}}_l[X]$ erfüllt ist. Die Anwendung des Hauptsatzes aus Kapitel 2 liefert dann sofort die Gültigkeit von CA_d in beliebigen Körpern der Charakteristik 0. Zudem garantiert der Hauptsatz, dass CA_d auch bis auf endlich viele Primzahlen p in algebraisch abgeschlossenen Körpern mit Primzahlcharakteristik p gilt.

In der Folge werden einige Sätze und Lemmata bewiesen, die für den endgültigen Beweis notwendig sind.

Lemma 3.1 (nach [**GvBL+07**], S. 227, Proposition 2.3)**:** Es sei $\mathbb{K}$ ein beliebiger algebraisch abgeschlossener Körper und $f \in \mathbb{K}[X]$ ein *Casas-Alvero Polynom* mit $\deg(f) = 1$ oder $\deg(f) = 2$. Dann erfüllt f die *Vermutung von Casas-Alvero*.

Beweis: Ist f ein *Casas-Alvero Polynom* mit $\deg(f) = 1$, so besitzt es bereits das gewünschte Aussehen.

Sei deshalb $f = X^2 + a_1X$ ein *Casas-Alvero Polynom* vom Grad 2. Für die erste *Hasse-Ableitung* gilt:

$$f_1 = 2X + a_1$$

Fall 1: $\mathrm{char}(\mathbb{K}) = 2 \Rightarrow f_1 = a_1$. Weil f und f_1 eine gemeinsame Nullstelle besitzen, muss $a_1 = 0$ und somit $f = X^2$ gelten.

Fall 2: $\mathrm{char}(\mathbb{K}) \neq 2$. Annahme: f und f_1 besitzen eine gemeinsame Nullstelle $x \neq 0$. Dann ist x eine Nullstelle von $X + a_1$ und $2X + a_1$ und somit auch von

$$(2X + a_1) - (X + a_1) = X$$

Damit führt die Annahme $x \neq 0$ auf einen Widerspruch. Somit besitzen f und f_1 die gemeinsame Nullstelle $x = 0$. Also muss $a_1 = 0$ gelten und f hat die Form $f = X^2$. □

Definition 3.2: Für eine Zahl $n \in \mathbb{N}$ und eine Primzahl p definiere

$$\nu_p(n) := \max\{k \in \mathbb{N} : p^k \mid n\}$$

Folgendes Lemma wird später nützlich sein:

Lemma 3.3 (Lemma und Beweis nach [**GvBL+07**], S. 227, Lemma 2.4 sowie *Theorem von Lucas*)**:** Sei d eine positive ganze Zahl und p eine Primzahl mit $p \mid d$. Zudem sei auch i eine positive ganze Zahl und es gelte: $0 < i \leqslant d$. Dann gilt:

$$\nu_p(i) < \nu_p(d) \Rightarrow \binom{d}{i} \equiv 0 \mod p \tag{3.1}$$

Falls $\nu_p(i) = \nu_p(d)$ ist, also $d = p^k d'$ und $i = p^k i'$ mit $p \nmid d'$ und $p \nmid i'$, dann:

$$\binom{d}{i} \equiv \binom{d'}{i'} \bmod p \tag{3.2}$$

Beweis: Man kann leicht zeigen, dass für $d, i > 0$ die Beziehung

$$\binom{d}{i} = \frac{d}{i}\binom{d-1}{i-1}$$

stimmt. Deshalb:

$$i\binom{d}{i} = d\binom{d-1}{i-1} \tag{3.3}$$

Nun gilt:

$$\nu_p(d\binom{d-1}{i-1}) = \nu_p(d) + \underbrace{\nu_p(\binom{d-1}{i-1})}_{\geqslant 0} \geqslant \nu_p(d)$$

Wegen (3.3) muss aber $\nu_p(i\binom{d}{i}) = \nu_p(d\binom{d-1}{i-1})$ gelten, was sofort wegen $\nu_p(i) < \nu_p(d) \quad p \mid \binom{d}{i}$ impliziert.

