Singularitäten von Kummer-Varietäten in beliebiger Charakteristik

Inaugural-Dissertation

zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Benedikt Frederik Schilson
aus Düsseldorf

Düsseldorf, Mai 2018

aus dem Mathematischen Institut
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit der Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Berichterstatter:

1. Prof. Dr. Stefan Schröer

2. Prof. Dr. Benjamin Klopsch

Tag der mündlichen Prüfung: 18.07.2018

Zusammenfassung

Eine Kummer-Varietät X ist per Definition der Quotient einer abelschen Varietät A nach der $\mathbb{Z}/2\mathbb{Z}$-Wirkung der Vorzeicheninvolution ι. Gilt $g = \dim(A) \geq 2$, dann besteht der singuläre Ort von X genau aus den Bildern der 2-Torsionspunkte von A. Ziel dieser Arbeit ist eine Beschreibung der auftretenden Singularitäten. Um diese zu erreichen, werden die vervollständigten lokalen Ringe an den singulären Punkten berechnet.

Ist der Grundkörper k algebraisch abgeschlossen und $2 \neq 0$ in k, so besitzt X genau 2^{2g} singuläre Punkte. Der vervollständigte lokale Ring an jedem dieser Punkte wird über die induzierte Wirkung von ι auf dem Kotangentialraum ermittelt. Es wird u. a. bewiesen, dass die Singularitäten durch ein Blow-up mit dem singulären Ort als Zentrum aufgelöst werden und dass der exzeptionelle Divisor aus der disjunkten Vereinigung von 2^{2g} projektiven Räumen $\mathbb{P}_k^{g-1}$ besteht. Diese Aussage ist bekannt, ein Beweis war in der Fachliteratur jedoch nicht auffindbar.

Der Hauptteil dieser Arbeit behandelt den Fall, dass k ein algebraisch abgeschlossener Körper der Charakteristik $p = 2$ ist. Für Kummer-Varietäten, die von Produkten elliptischer Kurven stammen, wird eine offene affine Umgebung genau eines singulären Punktes angegeben, aus der dann auch der vervollständigte lokale Ring gewonnen wird. Es wird zunächst eine geeignete offene affine ι-invariante Umgebung U eines 2-Torsionspunkts ermittelt und der Quotient U/ι gesucht. Nach geeigneter Wahl von Koordinaten kann das Spektrum des affinen Koordinatenrings $R = \Gamma(U, \mathscr{O}_A)$ als abgeschlossenes Unterschema von $\mathbb{A}_k^{2g}$ aufgefasst werden, sodass die $\mathbb{Z}/2\mathbb{Z}$-Wirkung auf U durch eine Involutionswirkung auf $\mathbb{A}_k^{2g}$ induziert wird. Der entscheidende Beweisschritt ist, dass die Bildung des Quotienten von $\mathbb{A}_k^{2g}$ nach dieser Wirkung verträglich mit dem Übergang zum genannten abgeschlossenen Unterschema ist. Die $\mathbb{Z}/2\mathbb{Z}$-Wirkung auf $\mathbb{A}_k^{2g}$ wurde von Richman 1990 im wichtigsten Spezialfall untersucht, auf den die Berechnung von U/ι zurückgeführt werden kann. Es wird auch ein Beweis gegeben, der das Resultat von Richman nicht benutzt.

Im Fall $\mathrm{char}(k) = 2$ folgt aus der Beschreibung der Singularitäten, dass ihre Einbettungsdimension $2^g - 1$ beträgt. Das Resultat lässt sich mittels der Isomorphie der zugehörigen formalen Gruppen auf gewöhnliche abelsche Varietäten ausdehnen. Für Kummer-Flächen erhält man die bekannten Isomorphietypen der Singularitäten aus den Arbeiten von Artin, Shioda und Katsura aus den 1970er Jahren.

Summary

A Kummer variety X is by definition the quotient of an abelian variety A by the $\mathbb{Z}/2\mathbb{Z}$-action of the sign involution ι. If $\dim(A) \geq 2$, then the singular locus of X consists of the images of the 2-division points of A. The goal of this thesis is to give a description of these singularities. To do so, the completed local rings of the singular points are computed.

For an algebraically closed ground field k with $2 \neq 0$, X has exactly 2^{2g} singular points. The completed local ring is obtained by using the induced ι-action on the cotangent space at the singular points. It will be proven, among other statements, that X possesses a resolution of singularities which is given by a blow-up in the singular locus. The exceptional divisor is the disjoint union of 2^{2g} copies of projective space $\mathbb{P}_k^{g-1}$. This result is known, but a proof was not found in the literature.

The main part of this thesis deals with the case that k is an algebraically closed field of characteristic $p = 2$. If X is the Kummer variety of a product of elliptic curves, an open affine neighbourhood of one singular point is given from which the completed local ring can be derived. First, a suitable open affine ι-invariant subset U containing exactly one point of order (at most) 2 is searched for. The quotient U/ι is the desired open affine neighbourhood of the singular point in X. After a change of variables, the spectrum of the affine coordinate ring $R = \Gamma(U, \mathscr{O}_A)$ can be considered as a closed subscheme of affine space $\mathbb{A}_k^{2g}$ such that the $\mathbb{Z}/2\mathbb{Z}$-action on U coincides with the induced action of an involution on $\mathbb{A}_k^{2g}$. The decisive step of the computation is that passing to the quotient of $\mathbb{A}_k^{2g}$ by the group action is compatible with taking the closed subscheme mentioned above. The $\mathbb{Z}/2\mathbb{Z}$-action on $\mathbb{A}_k^{2g}$ has been studied by Richman in the linear case, on which the computation of U/ι relies. We also give a proof which does not use Richman's result.

In characteristic 2, it follows from the description of the completed local rings that the embedding dimension of the singularities is equal to $2^g - 1$ and this result can be extended to abelian varieties whose associated formal group is isomorphic to that of a product of elliptic curves. This is the case e. g. for all ordinary abelian varieties. For Kummer surfaces, one gets the known types of the singularities as described by Artin, Shioda and Katsura in the 1970s.

Inhaltsverzeichnis

Einleitung **1**

1 Grundlagen **7**
1.1 Abelsche Varietäten 7
1.2 Quotienten nach endlicher Gruppenwirkung 16
1.3 Einige Eigenschaften von Ringen 22
1.4 Blow-ups 31

2 Klassische Kummer-Varietäten **37**
2.1 Eigenschaften der Singularitäten 37
2.1.1 Eigenschaften des lokalen Rings 37
2.1.2 Auflösung der Singularität 46
2.2 Die Kummer-Konfiguration 50

3 Wilde Kummer-Varietäten **63**
3.1 Kummer-Flächen 63
3.2 Produkte elliptischer Kurven 67
3.2.1 Die Diagonalwirkung auf den Faktoren 67
3.2.2 Die Erzeuger des Invariantenrings 74
3.2.3 Die Relationen zwischen den Erzeugern 81
3.3 Beispiele 91
3.3.1 Flächen und Dreifaltigkeiten 91
3.3.2 Rationalität und Kummer-Varietäten 93
3.3.3 Analoga in Charakteristik p 94
3.4 Formale Gruppen 97

Literaturverzeichnis **105**

Tabellen- und Abbildungsverzeichnis **111**

Einleitung

Eine zusammenhängende algebraische Gruppe A, die über einem Grundkörper k eigentlich ist, wird *abelsche Varietät* genannt. Die Menge der rationalen Punkte $A(k)$ besitzt die Struktur einer abelschen Gruppe, die von Morphismen von Schemata induziert wird. Insbesondere das Invertieren eines Elements ist durch einen Morphismus $\iota\colon A \to A$ gegeben, der als *Vorzeicheninvolution* bezeichnet wird. Eine *Kummer-Varietät* ist per Definition der Quotient $X = A/\iota$ einer abelschen Varietät nach der $\mathbb{Z}/2\mathbb{Z}$-Operation, die jeden Punkt mit seinem Inversen vertauscht.

Ist $U = \mathrm{Spec}(R)$ ein offenes affines Unterschema von A mit der Eigenschaft $\iota(U) = U$, dann induziert ι eine $\mathbb{Z}/2\mathbb{Z}$-Wirkung auf R und der Quotient U/ι ist das Spektrum des Unterrings R^ι der Elemente, die unter der Gruppenwirkung invariant sind. Der Quotient A/ι kann durch Verklebung solcher affiner Quotienten erhalten werden.

Die ersten beschriebenen Kummer-Varietäten waren bestimmte Flächen, die der Mathematiker Ernst Eduard Kummer 1864 in [35] untersuchte, wenn auch in einem anderen Zusammenhang: Ausgangspunkt für Kummers Analyse war die sogenannte *Fresnelsche Wellenfläche*, welche als Modell für die Ausbreitung von Licht in Kristallen beschrieben worden war und die durch eine quartische Gleichung gegeben ist (siehe [34], S.118, Gl. 3). Mit seiner Theorie der Strahlensysteme ebenfalls auf dem Gebiet der geometrischen Optik tätig, bemerkte Kummer, dass die (reelle) Fresnelsche Wellenfläche über den komplexen Zahlen 16 singuläre Punkte besitzt. Dies sind Punkte, an denen die Fläche nicht glatt ist, sondern Spitzen auftreten. Die Zahl der Singularitäten entspricht zugleich der maximalen Anzahl an (isolierten) singulären Punkten einer komplexen quartischen Fläche, was Kummer veranlasste, allgemeiner alle Flächen vierten Grades mit 16 solchen singulären

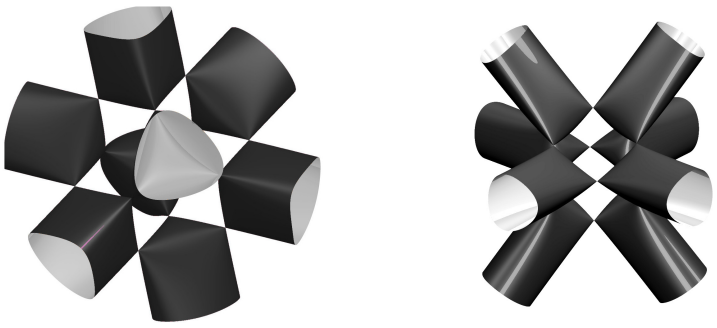


Abbildung 1: Reelles Bild einer Kummer-Fläche (verschiedene Perspektiven)

Punkten zu betrachten. Dabei dienten weiterhin Fragestellungen der Optik als Motivation, etwa nach den Konsequenzen, wenn eine solche Fläche als Brennfläche eines Strahlensystems auftritt, d. h. als der Ort aller Punkte, an denen mindestens zwei Strahlen zu einem vereinigt werden. Zu den Resultaten hierzu sagt Kummer selbst: „Durch diese besondere Eigenschaft der Flächen vierten Grades mit 16 singulären Punkten [...] bin ich zuerst auf die Wichtigkeit dieser Flächen vierten Grades aufmerksam gemacht worden." ([35], S. 431)

Zu Kummers Ergebnissen, die am stärksten nachwirken, gehören die Bestimmung der allgemeinen Gleichung einer quartischen Fläche mit 16 singulären Punkten und die Beobachtung, dass zu einer solchen Fläche im projektiven Raum $\mathbb{P}^3_{\mathbb{C}}$ 16 Ebenen existieren, sodass jeder singuläre Punkt auf sechs der Ebenen liegt und jede dieser Ebenen sechs der singulären Punkte enthält. Diese Konfiguration aus Punkten und Ebenen wird auch als *Kummer-Konfiguration* oder $(16, 6)$-*Konfiguration* bezeichnet, die untersuchten Quartiken als *Kummer-Flächen*. Der Zusammenhang zur anfangs gegebenen Definition von Kummer-Varietäten ist nach [20], Propositionen 4.22 und 4.23, wie folgt:

Proposition. *Jede Kummer-Fläche in $\mathbb{P}^3_{\mathbb{C}}$ ist isomorph zu einer Kummer-Varietät einer abelschen Fläche. Umgekehrt ist die Kummer-Varietät einer abelschen Fläche, die die Jacobi-Varietät einer glatten Kurve vom Geschlecht 2 ist, isomorph zu einer Kummer-Fläche in $\mathbb{P}^3_{\mathbb{C}}$.*

Häufig werden Kummer-Flächen auch als minimale Desingularisierung der singulären Kummer-Fläche definiert. Diese sind im oben beschriebenen Fall $K3$-*Flächen* (siehe [20], Thm. 3.4) und in einigen Fällen kann der Nachweis von Eigenschaften von $K3$-Flächen auf den Fall der (desingularisierten) Kummer-Flächen reduziert werden.