Für den zweiten Teil der Aussage sei auf das *Theorem von Lucas* verwiesen, aus dem unmittelbar (3.2) folgt.

□

Proposition 3.4 (Proposition und Beweis nach [**GvBL+07**], S. 227, Proposition 2.5)**:** Sei p eine Primzahl und $d = p^e$ für ein $e \in \mathbb{N}$. Dann gilt CA_d in $\overline{\mathbb{F}}_p$.

Beweis: Dazu sei $f = X^d + \ldots + a_1 X \in \overline{\mathbb{F}}_p[X]$ ein *Casas-Alvero Polynom*.

Für $i \in \{1, \ldots, d-1\}$ gilt wegen $d = p^e$: $\quad \nu_p(i) < \nu_p(d)$ und somit:

$$\forall i \in \{1, \ldots, d-1\} : \binom{d}{i} = 0 \quad \text{in } \overline{\mathbb{F}}_p \tag{3.4}$$

Das impliziert insbesondere $\binom{d}{d-1} = 0$. Das bedeutet für die $(d-1)$*-te Hasse-Ableitung*:

$$f_{d-1} = \underbrace{\binom{d}{d-1}}_{=0} X + a_{d-1} = a_{d-1}$$

Weil nun f und f_{d-1} laut Voraussetzung eine gemeinsame Nullstelle besitzen, muss $a_{d-1} = 0$ gelten.

Dieselbe Argumentation kann nun für f_{d-2} angewandt werden. (3.4) impliziert $\binom{d}{d-2} = 0$ und damit:

$$f_{d-2} = \underbrace{\binom{d}{d-2}}_{=0} X^2 + \binom{d-1}{d-2} \underbrace{a_{d-1}}_{=0} X + a_{d-2} = a_{d-2}$$

Weil aber auch f und f_{d-2} eine gemeinsame Nullstelle besitzen, muss $a_{d-2} = 0$ gelten.

Führt man diese Argumentation fort, folgt irgendwann

$$a_1 = \ldots = a_{d-1} = 0$$

und damit $f = X^d$. Also erfüllt f die *Vermutung von Casas-Alvero*.

□

Proposition 3.5 (Proposition und Beweis nach [**GvBL+07**], S. 228, Proposition 2.7)**:** Seien $d \geqslant 1$ und $k \geqslant 0$ ganze Zahlen. Besitzt d die Form $d = np^k$ für eine Primzahl p und $n \in \mathbb{N}$, dann gilt:

$$\mathrm{CA}_n \text{ gilt in } \overline{\mathbb{F}}_p \Rightarrow \mathrm{CA}_d \text{ gilt in } \overline{\mathbb{F}}_p$$

Beweis: Sei wieder $f = X^d + \ldots + a_1 X \in \overline{\mathbb{F}}_p[X]$ ein *Casas-Alvero Polynom*.

Erneute Anwendung von **Lemma 3.3** liefert:

$$\forall i = 1, \ldots, d - (p^k - 1) : \binom{d}{i} = 0 \text{ in } \mathbb{F}_p$$

Denn solche i werden von p weniger als k-mal geteilt, während das beispielsweise für $i = d - p^k = np^k - p^k = (n-1)p^k$ nicht der Fall ist.

Damit gilt mit derselben Argumentation wie im vorigen Beweis:

$$a_{d-1} = \ldots = a_{d-(p^k-1)} = 0$$

Betrachtet man aber die $d-p^k$*-te Hasse-Ableitung*, so muss $\binom{d}{d-p^k}$ nicht verschwinden.

$$f_{d-p^k} = \binom{d}{d-p^k} X^{d-(d-p^k)} + \binom{d-1}{d-p^k} \underbrace{a_{d-1}}_{=0} X^{d-(d-p^k)-1}$$
$$+ \ldots + \binom{d-(p^k-1)}{d-p^k} \underbrace{a_{d-(p^k-1)}}_{=0} + a_{d-p^k} = \binom{d}{d-p^k} X^{p^k} + a_{d-p^k}$$

Da aber $d-p^k-1$ weniger oft von p^k geteilt wird als d und $d-p^k$, gilt für die $(d-p^k-1)$*-te Hasse-Ableitung* wieder mit derselben Argumentation wie zuvor:

$$f_{d-p^k-1} = \underbrace{\binom{d}{d-p^k-1}}_{=0} X^{d-(d-p^k-1)} + \binom{d-1}{d-p^k-1} \underbrace{a_{d-1}}_{=0} X^{d-(d-p^k-1)-1}$$
$$+ \ldots + \underbrace{\binom{d-p^k}{d-p^k-1}}_{=0} a_{d-p^k} + a_{d-p^k-1} = a_{d-p^k-1}$$

Weil f und f_{d-p^k-1} eine gemeinsame Nullstelle besitzen, gilt wieder $a_{d-p^k-1} = 0$.

Führt man diese Argumentationsweise fort, sieht man: $\forall i \in \{1, \ldots, d\} : p^k \nmid i \Rightarrow a_i = 0$. Also muss das Polynom f folgende Form haben:

$$f = X^d + a_{d-p^k} X^{d-p^k} + \ldots + a_{p^k} X^{p^k} \tag{3.5}$$

Sei nun $d_{\frac{l}{p^k}}$ eine p^k-te Wurzel von a_l, also $d_{\frac{l}{p^k}}^{p^k} = a_l$.

Beachte: $d_{\frac{l}{p^k}} \in \overline{\mathbb{F}}_p$, denn $d_{\frac{l}{p^k}}$ ist Nullstelle von $X^{p^k} - a_l \in \overline{\mathbb{F}}_p[X]$ und $\overline{\mathbb{F}}_p$ ist algebraisch abgeschlossen.

Das Polynom $g \in \overline{\mathbb{F}}_p[X]$ sei nun wie folgt definiert:

$$g = X^n + d_{n-1}X^{n-1} + \ldots + d_1 X \tag{3.6}$$

Bemerkung 3.6: In einem Körper $\mathbb{K}$ mit Primzahlcharakteristik p gilt für $a, b \in \mathbb{K}$: $(a+b)^p = a^p + b^p$. Daraus folgt zudem leicht $(a+b)^{p^e} = a^{p^e} + b^{p^e}$ für ein $e \in \mathbb{N}$. Diese Eigenschaft wird in der Literatur oft als *Freshman's dream* bezeichnet. Macht man sich diese Tatsache zunutze, so gilt:

$$\begin{aligned} g^{p^k} &= (X^n + d_{n-1}X^{n-1} + \ldots + d_1 X)^{p^k} \overset{\text{Freshman's dream}}{=} \\ &= (X^n)^{p^k} + (d_{n-1}X^{n-1})^{p^k} + \ldots + (d_1 X)^{p^k} = \\ &= X^{np^k} + d_{n-1}^{p^k} X^{(n-1)p^k} + \ldots + d_1^{p^k} X^{p^k} = \\ &X^d + a_{(n-1)p^k} X^{(n-1)p^k} + \ldots + a_{p^k} X^{p^k} \overset{(n-1)p^k = d-p^k}{=} f \end{aligned}$$

Insgesamt bedeutet das:

$$f = g^{p^k} \text{ für } g \in \overline{\mathbb{F}}_p[X] \text{ mit } \deg(g) = n \tag{3.7}$$

Nun bleibt noch zu zeigen, dass es sich auch bei g um ein *Casas-Alvero Polynom* handelt. Dazu betrachte die p^k-te Potenz der i*-ten Hasse-Ableitung* von g.

$$\begin{aligned} g_i^{p^k} &= (\binom{n}{i} X^{n-i} + \binom{n-1}{i} d_{n-1} X^{n-i-1} + \ldots + \binom{i}{i} d_i)^{p^k} \overset{\text{Freshman's dream}}{=} \\ &= (\binom{n}{i} 1)^{p^k} X^{(n-i)p^k} + (\binom{n-1}{i} d_{n-1})^{p^k} X^{(n-i-1)p^k} + \ldots + (\binom{i}{i} d_i)^{p^k} = (\triangle) \end{aligned}$$