Im Rahmen dieser Arbeit wird mit dem Begriff Kummer-Fläche eine zweidimensionale Kummer-Varietät bezeichnet. Solange der Grundkörper k algebraisch abgeschlossen und von Charakteristik $\mathrm{char}(k) \neq 2$ ist, besitzen Kummer-Flächen wie zuvor 16 singuläre Punkte, bei denen es sich um die einfachsten Beispiele von Singularitäten handelt, den sogenannten A_1-*Flächensingularitäten*. Diese können durch ein *Blow-up* in jedem singulären Punkt aufgelöst werden, wobei anschaulich jeder singuläre Punkt durch einen projektiven Raum $\mathbb{P}^1_k$ ersetzt wird, während der Rest der Fläche unverändert bleibt. Abbildung 1 zeigt einen Teil einer Kummer-Fläche über den rellen Zahlen und in Abbildung 2 wird die Auflösung eines singulären Punktes dargestellt. Auch in höherer Dimension bleiben die Singularitäten von Kummer-Varietäten mild:

Theorem. *Es sei A eine g-dimensionale abelsche Varietät über einem algebraisch abgeschlossenen Grundkörper der Charakteristik $p \neq 2$. Es gelte $g \geq 2$. Die Kummer-Varietät $X = A/\iota$ besitzt genau 2^{2g} singuläre Punkte, die durch ein Blow-up mit dem singulären Ort als Zentrum aufgelöst werden können. Der exzeptionelle Divisor besteht dabei aus 2^{2g} disjunkten projektiven Räumen $\mathbb{P}^{g-1}_k$. Ist E eine irreduzible Komponente des exzeptionellen Divisors, dann ist $(E^g) = (-2)^{g-1}$ die Selbstschnittzahl.*

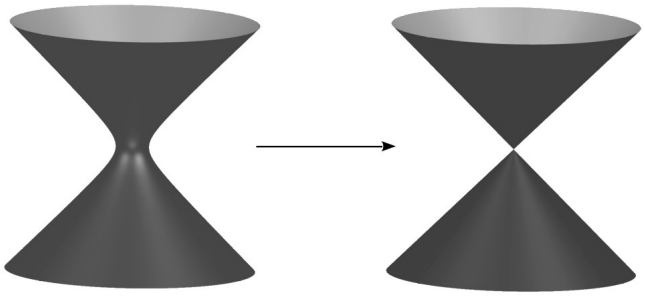


Abbildung 2: Auflösung der A_1-Singularität (reelles Bild)

Dieses Resultat ist bekannt, so wird es etwa in [14], Abschnitt 2.2, im Fließtext erwähnt, allerdings ohne Beweis oder genaue Voraussetzungen anzugeben. Da ein Beweis nicht auffindbar war, wird in Kapitel 2 ein eigener Beweis der Aussage gegeben. Die Beweisstrategie besteht darin, zuerst die Singularitäten (in Form der vervollständigten lokalen Ringe) durch die induzierte $\mathbb{Z}/2\mathbb{Z}$-Wirkung auf dem Kotangentialraum zu ermitteln und die weiteren Berechnungen mithilfe dieser Information „zu Fuß“ auszuführen.

Im Fall $\mathrm{char}(k) = 2$ ändert sich die Situation grundlegend. Für Kummer-Flächen sind die auftretenden Singularitäten und ihre Auflösungen seit den 1970er Jahren durch die Arbeiten [1], [2] von Artin, [51] von Shioda und [32] von Katsura bekannt. Kurioserweise wird der Isomorphietyp der auftretenden rationalen Singularitäten nicht explizit genannt (erst 2009 von Schröer in [48], Prop. 5.1, 5.2), obwohl der bloße Auflösungsgraph diese Information nicht enthält. Das folgende Theorem fasst Resultate aus [2], S. 64; [32], Prop. 8, und [48], Prop. 5.3, zusammen.

Es sei nun k algebraisch abgeschlossen von Charakteristik $p = 2$.

Theorem. *Es sei $X = A/\iota$ die Kummer-Fläche zu einer abelschen Fläche und $x \in X$ ein singulärer Punkt. Es sei r die Anzahl der singulären Punkte von X. Der vervollständigte lokale Ring $\hat{\mathcal{O}}_{X,x}$ ist dann isomorph zu einem der folgenden vollständigen Ringe:*

$$
\begin{array}{ll}
k[\![X_1, X_2, T]\!]/(T^2 + X_1X_2T + X_1^2X_2 + X_2^2X_1), & \text{wenn } r = 4, \\
k[\![X_1, V_2, T]\!]/(T^2 + X_1V_2^2T + X_1^2V_2 + V_2^4X_1), & \text{wenn } r = 2, \\
k[\![V_1, V_2, T]\!]/(T^2 + V_1^2V_2^2T + V_1^4V_2 + V_2^4V_1), & \text{wenn } r = 1,\ A \cong E \times E, \\
k[\![x, y, z]\!]/(z^2 + x^2bz + x^4y + xb^2), & \text{wenn } r = 1,\ A \ncong E \times E.
\end{array}
$$

Hierbei bezeichnen E die bis auf Isomorphie eindeutige supersinguläre elliptische Kurve ($j(E) = 0$) und $b = (q^4 + q)x + y^2$ für ein geeignetes Element $q \in k$.

Für endliche Produkte elliptischer Kurven und deren Kummer-Varietäten ist in dieser Arbeit eine derartige Beschreibung der Singularitäten durch die vervollständigten lokalen Ringe in jeder Dimension gelungen. Für gewöhnliche abelsche Varietäten konnte zudem

gezeigt werden, dass ihre Kummer-Varietäten „die gleichen Singularitäten“, d. h. mit isomorphem vervollständigten lokalen Ring, besitzen. (Eine ähnliche Verallgemeinerung ist auch für Kummer-Varietäten mit 2^{g-1} singulären Punkten möglich.) Stellvertretend für die anderen berechneten Fälle wird hier daher dieses Resultat aufgeführt:

Theorem. *Es sei A eine gewöhnliche g-dimensionale abelsche Varietät, d. h., die Gruppe $A(k)$ besitze genau 2^g Elemente der Ordnung höchstens 2. Es sei $X = A/\iota$ und es gelte $g \geq 2$. Der vervollständigte lokale Ring an jedem singulären Punkt von X ist isomorph zu*

$$k[\![T_M, X_i \mid M \subset \{1, \ldots, g\},\ i = 1, \ldots, g]\!]/J,$$

wobei das Ideal J von allen Polynomen der Form

$$T_\emptyset, \qquad X_i - T_{\{i\}}\,, \qquad \sum_{L \subsetneq D} X_{D\setminus L}\, T_L,$$
$$T_A T_B + \sum_{L \subsetneq A\cap B} X_{(A\cap B)\setminus L}\ P_L\ T_{(A\cup B)\setminus L} + P_{A\cap B} \sum_{M \subsetneq A\setminus B} X_{(A\setminus B)\setminus M}\ T_{M\cup(B\setminus A)}$$

erzeugt wird. Hierbei wird die abkürzende Schreibweise

$$X_M = \prod_{i\in M} X_i, \qquad P_M = \prod_{i\in M} (X_i^3 + X_i)$$

benutzt. Für die Indizes gilt $1 \leq i \leq g$, $A, B, D \subset \{1, \ldots, g\}$ mit $|D| \geq 3$ und $|A|, |B| \geq 2$.

Produkte elliptischer Kurven bieten sich in besonderer Weise als Beispielklasse an, weil sie durch Weierstraß-Gleichungen explizit beschrieben werden können. Ist E eine gewöhnliche elliptische Kurve, d. h., besitzt E einen Punkt der Ordnung 2, dann ist das Komplement des neutralen Elements $E\setminus\{O\}$ bereits ein ι-invariantes offenes affines Unterschema. Für die supersinguläre elliptische Kurve kann durch Entfernen von zwei Punkten eine offene affine ι-invariante Umgebung des neutralen Elements gefunden werden. Als geschickte Wahl in Hinblick auf die induzierte Wirkung haben sich die folgenden k-Algebren mit Involutionswirkung herausgestellt:

$$k[x,y]/(y^2 + xy + j_E^{\frac{1}{2}} x^3 + j_E^{-1} x), \quad x \mapsto x,\ y \mapsto y + x, \quad \text{wenn } E \text{ gewöhnlich}, \qquad (*)$$
$$k[v,w]/(w^2 + v^2 w + v), \qquad v \mapsto v,\ w \mapsto w + v^2, \quad \text{wenn } E \text{ supersingulär}. \qquad (**)$$

Ist $A = E_1 \times \ldots \times E_g$, dann liefern Tensorprodukte dieser k-Algebren den Koordinatenring eines offenen affinen Unterschemas von A, das genau einen Punkt der Ordnung ≤ 2 enthält. Die Unter-k-Algebra der invarianten Elemente ist wiederum der affine Koordinatenring eines offenen Unterschemas der zugehörigen Kummer-Varietät.

Die Gruppenwirkung in $(*)$ auf dem Polynomring $k[x_1, y_1, \ldots, x_g, y_g]$ bzw. auf dem

affinen Raum $\mathbb{A}_k^{2g}$ ist in der Modularen Darstellungstheorie eingehend studiert worden. Richman gab 1990 in [47], Proposition 2, ein Erzeugendensystem des Invariantenrings an. Richmans Resultat kann mithilfe der folgenden Proposition auf manche abgeschlossenen Unterschemata von $\mathbb{A}_k^{2g}$ übertragen werden. Insbesondere das eben beschriebene offene affine Unterschema von A kann als abgeschlossenes Unterschema von $\mathbb{A}_k^{2g}$ aufgefasst werden.

Proposition. *Es seien K ein Körper der Charakteristik $p > 0$ und $G = \mathbb{Z}/p\mathbb{Z}$ zyklisch der Ordnung p. Auf dem Polynomring $S = K[A_i, B_i \mid 1 \leq i \leq g]$ operiere G durch $A_i \mapsto A_i$, $B_i \mapsto B_i + A_i^{e_i}$ für $e_i \geq 1$. Weiter sei $I = (B_i^p - A_i^{(p-1)e_i} B_i + P_i(A_i),\ 1 \leq i \leq g) \subset S$ mit Polynomen $P_i \in A_i\, K[A_i]$. Dann induziert die Restklassenabbildung einen Isomorphismus*

$$S^G/I \cap S^G \cong (S/I)^G\,,$$

wobei die G-Wirkung auf S/I ebenso durch $A_i \mapsto A_i$, $B_i \mapsto B_i + A_i^{e_i}$ definiert ist.

Der Fall der Wirkung $(**)$ auf supersingulären Faktoren kann schließlich auf den gewöhnlichen Fall $(*)$ zurückgeführt werden.

Aufbau der Arbeit. In Kapitel 1 werden einige grundlegende Resultate über abelsche Varietäten und Quotienten nach einer endlichen Gruppenwirkung wiederholt. Weiterhin werden einige Begriffe der Kommutativen Algebra eingeführt, mit denen Eigenschaften der Singularitäten ausgedrückt werden können.

Der Fokus in Kapitel 2 liegt auf den Singularitäten von Kummer-Varietäten über einem algebraisch abgeschlossenen Körper, dessen Charakteristik nicht 2 beträgt. Es werden einige Resultate genannt und bewiesen, die größtenteils zwar bekannt sind, aber in der Literatur meist lediglich im Fließtext ohne Beweis oder genaue Voraussetzungen erwähnt werden. Darunter sind die Auflösung der Singularitäten mittels eines Blow-up und der Selbstschnitt des exzeptionellen Divisors. Zudem wird eine Inzidenzrelation zur Verallgemeinerung der $(16, 6)$-Konfiguration von Kummer-Flächen gegeben, die bislang nur im Flächenfall explizit benannt worden ist.

Den Hauptteil dieser Arbeit bildet Kapitel 3, in dem Kummer-Varietäten über einem algebraisch abgeschlossenen Körper der Charakteristik $p = 2$ betrachtet werden. Nach einer Zusammenfassung bekannter Resultate aus [51], [32] und [48] über Kummer-Flächen wird im folgenden Abschnitt 3.2 für Produkte elliptischer Kurven ein offenes affines Unterschema der Kummer-Varietät berechnet und in Form des Koordinatenrings angegeben. Hieraus werden die auftretenden Singularitäten in Form des vervollständigten lokalen Rings bestimmt. Durch den Nachweis der Isomorphie der jeweiligen assoziierten formalen Gruppen kann in Abschnitt 3.3 gezeigt werden, dass sich die Berechnung der Singularitäten auf Kummer-Varietäten von gewöhnlichen abelschen Varietäten ausdehnen lässt.

Danksagung. Auch wenn auf dem Titel nur mein Name erscheint, wäre die Erstellung dieser Arbeit ohne die Unterstützung vieler Anderer nicht möglich gewesen.

Zuallererst danke ich meinem Betreuer Prof. Dr. Stefan Schröer für das herausfordernde Thema, die fachlichen Diskussionen und seine Unterstützung, vor allem während der letzten Monate.

Weiterer Dank gebührt meinen Kollegen am Mathematischen Institut für das angenehme Arbeitsklima. Insbesondere möchte ich Ulrike Alba und Petra Simons für ihre unermüdliche Hilfe bei allen organisatorischen Problemen danken. Steffen Kionke, Lina Wedrich und André Schell danke ich herzlich für das Korrekturlesen von Teilen dieser Arbeit. Dies gilt umso mehr für Leif Zimmermann, der sich über das Korrekturlesen hinaus auch viel Zeit für Diskussionen genommen hat.

Zum guten Schluss danke ich natürlich meinen Eltern für ihre stete Unterstützung während meines gesamten Studiums.

Vielen Dank!

1 Grundlagen

Kummer-Varietäten sind per Definition Quotienten abelscher Varietäten nach der Wirkung der Vorzeicheninvolution. Um die genannte Definition greifbarer zu machen, werden in den Abschnitten 1.1 und 1.2 einige Eigenschaften abelscher Varietäten und die Konstruktion des Quotienten rekapituliert. In Abschnitt 1.3 werden einige Begriffe der Kommutativen Algebra eingeführt, welche für die genauere Analyse der Singularitäten in den späteren Kapiteln gebraucht werden und mit denen bereits erste Eigenschaften von Kummer-Varietäten wie Normalität angegeben werden können. Im letzten Abschnitt wird die Technik des Blow-up eingeführt, mit der im Fall klassischer Kummer-Varietäten die Singularitäten leicht aufgelöst werden können.

1.1 Abelsche Varietäten

Die wichtigste Referenz für diesen Abschnitt sind die Monographie [42] und die darauf basierende, etwas strukturierter aufgeschriebene Zusammenfassung [40].

Zur Vorbereitung beginnen wir mit der Definition von Gruppenobjekten im Sinne der Kategorientheorie.

Definition 1.1. Es sei $\mathcal{C}$ eine Kategorie mit endlichen Produkten und einem terminalen Objekt t. Ein Objekt G in $\mathcal{C}$, zusammen mit Morphismen $\mu\colon G \times G \to G$, $\iota\colon G \to G$, $e\colon t \to G$, wird *Gruppenobjekt* genannt, wenn die folgenden drei Diagramme kommutativ sind:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mu\times\mathrm{id}} & G \times G \\ \downarrow{\scriptstyle \mathrm{id}\times\mu} & & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow{\mu} & G, \end{array} \tag{1.1}$$

welches auch als Assoziativgesetz bezeichnet wird; sowie

$$\begin{array}{ccccc} G \times G & \xleftarrow{e\times\mathrm{id}} & t \times G \cong G \cong G \times t & \xrightarrow{\mathrm{id}\times e} & G \times G \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mu} \\ G & \xleftarrow{\mathrm{id}} & G & \xrightarrow{\mathrm{id}} & G \end{array} \tag{1.2}$$

und

$$\begin{array}{ccccc} G & \longrightarrow & t & \longleftarrow & G \\ \downarrow{\scriptstyle (\mathrm{id},\iota)} & & \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle (\iota,\mathrm{id})} \\ G \times G & \xrightarrow{\mu} & G & \xleftarrow{\mu} & G \times G, \end{array} \tag{1.3}$$

in denen die Existenz eines neutralen Elements bzw. die Existenz inverser Elemente dargestellt wird.

Ist $\mathcal{C}$ die Kategorie der Schemata (über einem Körper k), so spricht man auch von *Gruppenschemata*. Eine *algebraische Gruppe* über einem Körper k kann nun als geometrisch reduziertes, separiertes Gruppenschema von endlichem Typ über k definiert werden. Abelsche Varietäten sind besondere algebraische Gruppen:

Definition 1.2. Eine *abelsche Varietät* A über einem Grundkörper k ist ein Gruppenschema A, das zusammenhängend, geometrisch reduziert und eigentlich über k ist.

Abelsche Varietäten sind auch geometrisch irreduzibel und insbesondere geometrisch integer, denn für algebraische Gruppen stimmen nach [6], Proposition in I.1.2, die Begriffe „irreduzibel“ und „zusammenhängend“ überein und, da $A(k) \neq \emptyset$, bleibt A über k^{sep} zusammenhängend.

Für jedes k-Schema T induzieren die Morphismen e, μ und ι eine Gruppenstruktur auf der Menge $A(T) = \mathrm{Hom}(T, A)$. Im Fall $T = \mathrm{Spec}(k)$ schreiben wir auch kurz $A(k)$. Wir identifizieren die Morphismen $x \in A(k)$ mit den Bildpunkten, den rationalen Punkten von A, und lassen die Unterscheidung häufig fallen.

Für jeden rationalen Punkt $x \in A$ ist die *Translation um x* definiert als der Morphismus $t_x \colon A \cong A \times \mathrm{Spec}(k) \to A$, welcher durch $t_x = \mu \circ (\mathrm{id} \times x)$ gegeben ist. Die Translationen sind Automorphismen, da t_x und $t_{\iota(x)}$ invers zueinander sind. Ein *Homomorphismus* $h \colon A \to B$ zwischen abelschen Varietäten ist ein Morphismus von k-Schemata, der verträglich mit dem Gruppengesetz ist, d. h., es gilt $\mu_B \circ (h \times h) = h \circ \mu_A$. Wird von einem Morphismus zwischen abelschen Varietäten gesprochen, ist damit ein Morphismus von k-Schemata gemeint. Das folgende Resultat (siehe z. B. [40], Cor. 2.2) zeigt die enge Verbindung zwischen Morphismen und Homomorphismen:

Proposition 1.3. *Jeder Morphismus $f \colon A \to B$ zwischen zwei abelschen Varietäten ist die Komposition aus einem Homomorphismus und einer Translation. Genauer: Bezeichnet $b = f(e_A)$ das Bild des neutralen Elements, dann ist $f = t_b \circ h$ für einen Homomorphismus $h \colon A \to B$.*

Insbesondere ist die Inversion ι ein Homomorphismus, denn ι respektiert das neutrale Element. Als Anwendung ergibt sich als Korollar, warum überhaupt von *abelschen* Varietäten gesprochen wird:

Korollar 1.4. *Abelsche Varietäten sind kommutativ.*

Beweis. Wir zeigen, dass alle Kommutatoren trivial sind, d. h., wir zeigen, dass der Morphismus $\mu \circ (\mu, \mu \circ (\iota \times \iota)) \colon A \times A \to A$ konstant mit Bildpunkt $e \in A(k)$ ist. Aus Proposition 1.3 folgt sofort, dass ι ein Homomorphismus ist. Damit besteht das Bild von $\mu \circ (\mu, \mu \circ (\iota \times \iota)) = \mu \circ (\mu, \iota \circ \mu)$ nur aus dem neutralen Element. □

Das Gruppengesetz μ wird daher in der Regel additiv als Verknüpfung „+“ notiert, während $\iota(x) = -x$ als negatives Vorzeichen geschrieben wird. Der Morphismus ι wird aus diesem Grund im weiteren Verlauf als *Vorzeicheninvolution* bezeichnet. Durch sukzessives Anwenden des Gruppengesetzes μ erhält man einen Morphismus n_A, der als Multiplikation mit einer natürlichen Zahl n gedeutet werden kann. Eine andere Sicht hierauf ist folgende: Für jede ganze Zahl n und jede k-Algebra L kann der Gruppenhomomorphismus $n_A(L) \colon A(L) \to A(L),\ a \mapsto n \cdot a$ definiert werden. Dies ist eine natürliche Transformation des Punktefunktors $A(\,.\,) = \mathrm{Hom}(\,.\,, A)$ und liefert nach dem Yoneda-Lemma einen Morphismus n_A von k-Schemata ([21], Cor. 4.7). Speziell kann die Vorzeicheninvolution ι auch aufgefasst werden als der Morphismus $(-1)_A$.

Ist $f \colon A \to B$ ein Homomorphismus zwischen abelschen Varietäten, so kann auch vom Kern $\ker(f) = f^{-1}(e_B)$ gesprochen werden. Dieser ist ein Untergruppenschema von A. Von besonderer Bedeutung sind surjektive Homomorphismen mit endlichem Kern. Diese Eigenschaft von f besitzt eine Reihe äquivalenter Charakterisierungen (siehe z. B. [40], Prop. 8.1):

Proposition 1.5. *Es sei $f \colon A \to B$ ein Homomorphismus zwischen abelschen Varietäten. Die folgenden Aussagen sind äquivalent:*

(i) Das Schema $\ker(f)$ *ist ein endliches Gruppenschema und f ist surjektiv.*

(ii) Das Schema $\ker(f)$ *ist ein endliches Gruppenschema und es gilt* $\dim(A) = \dim(B)$.

(iii) Der Morphismus f ist surjektiv und es gilt $\dim(A) = \dim(B)$.

(iv) Der Morphismus f ist endlich, flach und surjektiv.

Definition 1.6. Erfüllt ein Morphismus $f \colon A \to B$ die äquivalenten Bedingungen aus Proposition 1.5, so bezeichnet man ihn als *Isogenie*. Der Erweiterungsgrad $[k(A) : k(B)]$ heißt dann auch *Grad der Isogenie*. Er stimmt nach [21], Proposition 12.21, überein mit der k-Vektorraumdimension von $\Gamma(\ker(f), \mathscr{O}_{\ker(f)})$.

Obige Definition des Grades stimmt mit der üblichen Definition des Grades eines endlichen Morphismus überein und kann daher als Spezialfall aufgefasst werden. Aus der Multiplikationsformel für Erweiterungsgrade folgt, dass bei der Verkettung von Isogenien die Grade multipliziert werden, also $\deg(f \circ g) = \deg(f)\deg(g)$ gilt.

Die Morphismen der Form $n_A\colon A \to A$ für $n \neq 0$ sind Isogenien. Für den Beweis hierzu und die Berechnung des Grades benötigen wir zwei Resultate. Das erste Resultat, das *Theorem of the Cube* (siehe [40], Thm. 6.1), gibt als Korollar eine Formel für das Pullback invertierbarer Garben bzgl. n_A:

Theorem 1.7. *Es seien U, V, W geometrisch integre eigentliche Schemata über einem Körper k mit rationalen Punkten $u \in U(k)$, $v \in V(k)$, $w \in W(k)$. Weiter sei $\mathscr{L}$ eine invertierbare Garbe auf $U \times V \times W$, sodass die Einschränkungen $\mathscr{L}|_{\{u\}\times V\times W}$, $\mathscr{L}|_{U\times\{v\}\times W}$ und $\mathscr{L}|_{U\times V\times\{w\}}$ trivial, d. h. isomorph zur jeweiligen Strukturgarbe, sind. Dann ist auch $\mathscr{L}$ trivial.*

Das Theorem lässt sich insbesondere auf den Fall $U = V = W = A$ anwenden. Mithilfe von Pullbacks bzgl. Projektionen ergibt sich das folgende Korollar (siehe [40], Cor. 6.5):

Korollar 1.8. *Es seien A eine abelsche Varietät und $f_1, f_2, f_3\colon A \to A$ Morphismen. Für jede invertierbare Garbe $\mathscr{L}$ auf A ist*

$$(f_1 + f_2 + f_3)^*\mathscr{L} \otimes \bigotimes_{1\leq i<j\leq 3} (f_i + f_j)^*\mathscr{L}^{-1} \otimes \bigotimes_{1\leq i\leq 3} f_i^*\mathscr{L} \tag{1.4}$$

isomorph zur Struktugarbe $\mathscr{O}_A$.

Beweis. Wir betrachten zunächst die folgenden Morphismen $A \times A \times A \to A$: Es seien p_i die Projektion auf den i-ten Faktor, $p_{ij} = p_i + p_j$ und $p_{123} = p_1 + p_2 + p_3$, wobei die Addition die Verkettungen mit dem Gruppengesetz μ bezeichnet. Weiter sei

$$\mathscr{F} = p_{123}^*\mathscr{L} \otimes \bigotimes_{1\leq i<j\leq 3} p_{ij}^*\mathscr{L}^{-1} \otimes \bigotimes_{1\leq i\leq 3} p_i^*\mathscr{L}.$$

Die Einschränkung von $\mathscr{F}$ auf $\{e\} \times A \times A$ ist

$$p_{23}^*\mathscr{L} \otimes p_{23}^*\mathscr{L}^{-1} \otimes p_3^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L} \otimes p_3^*\mathscr{L} \;\cong\; \mathscr{O}_{\{e\}\times A\times A},$$

Analoges gilt für die Einschränkungen auf $A\times\{e\}\times A$ und $A\times A\times\{e\}$. Nach dem Theorem of the Cube ist $\mathscr{F}$ auf $A \times A \times A$ trivial. Die Garbe in (1.4) ist das Pullback von $\mathscr{F}$ unter dem Morphismus $(f_1, f_2, f_3)\colon A \to A \times A \times A$ und daher isomorph zu $\mathscr{O}_A$. □

Wir erhalten hieraus eine Beschreibung von $n_A^*\mathscr{L}$, die wir im folgenden Korollar (siehe z. B. [40], Cor. 6.6) geben. Wir schreiben kurz $\mathscr{L}^m$ statt $\mathscr{L}^{\otimes m}$.

Korollar 1.9. *Es seien $n \neq 0$ eine ganze Zahl und A eine abelsche Varietät. Dann gilt*

$$n_A^*\mathscr{L} \cong \mathscr{L}^{\frac{n^2+n}{2}} \otimes (-1)_A^*\mathscr{L}^{\frac{n^2-n}{2}}, \tag{1.5}$$

für jede invertierbare Garbe $\mathscr{L}$ auf A.

Im Fall, dass $\mathscr{L} \cong (-1)_A^*\mathscr{L}$ gilt, vereinfacht sich (1.5) zu $n_A^*\mathscr{L} \cong \mathscr{L}^{n^2}$. Eine solche invertierbare Garbe wird auch als *symmetrisch* bezeichnet.