Aus

$$(\underbrace{c}_{\in\mathbb{Z}} \cdot \underbrace{a}_{\in\mathbb{F}_p})^p = (\underbrace{a + \ldots + a}_{c\text{-mal}})^p \overset{\text{Freshman's dream}}{=} \underbrace{(a^p + \ldots + a^p)}_{c\text{-mal}} = ca^p$$

folgt leicht $(ca)^{p^e} = ca^{p^e}$. Zudem gilt wegen (3.2):

$$\binom{n}{i} = \binom{np^k}{ip^k} = \binom{d}{ip^k} \text{ in } \overline{\mathbb{F}}_p$$

Damit:

$$(\triangle) = \binom{d}{ip^k} X^{d-ip^k} + \binom{d-p^k}{ip^k} a_{(n-1)p^k} X^{d-ip^k-p^k} + \ldots + \binom{ip^k}{ip^k} a_{ip^k} = f_{ip^k}$$

Insgesamt bedeutet das also:

$$g_i^{p^k} = f_{ip^k} \tag{3.8}$$

Weil f ein *Casas-Alvero Polynom* ist, muss das wegen (3.8) auch für g gelten. Wegen $\deg(g) = n$ erfüllt g laut Voraussetzung die *Vermutung von Casas-Alvero*, woraus

$$g = X^n$$

folgt. Wegen (3.7) bedeutet das: $f = g^{p^k} = (X^n)^{p^k} = X^{np^k} = X^d$. Damit erfüllt auch f die *Vermutung von Casas-Alvero*.

□

Bemerkung 3.7: Möchte man CA_d für einen möglicherweise großen Grad $d = np^k$ in $\overline{\mathbb{F}}_p$ beweisen, so erlaubt es **Proposition 3.5**, stattdessen *Casas-Alvero Polynome* vom Grad n zu betrachten. Sind n und p klein genug gewählt, so ist es in manchen Fällen möglich, CA_d in $\overline{\mathbb{F}}_p$ durch einfaches Nachrechnen zu beweisen. Dies soll anhand eines Beispiels verdeutlicht werden.

Beispiel 3.8: Im Folgenden wird gezeigt, dass CA_3 in $\overline{\mathbb{F}}_5$ gilt. **Proposition 3.5** garantiert dann unter anderem die Gültigkeit von CA_{15} in $\overline{\mathbb{F}}_5$ und nach Anwendung des Hauptsatzes auch in algebraisch abgeschlossenen Körpern der Charakteristik 0.

Sei dazu $f = X^3 + aX^2 + bX \in \overline{\mathbb{F}}_5[X]$ ein *Casas-Alvero Polynom* vom Grad 3. Die beiden *Hasse-Ableitungen* f_1 und f_2 lauten:

$$f_1 = 3X^2 + 2aX + b$$
$$f_2 = 3X + a$$

Laut Voraussetzung teilt f mit diesen beiden *Hasse-Ableitungen* eine gemeinsame Nullstelle. Sei $x \in \overline{\mathbb{F}}_5$ die Nullstelle von f_2. Dann gilt:

$$f_2(x) = 0 \Leftrightarrow 3x + a = 0 \Leftrightarrow 3x = -a = 4a \Leftrightarrow [\frac{1}{3} = 2 \text{ in } \overline{\mathbb{F}}_5] \Leftrightarrow x = 8a = 3a$$

Die Zahl $x = 3a$ muss auch eine Nullstelle von f sein. Einsetzen in f liefert:

$$f(3a) = (3a)^3 + a(3a)^2 + b(3a) = 27a^3 + 9a^3 + 3ab = a^3 + 3ab = a(a^2 + 3b) = 0$$
$$\Leftrightarrow a = 0 \vee a^2 + 3b = 0$$