Beweis. Der Beweis erfolgt mit vollständiger Induktion. Für $n = 1$ ist in (1.5) nichts zu zeigen. Wir beweisen die Aussage nun für (positives) $n+1$ und nehmen an, dass die Formel für alle kleineren positiven Zahlen gilt. Aus Korollar 1.8 ergibt sich mit $f_1 = n_A$, $f_2 = 1_A$, $f_3 = (-1)_A$ die Beziehung

$$\begin{aligned} \mathscr{O}_A &\cong n_A^*\mathscr{L} \otimes (n+1)_A^*\mathscr{L}^{-1} \otimes (n-1)_A^*\mathscr{L}^{-1} \otimes n_A^*\mathscr{L} \otimes \mathscr{L} \otimes (-1)_A^*\mathscr{L} \\ \iff (n+1)_A^*\mathscr{L} &\cong n_A^*\mathscr{L}^2 \otimes (n-1)_A^*\mathscr{L}^{-1} \otimes \mathscr{L} \otimes (-1)_A^*\mathscr{L}. \end{aligned}$$

Durch Anwenden der Induktionsvoraussetzung kann die rechte Seite umgeformt werden zu

$$\begin{aligned} (n+1)_A^*\mathscr{L} &\cong \mathscr{L}^{(n^2+n+\frac{-(n-1)^2-(n-1)}{2}+1)} \otimes (-1)_A^*\mathscr{L}^{(n^2-n+\frac{-(n-1)^2+(n-1)}{2}+1)} \\ &\cong \mathscr{L}^{\frac{n^2+3n+2}{2}} \otimes (-1)_A^*\mathscr{L}^{\frac{n^2+n}{2}} = \mathscr{L}^{\frac{(n+1)^2+(n+1)}{2}} \otimes (-1)_A^*\mathscr{L}^{\frac{(n+1)^2-(n+1)}{2}}, \end{aligned}$$

was die Aussage für positive n beweist. Für $n < 0$ kann $n_A = (-1)_A \circ (-n)_A$ geschrieben werden und die Aussage folgt. □

Um neben dem Nachweis der Isogenie-Eigenschaften auch den Grad der Isogenie n_A auszurechnen, wird als zweites Resultat die Existenz einer amplen invertierbaren Garbe gebraucht (siehe z. B. [40], Thm. 7.1):

Theorem 1.10. *Jede abelsche Varietät A ist projektiv.*

Über den komplexen Zahlen kann jede abelsche Varietät als komplexer Torus $\mathbb{C}^g/\Lambda$ für ein Gitter $\Lambda \subset \mathbb{C}^g$ aufgefasst werden. Ist umgekehrt $\mathbb{C}/\Lambda$ ein eindimensionaler komplexer Torus, so existiert auch eine elliptische Kurve E, sodass $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ gilt (siehe etwa [52], Prop. VI.3.6). Allgemeiner stammt ein komplexer Torus genau dann von einer abelschen Varietät, wenn er (holomorph) in $\mathbb{P}^n(\mathbb{C})$ eingebettet werden kann (Chow's Theorem, siehe [42], S. 33). Im Fall $g \geq 2$ besitzt nicht jeder komplexe Torus diese Eigenschaft.

Mit den genannten Resultaten kann nun die Isogenie-Eigenschaft für die Homomorphismen n_A nachgewiesen werden:

Theorem 1.11. *Es seien A eine abelsche Varietät der Dimension g und $n \neq 0$ eine ganze Zahl. Dann ist der Morphismus $n_A \colon A \to A$, $x \mapsto n \cdot x$ eine Isogenie vom Grad n^{2g}.*

Wir folgen dem Beweis von Theorem 8.2 in [40]:

Beweis. Es sei $\mathscr{F}$ eine ample invertierbare Garbe auf A. Da $(-1)_A = \iota$ ein Automorphismus ist, ist auch $(-1)_A^*\mathscr{F}$ und somit $\mathscr{L} = \mathscr{F} \otimes (-1)_A^*\mathscr{F}$ ampel. Offensichtlich ist $\mathscr{L}$

symmetrisch, d. h. $(-1)_A^*\mathscr{L} \cong \mathscr{L}$. Nach (1.5) gilt $n_A^*\mathscr{L} \cong \mathscr{L}^{n^2}$ und auch $n_A^*\mathscr{L}$ ist ampel. Die Einschränkung einer amplen Garbe auf ein abgeschlossenes Unterschema ist wieder ampel, was insbesondere auch für die Einschränkung von $n_A^*\mathscr{L}$ auf $\ker(n_A)$ gilt. Andererseits ist diese Restriktion trivial, da die Verkettung $\ker(n_A) \hookrightarrow A \xrightarrow{n_A} A$ konstant ist, also ist die Strukturgarbe von $\ker(n_A)$ ampel. Für jede kohärente Garbe $\mathscr{M}$ auf $\ker(n_A)$ gilt daher $H^i(\ker(n_A), \mathscr{M}) = H^i(\ker(n_A), \mathscr{M} \otimes \mathscr{O}_{\ker(n_A)}^m) = 0$ für alle $i > 0$ (siehe z. B. [24], Prop. III.5.3). Nach Serres Verschwindungssatz (Thm. III.3.7 in [24]) ist das Schema $\ker(n_A)$ affin, also $\ker(n_A) = \mathrm{Spec}(R)$ für eine endlich erzeugte k-Algebra R. Da es sich bei $\ker(n_A)$ um ein eigentliches k-Schema handelt, ist $R = \Gamma(\ker(n_A), \mathscr{O}_{\ker(n_A)})$ ein endlich-dimensionaler k-Vektorraum ([21], Thm. 12.65). Nach Proposition 1.5 ist n_A eine Isogenie.

Für die Berechnung des Grades der Isogenie benutzen wir Schnittzahlen. Wir können annehmen, dass k algebraisch abgeschlossen ist, da sich beim Tensorieren mit $\bar{k}$ die Vektorraumdimension von R nicht ändert. Es sei $\mathscr{L}$ wie oben ampel und symmetrisch. Es seien $\mathscr{L}_i$ für $1 \leq i \leq g-1$ invertierbare Garben auf A und $(n_A^*\mathscr{L} \cdot \mathscr{L}_1 \cdots \mathscr{L}_{g-1})$ die Schnittzahl. Diese ist per Definition der Koeffizient des Monoms $x_1 \cdots x_{g-1}$, der in der Euler-Charakteristik $\chi(\mathscr{L} \otimes \mathscr{L}_1^{x_1} \otimes \ldots \otimes \mathscr{L}_{g-1}^{x_{g-1}})$ auftritt. Da die Schnittform multilinear ist (siehe [3], Lemma 1.6) und $n_A^*\mathscr{L} \cong \mathscr{L}^{n^2}$ gilt, folgt

$$(n_A^*\mathscr{L} \cdot \mathscr{L}_1 \cdots \mathscr{L}_{g-1}) = n^2 \cdot (\mathscr{L} \cdot \mathscr{L}_1 \cdots \mathscr{L}_{g-1}).$$

Wir wählen nun $\mathscr{L}_i = \mathscr{L}$ und betrachten den Selbstschnitt von $\mathscr{L}$. Nach [3], Lemma 1.18, wandelt die Schnittform das Pullback entlang eines Morphismus in Multiplikation mit dem Grad um, also

$$\deg(n_A) \cdot (\mathscr{L} \cdot \mathscr{L} \cdots \mathscr{L}) = (n_A^*\mathscr{L} \cdot n_A^*\mathscr{L} \cdots n_A^*\mathscr{L}) = n^{2g} \cdot (\mathscr{L} \cdot \mathscr{L} \cdots \mathscr{L}),$$

wobei für die letzte Gleichheit wieder die Multilinearität genutzt wurde. Da $\mathscr{L}$ ampel ist, muss der Selbstschnitt von $\mathscr{L}$ positiv sein, was man etwa mit dem Nakai–Moishezon-Kriterium ([3], Thm. 1.22) sehen kann. Also ist $\deg(n_A) = n^{2g}$ erfüllt. □

Korollar 1.12. *Es sei k algebraisch abgeschlossen. Die Gruppe der rationalen Punkte $A(k)$ ist eine divisible Gruppe, d. h., zu jedem $x \in A(k)$ und jedem $n \in \mathbb{N}$ existiert ein $y \in A(k)$ mit $ny = x$.*

Nachdem nun bekannt ist, dass der Kern von n_A ein endliches Gruppenschema ist, stellt sich die Frage, wie viele Elemente die Gruppe $\ker(n_A)(k)$ besitzt und welche endliche abelsche Gruppe vorliegt. Die Zahl der rationalen Punkte ist zwar durch den Grad der Isogenie beschränkt, sie kann aber auch kleiner sein. Über einem algebraisch abgeschlossenen Körper tritt dieser Fall auf, wenn die induzierte Erweiterung der Funktionenkörper

nicht separabel ist, wie die folgende Proposition (siehe [5], A 12.9) zeigt:

Proposition 1.13. *Es seien k algebraisch abgeschlossen, X und Y zwei integre eigentliche k-Schemata der gleichen Dimension und $\phi\colon X \to Y$ ein dominanter Morphismus. Dann existiert ein offenes Unterschema U von Y, sodass die Einschränkung $\phi^{-1}(U) \to U$ ein endlicher Morphismus ist. Für jeden Punkt $x \in U(k)$ besitzen die Fasern $\phi^{-1}(x)$ die Kardinalität $[k(X) : k(Y)]_{\mathrm{sep}}$, den Separabilitätsgrad der Körpererweiterung.*

Für den Fall einer Isogenie gibt der Separabilitätsgrad die Kardinalität aller Fasern von rationalen Punkten an, insbesondere also auch die des Kerns. Die Bedingung $k = \bar{k}$ ist hier notwendig, um sicherzustellen, dass alle abgeschlossenen Punkte auch rationale Punkte sind.

Bei separablen Erweiterungen der Funktionenkörper verlaufen viele Beweise über Berechnungen im Tangentialraum bzw. dessen Dualraum, dem Kotangentialraum. Der Tangentialraum $T_x(X)$ eines k-Schemas an einem Punkt $x \in X$ ist per Definition der Vektorraum $\mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k)$. Für einen Morphismus $f\colon X \to Y$ erhält man aus dem lokalen Ringhomomorphismus $\mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ einen Homomorphismus von Vektorräumen $\mathfrak{m}_{f(x)}/\mathfrak{m}_{f(x)}^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$, wenn die Restekörper von x und $f(x)$ übereinstimmen. Durch Dualisieren erhält man eine lineare Abbildung $T_x f\colon T_x(X) \to T_{f(x)}(Y)$, die auch als Ableitung von f bezeichnet wird. Die Ableitung des Gruppengesetzes am neutralen Element liefert dabei die Addition im Vektorraum (siehe [6], I.3.2):

Lemma 1.14. *Der vom Gruppengesetz $\mu\colon A \times A \to A$ induzierte Morphismus auf den Tangentialräumen*

$$T_{(e,e)}\mu\colon\ T_{(e,e)}(A \times A) \cong T_e(A) \oplus T_e(A) \longrightarrow T_e(A)$$

ist durch die Vektorraumaddition $T_{(e,e)}\mu(x, y) = x + y$ gegeben.

Wir können nun Aufschluss über die abelsche Gruppe $\ker(n_A)(\bar{k})$ geben. Im Fall, dass n kein Vielfaches von $\mathrm{char}(k)$ ist, folgen wir dem Beweis in [42], S. 63:

Proposition 1.15. *Es seien A eine g-dimensionale abelsche Varietät über einem algebraisch abgeschlossenen Körper k und $n \in \mathbb{N}$ teilerfremd zu $\mathrm{char}(k)$. Für die Untergruppe H der n-Torsionspunkte von $A(k)$ gilt dann*

$$H = \ker(n_A)(k) \cong (\mathbb{Z}/n\mathbb{Z})^{\oplus 2g}.$$

Insbesondere hängt die Ordnung von H nur von g und n ab.

Beweis. Die von n_A induzierte Abbildung $T_e(n_A)\colon T_e(A) \to T_e(A)$ auf dem Tangentialraum ist durch $x \mapsto n \cdot x$ gegeben: Wir schreiben dazu n_A als Komposition einer Diagonaleinbettung $\Delta\colon A \to A \times \ldots \times A$ und einer Iteration des Gruppengesetzes μ. Die Ableitung

des Diagonalmorphismus ist dabei wieder eine Diagonaleinbettung

$$T_e(\Delta)\colon T_e(A) \longrightarrow T_{(e,\ldots,e)}(A \times \ldots \times A) \cong T_e(A) \oplus \ldots \oplus T_e(A)$$

und die Behauptung folgt induktiv aus Lemma 1.14.

Da n in k invertierbar ist, ist $T_e(n_A)$ ein Isomorphismus. Durch Verketten mit Translationen sieht man, dass $T_x(n_A)$ für alle abgeschlossenen Punkte $x \in A$ ein Isomorphismus ist: Es gilt ja $n_A = t_{nx} \circ n_A \circ t_{-x}$ und damit

$$T_x(n_A) = T_e(t_{nx}) \circ T_e(n_A) \circ T_x(t_{-x}),$$

was als Verkettung von Isomorphismen auch ein Isomorphismus ist. Damit ist n_A glatt von relativer Dimension 0 (siehe [24], Prop. III.10.4), also étale. Die Körpererweiterungen $\kappa(n_A(x)) \hookrightarrow \kappa(x)$ sind daher für alle $x \in A$ endlich und separabel, speziell gilt dies für den generischen Punkt. Der Grad der Isogenie n_A stimmt daher mit dem Separabilitätsgrad überein und H besitzt n^{2g} Punkte.

Der Hauptsatz über endlich erzeugte abelsche Gruppen impliziert nun, dass H von der Form

$$H \cong \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}, \quad d_1 | \ldots | d_r \,|\, n, \; d_1 \cdots d_r = n^{2g}$$

sein muss. Wir betrachten zu $d := d_1$ die Untergruppe $H' = \ker(d_A)(k)$ von H, welche nun Aufschluss über die genaue Gruppenstruktur gibt: Jeder der Summanden von H besitzt eine eindeutig bestimmte zyklische Untergruppe der Ordnung d, also gilt $|H'| = d^r$. Auf der anderen Seite folgt mit obigem Beweis für d_A auch $|H'| = d^{2g}$. Folglich gilt $r = 2g$, $d_1 = \ldots = d_r = n$. □

Für den Fall, dass die Charakteristik p des Grundkörpers ein Teiler von n ist, funktioniert das Argument nicht mehr, da die induzierte Abbildung $T_e(n_A)$ die Nullabbildung auf dem Tangentialraum ist. Tatsächlich kann die Anzahl der n-Torsionspunkte variieren.

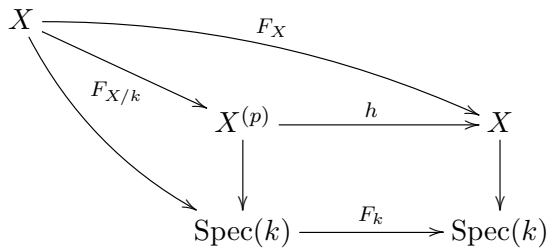
Proposition 1.16. *Es sei A eine g-dimensionale abelsche Varietät über einem algebraisch abgeschlossenen Körper der Charakteristik $p > 0$. Es existiert ein $f \in \{0, \ldots, g\}$, sodass*

$$\ker(p_A^m)(k) \cong (\mathbb{Z}/p^m\mathbb{Z})^{\oplus f}$$

für jedes $m \geq 1$ gilt.

Im Beweis wird der Frobenius-Morphismus eine wichtige Rolle spielen. Wir erinnern daran, dass der absolute Frobenius-Morphismus $F_X\colon X \to X$ für ein k-Schema X aus der Identität auf dem zugrundeliegenden topologischen Raum und dem Garbenhomomorphismus $\mathscr{O}_X(U) \to \mathscr{O}_X(U),\ a \mapsto a^p$ besteht. Der relative Frobenius-Morphismus

$F_{X/k}\colon X \to X^{(p)}$ ist durch die universelle Eigenschaft des Faserprodukts



gegeben. Da k als algebraisch abgeschlossen vorausgesetzt wird, insbesondere also perfekt ist, sind die Morphismen $F_k = F_{\mathrm{Spec}(k)}$ und h als dessen Basiswechsel Isomorphismen.

Beweis. Wir betrachten zunächst den Fall $m = 1$, also den Kern von p_A. Der allgemeine Fall wird anschließend mit vollständiger Induktion bewiesen. Nach [11], Exposé VII_A, Absatz 4.3, kann der Morphismus p_A als Komposition aus (relativem) *Frobenius-* und *Verschiebungsmorphismus*

$$p_A : A \xrightarrow{F_{A/k}} A^{(p)} \xrightarrow{V_{A/k}} A \tag{1.6}$$

geschrieben werden. Die Verschiebung kann durch (1.6) definiert werden als die zu $F_{A/k}$ duale Isogenie. Bei $F_{A/k}$ handelt es sich um einen endlichen Morphismus, der eine rein inseparable Körpererweiterung $k(A^{(p)}) \subset k(A)$ induziert: Dazu wählen wir eine offene affine Teilmenge $U = \mathrm{Spec}(R)$ von A mit $R = k[T_i,\, i \in I]/(h_j,\, j \in J)$ und bilden das offene affine Unterschema $U^{(p)} \subset A^{(p)}$, indem der Frobeniusmorphismus von k auf die Koeffizienten der h_j angewendet wird ([21], 4.24). Dann wird $F_{A/k}|_U\colon U \to U^{(p)}$ durch den Homomorphismus induziert, der durch $T_i \mapsto T_i^p$ gegeben ist. Der Körper der Brüche von R besitzt Transzendenzgrad g, der Grad des Frobenius bzw. der Grad der Körpererweiterung beträgt folglich mindestens p^g. Damit besitzt die von $V_{A/k}$ induzierte Erweiterung $k(A^{(p)})/k(A)$ höchstens Grad p^g. Der Separabilitätsgrad dieser Erweiterung ist p^f für geeignetes $f \leq g$ und gibt nach Proposition 1.13 die Ordnung der Gruppe $\ker(p_A)(k)$. Da diese Gruppe abelsch ist und jedes Element außer dem neutralen Element die Ordnung p besitzt, kann es sich nur um eine direkte Summe von Kopien der zyklischen Gruppe handeln.

Es sei nun $m > 1$ und es gelte $\ker(p_A^d)(k) = (\mathbb{Z}/p^d\mathbb{Z})^{\oplus f}$ für alle $d < m$. Da $A(k)$ eine divisible Gruppe ist, kann jeder p-Torsionspunkt von $\ker(p_A)(k)$ als das p^{m-1}-fache eines p^m-Torsionspunktes geschrieben werden. Wir erhalten dadurch die kurze exakte Sequenz

$$0 \longrightarrow \underbrace{\ker(p_A^{m-1})(k)}_{\cong(\mathbb{Z}/p^{m-1}\mathbb{Z})^{\oplus f}} \longrightarrow \ker(p_A^m)(k) \xrightarrow{\cdot p^{m-1}} \underbrace{\ker(p_A)(k)}_{\cong(\mathbb{Z}/p\mathbb{Z})^{\oplus f}} \longrightarrow 0$$

von abelschen Gruppen. Um die Bedingungen aus der exakten Sequenz zu erfüllen, muss $\ker(p_A^m)(k) \cong (\mathbb{Z}/p^m\mathbb{Z})^{\oplus f}$ gelten. □

Ist $\mathrm{char}(k) = p$ und $n = n' \cdot p^m$ mit n' teilerfremd zu p, dann ist $\ker(p_A^m)$ die eindeutige p-Sylow-Untergruppe von $\ker(n_A)$. Da endliche abelsche Gruppen als Produkt ihrer Sylow-Untergruppen geschrieben werden können, ergibt sich $\ker(n_A) \cong \ker(n'_A) \times \ker(p_A^m)$.

1.2 Quotienten nach endlicher Gruppenwirkung

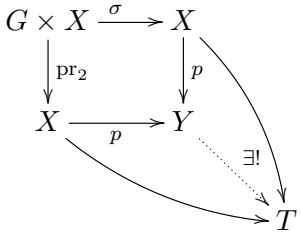
Da es sich bei Kummer-Varietäten um Quotienten von abelschen Varietäten handelt, wird zunächst noch die Konstruktion von Quotienten nach endlicher Gruppenwirkung erläutert, bevor Kummer-Varietäten definiert werden.

Definition 1.17. Es sei $\mathcal{C}$ eine Kategorie mit einem terminalen Objekt t, in der endliche Produkte existieren. Eine *Gruppenoperation* oder *Gruppenwirkung* eines Gruppenobjekts G auf einem Objekt X von links ist ein Morphismus $\sigma\colon G \times X \to X$, sodass

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{\mathrm{id}_G \times \sigma} & G \times X \\ \downarrow{\scriptstyle \mu \times \mathrm{id}_X} & & \downarrow{\scriptstyle \sigma} \\ G \times X & \xrightarrow[\sigma]{} & X \end{array}$$

kommutativ ist und sodass die Verkettung $X \cong t \times X \xrightarrow{e \times \mathrm{id}_X} G \times X \xrightarrow{\sigma} X$ die Identität auf X ist. Dabei bezeichnen $e\colon t \to G$ den Morphismus, der das neutrale Element beschreibt, und $\mu\colon G \times G \to G$ das Gruppengesetz von G. Analog definiert man Gruppenwirkungen von rechts.

Ein *kategorieller Quotient von X nach G* ist ein Objekt Y von $\mathcal{C}$, zusammen mit einem G-invarianten Morphismus $p\colon X \to Y$, d. h., es gilt $p \circ \sigma = p \circ \mathrm{pr}_2$, das die folgende universelle Eigenschaft besitzt: Ist $X \to T$ ein Morphismus, der das Diagramm



kommutativ macht, dann faktorisiert dieser Morphismus eindeutig durch $p\colon X \to Y$.

Aus der universellen Eigenschaft folgt, dass ein kategorieller Quotient eindeutig bis auf Isomorphie ist, wenn er denn existiert.

Für den Fall, dass $\mathcal{C}$ die Kategorie der Mengen ist (mit einer ein-elementigen Menge als terminalem Objekt), erhält man die übliche Definition für Gruppenoperation und Quotientenmenge. Wir sind am Fall interessiert, dass $\mathcal{C}$ die Kategorie der Schemata über einem

Körper k ist. Jede endliche Gruppe G kann als das endliche, konstante Gruppenschema $\coprod_{g\in G} \mathrm{Spec}(k) \cong \mathrm{Spec}(k \times \ldots \times k)$ aufgefasst werden, wobei die Gruppenstruktur nach Wahl einer Bijektion zwischen den Punkten des Schemas und den Elementen der Gruppe übertragen wird.

Wir beginnen mit dem Fall, dass eine endliche Gruppe G auf einem affinen Schema $X = \mathrm{Spec}(A)$ von rechts operiert. Die Gruppe G operiert dann auf A durch Ringautomorphismen von links. Es bezeichne

$$A^G = \{a \in A \,|\, g \cdot a = a \text{ für alle } g \in G\} \subset A$$

die Menge aller Ringelemente von A, die invariant unter der G-Wirkung sind. Durch die Kompatibilität der Gruppenoperation mit Addition und Multiplikation ist klar, dass A^G ein Unterring von A ist, der auch *Invariantenring* genannt wird. Es sei $Y = \mathrm{Spec}(A^G)$.

Lemma 1.18. *Es sei $p\colon X \to Y$ der Morphismus von affinen Schemata, der durch die Inklusion $A^G \to A$ gegeben ist. Der Morphismus $p\colon X \to Y$ bzw. die Erweiterung $A^G \subset A$ ist ganz.*

Beweis. Jedes Element $a \in A$ ist Nullstelle des Polynoms $\prod_{g\in G}(T - g(a))$. Dieses ist invariant unter der G-Wirkung auf den Koeffizienten, liegt also in $A^G[T]$ und gibt somit eine Ganzheitsgleichung. □

Das Schema Y wird als Quotient X/G fungieren. Aus [22], Exposé V, sind die folgenden dafür relevanten Eigenschaften des Morphismus p bekannt (Prop. 1.1, Cor. 1.2):

Proposition 1.19. *Es gelten die Voraussetzungen aus Lemma 1.18.*

(i) Der Morphismus p ist surjektiv. Die Fasern von p sind die Bahnen von G in X. Die Topologie auf Y stimmt mit der Quotiententopologie überein.

(ii) Der Homomorphismus $\mathcal{O}_Y \to (p_*\mathcal{O}_X)^G$ ist ein Isomorphismus.

Ein Schema Y mit den Eigenschaften (i) und (ii) wird auch als *geometrischer Quotient* von X nach der G-Wirkung bezeichnet.

Beweis. (i): Ganze Ringerweiterungen besitzen die *lying-over*-Eigenschaft (Prop. 4.15 in [16]), d. h., zu jedem Primideal $\mathfrak{q}$ in A^G existiert ein Primideal $\mathfrak{p}$ in A mit $\mathfrak{p} \cap A^G = \mathfrak{q}$. Damit ist p surjektiv. Um zu zeigen, dass die Topologie auf Y mit der Quotiententopologie übereinstimmt, beweisen wir, dass p abgeschlossen ist: Es sei $V(I) \cong \mathrm{Spec}(A/I)$ eine abgeschlossene Teilmenge von X. Die Ringerweiterung $A^G/(I \cap A^G) \to A/I$ erbt die Ganzheit, also gilt auch hier die *lying-over*-Eigenschaft. Folglich ist $V(I \cap A^G) \subset Y$ das Bild von $V(I)$ unter p. Wir betrachten nun die Bahnen der G-Wirkung: Es seien $\mathfrak{p}_1, \mathfrak{p}_2 \subset A$

zwei Primideale, die über $\mathfrak{q} \subset A^G$ liegen, also sodass $\mathfrak{p}_i \cap A^G = \mathfrak{q}$ gilt. Ist $f \in \mathfrak{p}_2$, dann erhalten wir durch Bilden der Norm

$$\prod_{g \in G} g(f) \in \mathfrak{p}_2 \cap A^G = \mathfrak{q} \subset \mathfrak{p}_1.$$

Da $\mathfrak{p}_1$ prim ist, muss daher bereits einer der Faktoren $g(f)$ in $\mathfrak{p}_1$ bzw. f in $g^{-1}(\mathfrak{p}_1)$ enthalten sein. Damit ist die Inklusion $\mathfrak{p}_2 \subset \bigcup_{g \in G} g(\mathfrak{p}_1)$ gezeigt. Da G durch Ringautomorphismen operiert, sind die Mengen der Form $g(\mathfrak{p}_1)$ ebenfalls Primideale mit $g(\mathfrak{p}_1) \cap A^G = \mathfrak{q}$. Aus dem Satz über *prime avoidance* (Lemma 3.3 in [16]) folgt, dass $\mathfrak{p}_2$ bereits in einem Primideal $g(\mathfrak{p}_1)$ enthalten ist. In ganzen Ringerweiterungen gibt es jedoch keine echten Inklusionen von Primidealen, die über dem gleichen Primideal liegen (Cor. 4.18 in [16]). Daher muss die Gleichheit $\mathfrak{p}_2 = g(\mathfrak{p}_1)$ gelten; damit ist gezeigt, dass verschiedene Urbilder eines Punktes von Y in einer Bahn in X liegen. Umgekehrt ist klar, dass jede Bahn in X auf einen Punkt in Y abgebildet wird, da p ein G-invarianter Morphismus ist.