Fall 1: a=0. Dann vereinfachen sich die Polynome f und f_1 wie folgt:

$$f = X^3 + bX$$
$$f_1 = 3X^2 + b$$

Annahme: f und f_1 besitzen die gemeinsame Nullstelle $x \neq 0$. Dann muss x eine Nullstelle von $X^2 + b$ sein. Damit gilt auch:

$$3x^2 + b - x^2 - b = 2x^2 = 0$$

Weil in Charakteristik 5 aber $2 \neq 0$ gilt, muss $x = 0$ sein, was im Widerspruch zur Annahme steht. Damit teilen f und f_1 die gemeinsame Nullstelle 0. Für f_1 bedeutet das:

$$f_1(0) = b = 0$$

Insgesamt gilt also $a = b = 0$ und damit $f = X^3$, was die Gültigkeit von CA_3 in $\overline{\mathbb{F}}_5$ impliziert.

Fall 2: $a^2 + 3b = 0 \Leftrightarrow a^2 = -3b = 2b \Leftrightarrow b = 3a^2$. Das bedeutet für f und f_1:

$$f = X^3 + aX^2 + 3a^2X$$
$$f_1 = 3X^2 + 2aX + 3a^2$$

Weil f und f_1 eine gemeinsame Nullstelle besitzen, muss $\mathrm{Res}(f, f_1) = 0$ gelten: Das bedeutet

$$\det \begin{pmatrix} 1 & a & 3a^2 & 0 & 0 \\ 0 & 1 & a & 3a^2 & 0 \\ 3 & 2a & 3a^2 & 0 & 0 \\ 0 & 3 & 2a & 3a^2 & 0 \\ 0 & 0 & 3 & 2a & 3a^2 \end{pmatrix} = 99a^6 = 4a^6 = 0$$

Weil in Charakteristik 5 aber $4 \neq 0$ gilt, muss $a = 0$ sein. Das impliziert sofort $b = 0$ und damit die Gültigkeit von CA_3 in $\overline{\mathbb{F}}_5$.

$\diamond$

Nun wurden genügend Vorbereitungen getroffen, um den Hauptsatz dieses Kapitels beweisen zu können.

Satz 3.9 (Satz und Beweis nach [**GvBL+07**], S. 228, Theorem)**:** Seien p eine Primzahl und $k \in \mathbb{N}$. Weiters gelte $d = p^k$ oder $d = 2p^k$. Dann stimmt die *Vermutung von Casas-Alvero* in Polynomringen über algebraisch abgeschlossenen Körpern der Charakteristik 0 für Polynome vom Grad d. Zudem ist sie auch bis auf endlich viele Primzahlen l in algebraisch abgeschlossenen Körpern der Charakteristik l erfüllt.

Beweis: Sei $d = p^k$. Laut **Proposition 3.4** gilt CA_d in $\overline{\mathbb{F}}_p$. Aufgrund des Hauptsatzes aus Kapitel 2 folgt dann die Behauptung.

Sei nun $d = 2p^k$. Wegen **Lemma 3.1** gilt CA_2 für Polynome, die über einem beliebigen Körper definiert wurden, also insbesondere in $\overline{\mathbb{F}}_p$. Aus **Proposition 3.5** folgt schlussendlich:

$$\mathrm{CA}_2 \text{ gilt in } \overline{\mathbb{F}}_p \Rightarrow \mathrm{CA}_{2p^k} \text{ gilt in } \overline{\mathbb{F}}_p$$

Erneute Anwendung des Hauptsatzes liefert die Behauptung.

□

KAPITEL 4

Gegenbeispiele in positiver Charakteristik

Wie bereits in der Einleitung erläutert, ist es noch niemandem gelungen, die *Vermutung von Casas-Alvero* für Polynome beliebigen Grades zu beweisen. Für Polynome, die über Körpern der Charakteristik 0 definiert sind, wurden aber bis heute noch keine Gegenbeispiele gefunden, die die Vermutung widerlegen könnten. Diese Tatsache könnte dafür sprechen, dass die *Vermutung von Casas-Alvero* in Polynomringen über algebraisch abgeschlossenen Körpern der Charakteristik 0 stimmt.

Für Körper mit Primzahlcharakteristik p fand man aber schnell Gegenbeispiele, die zeigten, dass die *Vermutung von Casas-Alvero* nicht immer stimmen muss. Das Standardbeispiel, das gerne zur Widerlegung der Vermutung angegeben wird, lautet wie folgt:

Beispiel 4.1 (nach [**GvBL+07**], S. 229, Proposition 3.1)**:** Sei $\mathbb{K}$ ein Körper mit $\mathrm{char}(\mathbb{K}) = p$ für eine Primzahl p und

$$f = X^{p+1} - X^p = X^p(X-1) \in \mathbb{K}[X]$$

Dieses Polynom vom Grad $d = p+1$ besitzt zwei Nullstellen (nämlich 0 und 1) und hat dennoch mit jeder seiner *Hasse-Ableitungen* einen nichttrivialen Faktor gemein. Denn $f_1, \ldots, f_{d-2}$ teilen mit f den Faktor X.

Für f_{d-1} gilt:

$$f_{d-1} = \binom{d}{d-1} X^{d-(d-1)} - \binom{d-1}{d-1} X^{d-(d-1)-1} =$$
$$= dX - 1 = (p+1)X - 1 = \underbrace{pX}_{=0} + X - 1 = X - 1$$

Also teilen f und f_{d-1} den Faktor $(X-1)$. Weil aber f zwei Nullstellen besitzt, ist die *Vermutung von Casas-Alvero* hier nicht erfüllt.

Betrachtet man nun aber wie in Kapitel 3 Polynome vom Grad $d = p^k$ oder $d = 2p^k$, so wurde für diesen Fall bewiesen, dass die *Vermutung von Casas-Alvero* in Körpern $\overline{\mathbb{F}}_l$ nur für endlich viele Primzahlen l verletzt werden kann. Diese Primzahlen können sehr groß sein.

So fanden *H.-C. Graf von Bothmer et al.* (vgl. [**GvBL+07**], S. 229, Remark 3.2) ein Polynom vom Grad $6 = 2 \cdot 3^1$ der Form

$$P = X^6 + 3144481702696843X^4 + X^3 + 2707944513497181X^2$$

in Charakteristik 7390044713023799, für das die *Vermutung von Casas-Alvero* nicht gilt.

Resümee

Ziel der vorliegenden Bachelorarbeit war es, dem Leser einige Ideen, die in den letzten Jahren hinsichtlich der *Vermutung von Casas-Alvero* aufgekommen sind, näherzubringen. Die Arbeit orientierte sich stark am Artikel [**GvBL+07**] von *H.-C. Graf von Bothmer et al.*, dem mit dem Beweis der Vermutung für unendlich viele Grade der Form $d = p^k$ beziehungsweise $d = 2p^k$ der wohl wichtigste Erfolg im Zusammenhang mit der *Vermutung von Casas-Alvero* zuzuschreiben ist.

Im ersten Teil der Arbeit wurde aufgezeigt, auf welche Weise man die Koeffizienten eines *Casas-Alvero Polynoms* als Elemente einer *affinen Varietät* auffassen kann. Das war nötig, um im zweiten Kapitel *Hilberts Nullstellensatz* zu formulieren und auf die *affine Varietät* anwenden zu können. *Hilberts Nullstellensatz* war der Grundstein für den Beweis des Hauptsatzes des zweiten Kapitels. Dieser Hauptsatz garantierte die Gültigkeit der Vermutung für Polynome vom Grad d mit Koeffizienten in algebraisch abgeschlossenen Körpern der Charakteristik 0 und bis auf endlich viele Ausnahmen p auch in algebraisch abgeschlossenen Körpern der Charakteristik p, falls CA_d bereits in einem Körper $\overline{\mathbb{F}}_l$ für eine beliebige Primzahl l gezeigt wurde. An dieser Stelle wich die vorliegende Bachelorarbeit von [**GvBL+07**] ab und illustrierte eine andere Möglichkeit, den Hauptsatz zu beweisen. Unter der Annahme, dass CA_d in $\overline{\mathbb{F}}_l$ richtig ist, wurde in einem ersten Schritt unter Zuhilfenahme von *Hilberts Nullstellensatz* die Gültigkeit von CA_d in fast allen $\overline{\mathbb{F}}_p$ nachgewiesen. Diese Tatsache garantierte dann die Gültigkeit der Vermutung im *Ultraprodukt der Körper* $\overline{\mathbb{F}}_p$, woraus unmittelbar deren Richtigkeit in Körpern der Charakteristik 0 folgte.