(*ii*): Der Ringhomomorphismus $A_f^G = \mathscr{O}_Y(D(f)) \longrightarrow \mathscr{O}_X(p^{-1}(D(f)))^G = (A_f)^G$ ist die Inklusion. Es reicht zu zeigen, dass Lokalisierung mit Bildung des Invariantenrings vertauscht: Ist $S \subset A^G$ ein multiplikatives System, dann gilt $(S^{-1}A)^G = S^{-1}A^G$. Wir betrachten die exakte Sequenz von A^G-Moduln

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{\alpha} \bigoplus_{g \in G} A,$$

wobei $\alpha \colon A \longrightarrow \bigoplus_g A \xrightarrow{g-1} \bigoplus_g A$ durch $\alpha(x) = ((g(x) - x)_{g \in G})$ gegeben ist. Durch die Eigenschaft $g|_{A^G} = \mathrm{id}|_{A^G}$ ist sichergestellt, dass α eine A^G-lineare Abbildung ist. Lokalisieren ist ein exakter Funktor, daher ist

$$0 \longrightarrow S^{-1}A^G \longrightarrow S^{-1}A \xrightarrow{\alpha_S} \bigoplus_{g \in G} S^{-1}A,$$

ebenfalls exakt, was die Aussage beweist. □

Offensichtlich gilt die Aussage von Proposition 1.19 auch für $p^{-1}(U) \to U$ (siehe auch [22], Cor. V.1.4):

Korollar 1.20. *Ist $U \subset Y$ ein offenes Unterschema, dann ist $p^{-1}(U) \to U$ ein geometrischer Quotient.*

Dazu halten wir fest, dass es sich beim oben eingeführten geometrischen Quotienten um „den“ Quotienten handelt ([43], Prop. 0.1):

Proposition 1.21. *Ein geometrischer Quotient ist auch ein kategorieller Quotient in der Kategorie der k-Schemata.*

In vielen Fällen ist die Quotientenabbildung p ein endlicher Morphismus. Das Argument zum Beweis der folgenden Aussage ([12], Prop. 3.0.1) wird Emmy Noether zugeschrieben:

Proposition 1.22. *Wenn A eine endlich erzeugte Algebra über einem Körper k ist, dessen Elemente invariant unter der Operation einer endlichen Gruppe G sind, dann gelten:*

(i) A ist ein endlich erzeugter A^G-Modul, p ist ein endlicher Morphismus.

(ii) Der Invariantenring A^G ist eine endlich erzeugte k-Algebra.

Beweis. Wir nehmen an, dass A als k-Algebra von endlich vielen Elementen $a_1, \ldots, a_n$ erzeugt wird. Für jedes a_i kann wie im Beweis von Lemma 1.18 eine Ganzheitsgleichung der Form

$$a_i^{m_i} + x_{m_i-1,i}\, a_i^{m_i-1} + \ldots + x_{0,i} = 0$$

mit Koeffizienten $x_{j,i} \in A^G$ gefunden werden. Bezeichnet B die von den Koeffizienten $x_{j,i}$ erzeugte Unter-k-Algebra von A, so ist A ein endlich erzeugter B-Modul mit Erzeugendensystem $a_1^{\nu_1} \cdots a_n^{\nu_n}$, $\nu_i < m_i$. Da auch k invariant unter der Gruppenwirkung ist, gilt weiterhin $B \subset A^G \subset A$. Also ist A ein endlich erzeugter A^G-Modul und der Morphismus p endlich. Nun folgt auch leicht, dass A^G eine endlich erzeugte k-Algebra ist: Der B-Modul A ist noethersch als endlich erzeugter Modul über einem noetherschen Ring, folglich ist auch der B-Untermodul A^G endlich erzeugt. Die Aussage folgt nun aus der Transitivität von „endlich erzeugt“. □

Bemerkung 1.23. Im Allgemeinen ist die Quotientenabbildung p kein endlicher Morphismus, auch wenn G eine endliche Gruppe ist: Dazu seien $G = \mathbb{Z}/2\mathbb{Z}$ und $A = \mathbb{C}[x_1, x_2, \ldots]$ Polynomring in (abzählbar) unendlich vielen Unbestimmten mit der G-Wirkung, die durch $\sigma(x_i) = -x_i$ für alle $i \geq 1$ gegeben ist. Durch diese Wirkung ändert sich bei jedem Monom höchstens das Vorzeichen des Koeffizienten. Ein Polynom $f \in A$ ist daher genau dann invariant, wenn alle auftretenden Monome invariant sind. Ist $f_{\underline{i}}\, x_1^{i_1} \cdots x_n^{i_n}$ ein solches Monom, dann bedeutet die Invarianz, dass die Exponenten sich zu einer geraden Zahl summieren, also $i_1 + \ldots + i_n \equiv 0 \bmod 2$. Umgekehrt ist auch jedes Monom, das diese Bedingung erfüllt, invariant unter der G-Wirkung. Der Invariantenring A^G besitzt als Erzeugendensystem daher alle Produkte von je zwei Unbestimmten, d. h. $A^G = \mathbb{C}[x_i x_j,\ i, j \geq 1]$. Der Ring A ist keine endlich erzeugte A^G-Algebra (und damit kein endlich erzeugter Modul): Jeder Homomorphismus der Form $A^G[T_1, \ldots, T_n] \to A$ ist nicht surjektiv, da in den Bildern der T_i unendlich viele der x_j gar nicht auftreten.

Es sei nun X ein nicht notwendigerweise affines Schema, auf dem eine endliche Gruppe G von rechts operiere. Wir nehmen weiter an, dass ein Quotient X/G existiert. Um diesen konstruktiv zu erhalten, wird man versuchen, eine offene affine Überdeckung $\bigcup_i U_i = X$ mit $U_i = \mathrm{Spec}(A_i)$ zu finden und lokal die Quotienten $U_i/G = \mathrm{Spec}(A_i^G)$ zu konstruieren.

Durch Korollar 1.20 ist sichergestellt, dass auf dem Schnitt der U_i die Quotientenabbildungen $p_i, p_j \colon U_i \cap U_j \to (U_i \cap U_j)/G$ übereinstimmen und sich somit verkleben lassen. Natürlich ist es auch notwendig, dass die U_i selbst von G in sich selbst überführt werden, um eine wohldefinierte G-Wirkung auf den affinen Schemata zu erhalten. Tatsächlich ist dies nach [22], Proposition V.1.8, die einzige Obstruktion bei der Konstruktion des Quotienten:

Proposition 1.24. *Es operiere eine endliche Gruppe G auf einem Schema X von rechts. Ein geometrischer (und damit ein kategorieller) Quotient X/G existiert genau dann, wenn X als Vereinigung von offenen affinen Unterschemata geschrieben werden kann, die jeweils von G in sich selbst überführt werden. Die Bedingung, dass eine solche Überdeckung existiert, ist gleichbedeutend damit, dass jede G-Bahn in einer offenen affinen Teilmenge von X enthalten ist.*

Für separiertes X ist die Äquivalenz der Bedingungen leicht zu sehen: Ist eine Bahn in der offenen affinen Teilmenge U enthalten, dann auch in der offenen affinen Teilmenge $\bigcap_{g\in G} Ug$, die von G in sich selbst abgebildet wird; die umgekehrte Implikation ist offensichtlich. Der große Vorteil dieser zweiten Bedingung liegt darin, dass man sie häufig leichter verifizieren kann.

Proposition 1.25. *Es seien k ein Körper und X ein quasi-projektives k-Schema, auf dem eine endliche Gruppe G operiert. Dann existiert ein Quotient X/G.*

Die Aussage folgt unmittelbar aus dem folgenden Lemma, das sich etwa in [36], Kap. 3, Proposition 3.36, findet:

Lemma 1.26. *Es seien k ein Körper und X ein quasi-projektives k-Schema, d. h., wir können X als offenes Unterschema eines abgeschlossenen Unterschemas $\bar{X} \subset \mathbb{P}^n_k$ ansehen. Zu jeder endlichen Menge von Punkten $\{x_1, \ldots, x_r\} \subset X$ existiert stets ein offenes affines Unterschema, das alle diese Punkte enthält.*

Beweis. Das Schema $Z = \bar{X} \setminus X \subset \mathbb{P}^n_k$ ist ein abgeschlossenes Unterschema, daher können wir $Z = V_+(I)$ für ein homogenes Ideal I schreiben. Zu jedem der endlich vielen Punkte ist $\overline{\{x_i\}} = V_+(\mathfrak{p}_i)$ Verschwindungsmenge eines Primideals. Da Z keinen der endlich vielen Punkte enthält, ist I in keinem der Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ enthalten. Nach dem Satz über *prime avoidance* liegt I auch nicht in der Vereinigung $\bigcup_i \mathfrak{p}_i$, also existiert ein $f \in I$, das in keinem der $\mathfrak{p}_i$ liegt. Die Punkte $x_1, \ldots, x_r$ liegen alle in $D_+(f) = \mathbb{P}^n_k \setminus V_+(f)$ und es gilt $\bar{X} \cap D_+(f) = X \cap D_+(f)$. Damit ist $X \cap D_+(f)$ einerseits ein affines Schema (als abgeschlossenes Unterschema vom affinen Schema $D_+(f)$), andererseits offen in X. □

Lemma 1.27. *Die Abbildung $p \colon X \to X/G$ ist ein Epimorphismus in der Kategorie (Sch/k) der k-Schemata.*

Beweis. Wir wissen bereits, dass p surjektiv ist. Die Surjektivität eines Morphismus ist zwar weder notwendig noch hinreichend für das Vorliegen eines Epimorphismus. Es reicht aber zu zeigen, dass zusätzlich der Garbenhomomorphismus $\mathscr{O}_Y \to p_*\mathscr{O}_X$ injektiv ist. Das ist aber klar, da p auf einer offenen affinen Überdeckung durch die Inklusion von Invariantenringen $R^G \hookrightarrow R$ gegeben ist. □

Die Vorzeicheninvolution $\iota\colon A \to A$ einer abelschen Varietät ist – vorausgesetzt A besteht nicht nur aus einem Punkt – ein Automorphismus der Ordnung 2, somit operiert die Gruppe $\mathbb{Z}/2\mathbb{Z} \cong \{\mathrm{id}_A, \iota\}$ auf A. Nach Theorem 1.10 sind abelsche Varietäten projektiv, daher existieren Quotienten nach endlicher Gruppenwirkung.

Definition 1.28. Es sei A eine abelsche Varietät mit Vorzeicheninvolution ι. Die *Kummer-Varietät zu* A ist der Quotient $A/\{\iota, \mathrm{id}_A\}$. Wir schreiben auch kurz A/ι.

Es gibt dabei zwei Typen von Endomorphismen, die A/ι von A erbt: Die Vervielfachung $n_A\colon A \to A$ induziert einen Endomorphismus $n_{A/\iota}$ von A/ι. Offensichtlich gilt die Gleichheit $\iota \circ n_A = n_A \circ \iota$. Daraus folgt, dass der Morphismus $p \circ n_A\colon A \to A/\iota$ invariant unter Vorschalten der Gruppenoperation bleibt. Die universelle Eigenschaft des Quotienten gibt nun, dass $p \circ n_A$ durch einen Morphismus $n_{A/\iota}\colon A/\iota \to A/\iota$ faktorisiert.

Ein anderer Typ von Endomorphismen der Kummer-Varietät entsteht aus bestimmten Translationen: Ist $x \in A$ ein rationaler 2-Torsionspunkt und t_x die zugehörige Translationsabbildung, so erhält man einen wohldefinierten Morphismus $\bar{t}_x\colon A/\iota \to A/\iota$, da $\iota \circ t_x = t_x \circ \iota$ gilt; dies kann auf L-wertigen Punkten $A(L)$, L eine k-Algebra, leicht mit

$$\iota(t_x(a)) = \iota(a + x) = -a - x = -a + x = t_x(\iota(a))$$

nachgerechnet werden. Weiterhin erbt $\bar{t}_x$ die Eigenschaft $\bar{t}_x \circ \bar{t}_x = \mathrm{id}_{A/\iota}$, ist also ein Automorphismus der Ordnung 2 oder die Identität.

Zum Abschluss dieses Abschnitts werden nun erste Aussagen über den singulären Ort von Kummer-Varietäten getroffen. Abelsche Varietäten selbst besitzen wie alle algebraischen Gruppen keine singulären Punkte: Es reicht, den Fall $k = \bar{k}$ zu betrachten, da der Morphismus $A \otimes_k \bar{k} \to A$ surjektiv, flach und quasi-kompakt ist und die Eigenschaft Regularität in diesem Fall absteigt ([21], Prop. 14.57). Durch Anwendung von Translationen sieht man, dass die lokalen Ringe an allen rationalen Punkten isomorph sind. Da es einen nicht-singulären Punkt gibt, existieren keine singulären Punkte. An „den meisten“ Punkten wird diese Eigenschaft an die Kummer-Varietät vererbt ([22], Prop. V.2.2):

Proposition 1.29. *Es sei G eine endliche Gruppe, die auf einem eigentlichen k-Schema X operiert, sodass ein Quotient $p\colon X \to X/G$ existiert und die Quotientenabbildung ein endlicher Morphismus ist. Wenn der Stabilisator G_x an einem Punkt $x \in X$ trivial ist, dann induziert p einen Isomorphismus $\hat{\mathscr{O}}_{X/G,p(x)} \to \hat{\mathscr{O}}_{X,x}$ zwischen den vervollständigten lokalen Ringen.*

Ist $U \subset A$ das Komplement von $\ker(2_A)$, dann operiert die Vorzeicheninvolution ι frei auf U. Es sei $x \in U$ ein rationaler Punkt. Wir werden in Proposition 1.47 sehen, dass ein lokaler Ring genau dann regulär ist, wenn seine Vervollständigung am maximalen Ideal regulär ist. Somit ist $p(x)$ kein singulärer Punkt.

Korollar 1.30. *Es seien k algebraisch abgeschlossen und A/ι eine Kummer-Varietät mit singulären Punkten. Die singulären Punkte von A/ι liegen genau an den 2^{2g} Bildpunkten von $\ker(2_A)(k)$.*

Beweis. Es bezeichne $\bar{x} \in A/\iota$ das Bild eines 2-Torsionspunktes. Durch $\bar{t}_x$ wird ein Isomorphismus $\mathscr{O}_{A/\iota,\bar{x}} \to \mathscr{O}_{A/\iota,\bar{e}}$ induziert. Die Halme an den Bildern aller 2-Torsionspunkte sind also isomorph. □

Wir werden im nächsten Abschnitt sehen, dass Singularitäten genau dann auftreten, wenn $\dim(A) \geq 2$ gilt (siehe Prop. 1.54, Bsp. 1.55). Singuläre Kummer-Varietäten sind damit der Regelfall.

1.3 Einige Eigenschaften von Ringen

In diesem Abschnitt wird an einige Eigenschaften und Kennzahlen von kommutativen Ringen erinnert, um damit die (singulären) lokalen Ringe von Kummer-Varietäten zu untersuchen. Dabei sind Eigenschaften von lokalen Ringen, die stabil unter Vervollständigung bzgl. des maximalen Ideals sind, von besonderer Bedeutung. Die meisten Resultate lassen sich in Standardwerken zur Kommutativen Algebra finden; hier sind die Monographien [8] und [16] verwendet worden. Alle Ringe sind als kommutativ und mit einem Eins-Element vorausgesetzt.

Definition 1.31. Es sei R ein Ring und M ein R-Modul. Ein Element $x \in R$ heißt *regulär für M* oder kurz *M-regulär*, wenn aus $x \cdot m = 0$ für ein $m \in M$ bereits $m = 0$ folgt. Eine Folge $x_1, \ldots, x_r \in R$ heißt M-reguläre Folge, wenn $(x_1, \ldots, x_r)M \neq M$ und wenn für $1 \leq i \leq r$ das Element x_i ein reguläres Element für $M/(x_1, \ldots, x_{i-1})M$ ist.

Nach [8], Theorem 1.2.5, ist die Länge maximaler M-regulärer Folgen unter leichten Bedingungen konstant:

Proposition 1.32. *Es bezeichne R einen noetherschen Ring, M einen endlich erzeugten R-Modul und $I \subset R$ ein Ideal mit $IM \neq M$. In dieser Situation haben alle maximalen M-regulären Folgen mit Folgengliedern in I die gleiche Länge n. Diese Länge kann durch*

$$n = \min\{i \mid \operatorname{Ext}^i_R(R/I, M) \neq 0\}$$

explizit angegeben werden.

Die wichtigste Anwendung liegt für uns im Fall, dass R lokal und $I = \mathfrak{m}$ das maximale Ideal ist. Da die Länge einer maximalen M-regulären Folge nicht von der konkreten Wahl der Folge abhängt, kann diese Zahl als Eigenschaft des Moduls M aufgefasst werden.

Definition 1.33. Es sei $(R, \mathfrak{m})$ ein noetherscher lokaler Ring.

(*i*) Die *Tiefe* $\operatorname{depth}(R)$ ist die Länge einer maximalen R-regulären Folge.

(*ii*) Die *Einbettungsdimension* $\operatorname{edim}(R)$ ist die Kardinalität eines minimalen Erzeugendensystems von $\mathfrak{m}$.

Da $\mathfrak{m}$ endlich erzeugt ist, handelt es sich bei $\operatorname{edim}(R)$ um eine natürliche Zahl. Nach dem Nakayama-Lemma stimmt die Einbettungsdimension mit der Dimension von $\mathfrak{m}/\mathfrak{m}^2$, aufgefasst als Vektorraum über dem Restekörper, überein. Die Tiefe ist ebenfalls endlich, da sie durch die Einbettungsdimension beschränkt ist:

Proposition 1.34. *Für einen noetherschen lokalen Ring $(R, \mathfrak{m})$ sind die Ungleichungen*

$$\operatorname{depth}(R) \leq \dim(R) \leq \operatorname{edim}(R)$$

stets erfüllt.

Die Dimension eines Rings ist dabei definiert als das Supremum der Längen aller Primidealketten in R. Die erste Ungleichung ergibt sich aus Proposition 1.2.12 in [8], die zweite Ungleichung folgt unmittelbar aus dem Krullschen Höhensatz (Thm. 13.5 in [39]).

Definition 1.35. Es sei $(R, \mathfrak{m}, k)$ ein lokaler Ring mit Restekörper k. Der *Typ* von R, in Zeichen $r(R)$, ist die Zahl $\dim_k \left(\operatorname{Ext}^d_R(k, R)\right)$, wobei d die Tiefe von R bezeichnet.

Um den Typ auszurechnen, kann die Situation oft vereinfacht werden: Wir nehmen an, dass R eine Algebra über seinem Restekörper k ist. Bezeichnet d die Tiefe von R und ist $x_1, \ldots, x_d$ eine R-reguläre Folge, so existiert nach [8], Lemma 1.2.4, ein Isomorphismus

$$\operatorname{Ext}^d_R(k, R) \cong \operatorname{Hom}_R(k, R/(x_1, \ldots, x_d)) \tag{1.7}$$

von R-Moduln und damit insbesondere von k-Vektorräumen.

Definition 1.36. Es sei $(R, \mathfrak{m})$ ein noetherscher lokaler Ring.

(*i*) Man nennt R einen *regulären* lokalen Ring, wenn $\operatorname{edim}(R) = \dim(R)$ gilt.

(*ii*) Man nennt R einen *Cohen–Macaulay-Ring*, wenn $\operatorname{depth}(R) = \dim(R)$ gilt.

(*iii*) Man nennt R einen *Gorenstein-Ring*, wenn R ein Cohen–Macaulay-Ring vom Typ $r(R) = 1$ ist.

Ein noetherscher, nicht notwendigerweise lokaler Ring R heißt regulärer Ring bzw. Cohen–Macaulay-Ring bzw. Gorenstein-Ring, wenn die Lokalisierung $R_{\mathfrak{m}}$ an jedem maximalen Ideal einen lokalen Ring mit der jeweiligen oben angegebenen Eigenschaft liefert.

Häufig werden lokale Gorenstein-Ringe auch als lokale noethersche Ringe von endlicher injektiver Dimension definiert, d. h., es existiert eine endliche injektive Auflösung des Rings, aufgefasst als Modul über sich selbst. Nach [8], Theorem 3.2.10, ist diese Charakterisierung äquivalent zur gegebenen Definition.

In einem lokalen Cohen–Macaulay-Ring können reguläre Folgen über die Dimension des Faktorrings charakterisiert werden, für allgemeinere noethersche lokale Ringe gilt jedoch nur eine Implikation (siehe [8], Thm. 2.1.2, Bem. S. 12):

Proposition 1.37. *Es seien $(R, \mathfrak{m})$ ein noetherscher lokaler Ring und $x_1, \ldots, x_r$ eine R-reguläre Sequenz. Dann gilt*

$$\dim(R/(x_1, \ldots, x_i)) = \dim(R) - i \tag{1.8}$$

für jedes $i \in \{0, \ldots, r\}$. Wenn R zusätzlich ein Cohen–Macaulay-Ring ist, dann gilt auch die Umkehrung: Ist $x_1, \ldots, x_r$ eine Folge in R und gilt für $i = r$ die Gleichung (1.8)*, so ist die Folge R-regulär.*

Im Allgemeinen kann aus (1.8) nicht geschlossen werden, dass eine reguläre Folge vorliegt. Einfachstes Gegenbeispiel ist der zweidimensionale Ring $k[\![x, y, z]\!]/(xz, yz)$ (mit Primidealkette $(z) \subsetneq (x, z) \subsetneq (x, y, z)$), in dem x kein reguläres Element ist, aber der Quotient nach (x) eindimensional ist. Ein komplexeres Gegenbeispiel wird in Kapitel 3 erhalten: In Bemerkung 3.30 wird ein Integritätsring angegeben, in dem eine nicht-reguläre Folge $x_1, \ldots, x_r$ existiert, die die Bedingung (1.8) erfüllt und sodass die Spektren der jeweiligen Faktorringe auch irreduzibel sind.

Eine in dieser Arbeit häufig benötigte Operation ist die *Vervollständigung* eines Rings bzgl. eines Ideals.

Definition 1.38. Es sei R ein Ring und $I \subset R$ ein Ideal. Durch die Inklusionen $I^m \subset I^n$ für $m > n$ ist ein projektives System $p_{m,n} \colon R/I^m \to R/I^n$ gegeben. Die *Vervollständigung von R bzgl. I* ist definiert als der projektive Limes

$$\varprojlim_n R/I^n = \left\{ (a_1, a_2, \ldots) \in \prod_n R/I^n \;\middle|\; p_{m,n}(a_m) = a_n \;\text{ für alle } m > n \right\}$$

und wird als $\hat{R}$ geschrieben, wenn das Ideal I aus dem Kontext bekannt ist. Ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, dann bezeichnet $\hat{R}$ die Vervollständigung von R bzgl. $\mathfrak{m}$.

Als projektiver Limes besitzt die Vervollständigung die folgende universelle Eigenschaft: Für jeden Ring S mit Ringhomomorphismen $\pi_n \colon S \to R/I^n$, die die Kompatibilitätsbedingung $\pi_n = p_{m,n} \circ \pi_m$ für alle $m > n$ erfüllen, existiert ein eindeutiger Ringhomomorphismus $S \to \hat{R}$. Insbesondere existiert ein kanonischer Homomorphismus $R \to \hat{R}$. Wenn dieser ein Isomorphismus ist, wird R als *vollständig bzgl. I* bezeichnet. Der kanonische Homomorphismus ist im Allgemeinen nicht injektiv, sein Kern besteht aus den Elementen von $\cap_{n\in\mathbb{N}} I^n$. Nach dem *Durchschnittsatz* von Krull ([16], Cor. 5.4) ist dieser Durchschnitt für noethersche integre oder lokale Ringe das Nullideal.

Die folgende Proposition fasst einige Eigenschaften der Vervollständigung (siehe [16], Thm. 7.1 und 7.2) zusammen.

Proposition 1.39. *Es seien R ein noetherscher Ring und $\hat{R}$ die Vervollständigung bzgl. eines Ideals $I \subset R$. Dann gelten:*

(i) Der Ring $\hat{R}$ ist ebenfalls noethersch.

(ii) $\hat{R}/I^n\hat{R} = R/I^n$, also ist $\hat{R}$ vollständig bzgl. $I\hat{R}$.

(iii) $\hat{R}$ ist ein flacher R-Modul, d. h., Tensorieren $- \otimes_R \hat{R}$ erhält exakte Sequenzen von R-Moduln.

(iv) Ist M ein endlich erzeugter R-Modul, dann ist $\hat{R} \otimes_R M \longrightarrow \varprojlim M/I^nM$ ein Isomorphismus.

Insbesondere ergibt sich aus der Proposition: Ist S ein Ring, der als R-Modul endlich erzeugt ist, dann ist $\hat{R} \otimes_R S$ die Vervollständigung von S bzgl. IS.

Nach [16], Theorem 10.10, ändert sich die Dimension eines noetherschen lokalen Rings nach Vervollständigung nicht:

Proposition 1.40. *Es seien $(R, \mathfrak{m})$, $(S, \mathfrak{n})$ zwei noethersche lokale Ringe und $R \to S$ ein flacher, lokaler Ringhomomorphismus. Dann gilt*

$$\dim(S) = \dim(R) + \dim(S/\mathfrak{m}S).$$

Speziell gilt also im Fall $S = \hat{R}$ die Gleichheit $\dim(R) = \dim(\hat{R})$.

Beispiel 1.41. Wir betrachten den Polynomring $S = k[x_1, \ldots, x_n]$ über einem Körper k und eine endlich erzeugte k-Algebra $R = S/I$, weiter seien $\mathfrak{m} \subset S$ sowie $\bar{\mathfrak{m}} \subset R$ die von den Unbestimmten erzeugten maximalen Ideale. Die Vervollständigung von S bzgl. $\mathfrak{m}$ ist $\hat{S} = k[\![x_1, \ldots, x_n]\!]$ und die von R bzgl. $\bar{\mathfrak{m}}$ ist $\hat{R} = \hat{S}/I\hat{S}$.

Solche Quotienten von Potenzreihenringen sind nicht nur ein wichtiges Beispiel, sondern können sogar nach dem *Struktursatz* von Cohen (siehe z. B. [16], Thm. 7.7) als Prototyp für vollständige Ringe angesehen werden:

Theorem 1.42 (Cohen)**.** *Jeder vollständige lokale noethersche Ring R, der einen Körper enthält, ist isomorph zu einem Ring der Form $k[\![x_1, \ldots, x_n]\!]/I$, wobei k den Restekörper von R und I ein Ideal im Potenzreihenring bezeichnen.*

Für reguläre lokale Ringe kann sogar eine noch deutlich stärkere Aussage getroffen werden (siehe [16], Prop. 10.16):

Proposition 1.43. *Ist $(R, \mathfrak{m}, k)$ ein vollständiger regulärer lokaler Ring, der einen Körper enthält, dann gilt $R \cong k[\![x_1, \ldots, x_d]\!]$ mit $d = \dim(R)$.*

Bei den bisher genannten vervollständigten Ringen handelte es sich stets um lokale Ringe. Diese Beobachtung lässt sich nach [16], Diskussion auf S. 183, wie folgt fassen:

Proposition 1.44. *Es seien R ein noetherscher Ring, $\mathfrak{m} \subset R$ ein maximales Ideal und $\hat{R}$ die Vervollständigung bzgl. $\mathfrak{m}$. Dann ist $(\hat{R}, \mathfrak{m}\hat{R})$ ein lokaler Ring mit Restekörper $R/\mathfrak{m}$. Bezeichnet $R_\mathfrak{m}$ die Lokalisierung von R an $\mathfrak{m}$, so ist $\widehat{R_\mathfrak{m}} = \hat{R}$.*

Eine weitere Eigenschaft noetherscher (lokaler) Ringe wird darüber definiert, dass die Vervollständigung ein Faktorring nach „möglichst wenigen“ Relationen ist, was in Form einer regulären Folge systematisiert wird.