In einem dritten Kapitel wurde dann in Anlehnung an [**GvBL+07**] die *Vermutung von Casas-Alvero* in Charakteristik 0 für Primzahlpotenzen und das Doppelte von Primzahlpotenzen bewiesen.

Das letzte Kapitel der Arbeit zeigte auf, dass in Körpern mit positiver Charakteristik Polynome existieren, für die die *Vermutung von Casas-Alvero* nicht gilt.

Abschließend sei noch erwähnt, dass die Beweisidee von [**GvBL+07**] leider nicht ausreichte, um die *Vermutung von Casas-Alvero* für beliebige Grade zu lösen. Denn obwohl der Hauptsatz aus Kapitel 2 das Rechnen in positiver Charakteristik erlaubt, garantiert er die Richtigkeit der Vermutung nur bis auf endlich viele Ausnahmen p in algebraisch abgeschlossenen Körpern mit Primzahlcharakteristik p, falls CA_d in einem Körper $\overline{\mathbb{F}}_l$ gezeigt wurde. Es wurde beispielsweise nachgewiesen, dass CA_3 bis auf eine einzige Ausnahme ($p = 2$) in $\overline{\mathbb{F}}_p$ gilt. Aufgrund dieser Tatsache ist es leider nicht möglich, **Satz 3.5** für die Primzahl $p = 2$ anzuwenden. Das bedeutet, dass man mit der verwendeten Beweisidee nicht auf die Gültigkeit der Vermutung für Polynome vom Grad $d = 3 \cdot 2^k$ schließen kann. Aus diesem Grund ist es unter anderem bis heute noch nicht gelungen, die *Vermutung von Casas-Alvero* für Grad $24 = 3 \cdot 2^3$ zu beweisen.

Man kann also nur hoffen, dass irgendwann jemand eine zündende Idee hat, mithilfe derer die *Vermutung von Casas-Alvero* endgültig gelöst (oder auch widerlegt) werden kann. Bis dahin bleibt sie ein mathematisches Phänomen, dessen Aussage simpel und verständlich ist, dessen Lösung aber vielen Mathematikern ein Rätsel ist.

Literaturverzeichnis

[Bo06] S. BOSCH, *Algebra.* Springer-Verlag, 6. Auflage, Deutschland 2006.

[GvBL+07] H.C. GRAF V. BOTHMER, O. LABS, J. SCHICHO AND C. VAN DE WOESTIJNE, *The Casas-Alvero conjecture for infinitely many degrees.* Journal of Algebra 316, S. 224-230, 2007.

[DdJ11] J. DRAISMA AND J.P. DE JONG, *On the Casas-Alvero conjecture.* Newsletter of the EMS 80, S. 29-33, 2011.

[Fi11] G. FISCHER, *Lehrbuch der Algebra. Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern.* Vieweg+Teubner Verlag, 2. Auflage, Deutschland 2011.

[Ne16] T. NETZER, *Algebraische Geometrie*. Ein Skriptum zur Vorlesung *Einführung in die höhere Algebra und diskrete Mathematik. Algebraische Geometrie mit algorithmischen Aspekten.* Technische Universität Innsbruck im SoSe 2016.

[PD11] A. PRESTEL, C.N. DELZELL, *Mathematical Logic an Model Theory. A Brief Introduction.* Springer-Verlag, London 2011.