Definition 1.45. Ein noetherscher lokaler Ring $(R, \mathfrak{m})$ heißt *vollständiger Durchschnitt*, wenn die Vervollständigung von R bzgl. $\mathfrak{m}$ isomorph zu einem Ring der Form S/I ist, wobei S einen regulären lokalen Ring bezeichnet und das Ideal $I \subset R$ von einer regulären Folge erzeugt wird. Ein noetherscher Ring wird vollständiger Durchschnitt genannt, wenn die Lokalisierung an jedem maximalen Ideal einen lokalen vollständigen Durchschnitt liefert.

Die Frage, ob ein vollständiger Durchschnitt vorliegt, kann anhand einer Kennzahl, dem *Vollständiger-Durchschnitt-Defekt* $\delta(R)$, beantwortet werden. Eine einfache Formel für $\delta(R)$ ergibt sich aus der Kombination der Theoreme 2.3.2 und 2.3.3 aus [8]:

Proposition 1.46. *Es seien S ein noetherscher, regulärer lokaler Ring mit maximalem Ideal $\mathfrak{n}$ und $I \subset \mathfrak{n}^2$ ein Ideal von S. Der Faktorring $R = S/I$ ist genau dann ein vollständiger Durchschnitt, wenn*

$$\delta(R) := m(I) - \operatorname{edim}(R) + \dim(R) = 0$$

gilt. Dabei bezeichnet $m(I)$ die Kardinalität eines minimalen Erzeugendensystems von I. Der Wert $\delta(R)$ hängt nicht von der Darstellung S/I ab.

Die bisher genannten Ringeigenschaften bleiben nach Vervollständigung und Lokalisierung erhalten, die meisten Eigenschaften auch bei Quotienten nach einer regulären Folge. Bei der folgenden Proposition handelt es sich um eine Zusammenstellung von Resultaten aus [8], Thm. 2.3.4, Prop. 3.1.19, Thm 2.1.3, Cor. 2.1.8 und Prop. 2.2.2.

Proposition 1.47. *Es sei $(R, \mathfrak{m})$ ein noetherscher lokaler Ring, der Quotient eines regulären lokalen Rings ist. Wir nehmen an, dass R ein vollständiger Durchschnitt, ein Gorenstein- oder ein Cohen–Macaulay-Ring ist und bezeichnen diese Eigenschaft mit $\boldsymbol{P}$.*

(i) Wenn R die Eigenschaft $\boldsymbol{P}$ besitzt, dann gilt das auch für die Lokalisierung $R_\mathfrak{p}$ an einem beliebigen Primideal $\mathfrak{p} \subset R$.

(ii) Der Ring R hat genau dann die Eigenschaft $\boldsymbol{P}$, wenn die Vervollständigung $\hat{R}$ die jeweilige Eigenschaft besitzt.

(iii) Es sei I ein Ideal, das von einer R-regulären Folge $x_1, \ldots, x_r$ erzeugt wird. Der Ring R hat genau dann die Eigenschaft $\boldsymbol{P}$, wenn R/I die jeweilige Eigenschaft besitzt.

Die Bedingungen (i) und (ii) sind auch für die Eigenschaft „regulär“ erfüllt.

Die oben aufgezählten Eigenschaften bilden eine Kette: Jeder reguläre lokale Ring ist nach Proposition 1.47 ein vollständiger Durchschnitt. Nach [8], Proposition 3.1.20, ist wiederum jeder vollständige Durchschnitt ein Gorenstein-Ring. Gorenstein-Ringe sind per Definition Cohen–Macaulay-Ringe.

Bei der Untersuchung von Ringen, die von eigentlichen k-Schemata herrühren, ist die Frage nach der *Normalität* des Rings von Interesse, da hiermit einerseits a priori eine Aussage über die Kodimension des singulären Ortes getroffen werden kann, andererseits durch Normalisieren Singularitäten verbessert werden können.

Definition 1.48. Ein kommutativer Ring R heißt *normal*, wenn für jedes Primideal $\mathfrak{p} \subset R$ der lokale Ring $R_\mathfrak{p}$ ein ganzabgeschlossener integrer Ring ist.

Ein Integritätsring R ist genau dann normal, wenn er ganzabgeschlossen ist (siehe [39], S. 64). Ein praktisches, häufig anwendbares Kriterium für Normalität geht zurück auf Serre: Für $m \in \mathbb{N}$ betrachten wir die Bedingungen

$$\begin{aligned} \mathrm{R}_m &: \ \dim(R_\mathfrak{p}) = \operatorname{edim}(R_\mathfrak{p}) \ \text{ für alle } \mathfrak{p} \in \operatorname{Spec}(R) \text{ mit } \operatorname{height}(\mathfrak{p}) \leq m, \\ \mathrm{S}_m &: \ \operatorname{depth}(R_\mathfrak{p}) \geq \inf\{m, \operatorname{height}(\mathfrak{p})\} \ \text{ für alle } \mathfrak{p} \in \operatorname{Spec}(R). \end{aligned}$$

Die *Höhe* $\operatorname{height}(\mathfrak{p})$ eines Primideals $\mathfrak{p} \subset R$ ist dabei definiert als die Dimension des lokalen Rings $R_\mathfrak{p}$. Mithilfe dieser Bedingungen können etwa Cohen–Macaulay-Ringe charakterisiert werden als die noetherschen Ringe, die die Bedingungen S_m für alle $m \in \mathbb{N}$ erfüllen.

Das Kriterium von Serre (z. B. [39], Thm. 23.8) lautet:

Theorem 1.49 (Serre)**.** *Ein noetherscher Ring R ist genau dann normal, wenn die Bedingungen R_1 und S_2 erfüllt sind.*

Für viele lokale Ringe, die als Halme von k-Schemata auftreten, ist Normalität stabil unter Vervollständigung, wie das folgende Theorem, eine Kombination von [56], S. 357, und [57], Theorem 2, zeigt:

Theorem 1.50 (Zariski)**.** *Es seien X ein integres eigentliches Schema über einem Körper k und $R = \mathscr{O}_{X,x}$ der lokale Ring an einem Punkt. Wenn R normal ist, dann ist die Vervollständigung $\hat{R}$ normal und integer.*

Die Umkehrung von Theorem 1.50 gilt: Ist $\hat{R}$ integer, dann ist auch R als Unterring integer. Die folgende Proposition (siehe etwa [39], Thm. 23.9) zeigt, dass bei flachen Ringhomomorphismen wie $R \to \hat{R}$ die Eigenschaften R_m bzw. S_m von $\hat{R}$ an R vererbt werden:

Proposition 1.51. *Es sei $A \to B$ ein flacher lokaler Ringhomomorphismus zwischen lokalen noetherschen Ringen. Erfüllt B die Bedingung R_m bzw. S_m für ein $m > 0$, dann gilt dies auch für A.*

Es ist im Allgemeinen jedoch falsch, dass die Vervollständigung eines normalen Rings wieder normal ist, ebenso ist die Vervollständigung eines integren lokalen Rings an seinem maximalen Ideal nicht zwangsläufig wieder ein integrer Ring. Das Standardbeispiel hierfür ist der lokale Ring der affinen integren Kurve $V(y^2 - x^2(x-1)) \subset \mathbb{A}^2_{\mathbb{C}}$ am Ursprung. Im Potenzreihenring $\mathbb{C}[\![x, y]\!]$ ist das Polynom reduzibel, da $x - 1$ dort ein Quadrat ist.

Die Bildung des Invariantenrings R^G ist verträglich mit den Operationen Lokalisieren und Vervollständigen:

Proposition 1.52. *Es sei R eine endlich erzeugte integre k-Algebra mit Gruppenwirkung einer endlichen Gruppe G, die trivial auf den Elementen von k operiert.*

(i) Es sei zu jedem $s \in S$ auch die ganze Bahn $G \cdot s$ in S enthalten. In diesem Fall gilt $(S^{-1}R)^G = (S \cap R^G)^{-1}R^G$.

(ii) Es seien $\mathfrak{m}_2 \subset R$ ein maximales Ideal, $\mathfrak{m}_1 = \mathfrak{m}_2 \cap R^G$ und $\mathfrak{m}_2$ sei das einzige maximale Ideal, das über $\mathfrak{m}_1$ liegt. Es bezeichne $\hat{R}$ die Vervollständigung bzgl. $\mathfrak{m}_2$. In dieser Situation stimmen $\hat{R}^G$ und $\widehat{R^G}$, die Vervollständigung bzgl. $\mathfrak{m}_1$, überein.

Wegen der Eigenschaft (ii) wird in der Notation nur noch das Symbol $\hat{R}^G$ verwendet. Die Aussage ist wohlbekannt und wird in der Fachliteratur häufig ohne explizite Nennung verwendet. Beweise beschränken sich jedoch auf den Spezialfall, dass $\mathrm{char}(k)$ kein Teiler von $|G|$ oder die Wirkung linear ist, weshalb hier ein allgemeinerer Beweis ergänzt wird.

Beweis. (i): Die Inklusion „$\supset$“ ist offensichtlich. Es sei $f_1/f_2 \in (S^{-1}R)^G$. Wir können ohne Einschränkung $f_2 \in R^G$ annehmen (ansonsten kann durch Erweitern der invariante Nenner $\prod_{g \in G} g \cdot f_2$ erhalten werden). Da der Bruch invariant ist, muss nun auch f_1 invariant sein.

(ii): Nach Proposition 1.39 gilt $\widehat{R^G} \otimes_{R^G} R = \tilde{R}$, wobei $\tilde{R}$ die Vervollständigung von R bzgl. des Ideals $\mathfrak{m}_1 R$ bezeichnet. Wir zeigen zunächst, dass $\tilde{R}$ mit $\hat{R}$, der Vervollständigung von R bzgl. $\mathfrak{m}_2$, übereinstimmt: Offensichtlich gilt $\mathfrak{m}_1 R \subset \mathfrak{m}_2$. Nach Voraussetzung ist $\mathfrak{m}_2$ das einzige maximale Ideal, das über $\mathfrak{m}_1$ liegt. R ist ein endlich erzeugter R^G-Modul,

also ist $R/\mathfrak{m}_1 R$ ein endlich-dimensionaler Vektorraum über dem Körper $\kappa = R^G/\mathfrak{m}_1$ und damit insbesondere ein null-dimensionaler Ring. Noch dazu ist $R/\mathfrak{m}_1 R$ ein lokaler Ring, ansonsten würde ein zweites maximales Ideal über $\mathfrak{m}_1$ existieren. In diesem Faktorring ist das Nilradikal somit maximal, d. h., es gilt $\mathfrak{m}_2 = \sqrt{\mathfrak{m}_1 R}$. Wir nehmen an, dass das Ideal $\mathfrak{m}_2$ von Elementen $a_1, \ldots, a_\nu \in R$ erzeugt wird und dass $a_i^{d_i} \in \mathfrak{m}_1 R$ gilt. Für $d = d_1 + \ldots + d_\nu$ gilt dann $\mathfrak{m}_2^d \subset \mathfrak{m}_1 R$. Für beliebige $n, m \in \mathbb{N}$ gilt also $(\mathfrak{m}_1 R)^n \subset \mathfrak{m}_2^n$ und $\mathfrak{m}_2^{dm} \subset (\mathfrak{m}_1 R)^m$. Nach [16], Lemma 7.14, stimmen die Vervollständigungen bzgl. der beiden Ideale überein.

Wir betrachten nun die exakte Sequenz von R^G-Moduln

$$0 \longrightarrow R^G \longrightarrow R \xrightarrow{\alpha} \bigoplus_{g \in G} R,$$

wobei α durch $\alpha(x) = ((g(x) - x)_{g \in G})$ gegeben ist. Da $\widehat{R^G}$ flach über R^G ist, bleibt die Exaktheit der Sequenz erhalten, wenn wir mit $\widehat{R^G}$ tensorieren. Es ergibt sich die neue exakte Sequenz

$$0 \longrightarrow \widehat{R^G} \longrightarrow \hat{R} \xrightarrow{\hat{\alpha}} \bigoplus_{g \in G} \hat{R},$$

aus der nun die Gleichheit $\widehat{R^G} = \hat{R}^G$ folgt. □

Die Eigenschaft Normalität bleibt im Invariantenring erhalten:

Proposition 1.53. *Es sei R ein normaler, integrer Ring, auf dem eine Gruppe G operiert. Dann ist der Ring R^G auch normal.*

Beweis. Es reicht zu zeigen, dass R^G ein ganzabgeschlossener Ring ist. Ist $x \in \mathrm{Frac}(R^G)$ ganz über R^G, so existiert eine Ganzheitsgleichung der Form $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ mit $a_i \in R^G$. Als Ganzheitsgleichung in R aufgefasst, folgt $x \in R$. Da x aber invariant unter G ist, gilt $x \in R^G$. □

Zum Abschluss dieses Abschnitts werden nun der singuläre Ort von Kummer-Varietäten ermittelt und im Anschluss die einfachsten Beispiele von Kummer-Varietäten betrachtet, bei denen noch gar keine singulären Punkte auftreten. Wir wissen bereits, dass singuläre Punkte nur an den Bildern der 2-Torsionspunkte auftreten können. Das folgende Kriterium ([45], Prop. 1.2) zeigt, dass dies auch fast immer der Fall ist:

Proposition 1.54. *Es sei R ein noetherscher regulärer lokaler Ring, auf dem eine endliche Gruppe G operiert. Weiter sei $\mathfrak{p} \subset R$ ein minimales Primideal unter den Primidealen, an denen die Abbildung* $\mathrm{Spec}(R) \to \mathrm{Spec}(R^G)$ *verzweigt ist. Wenn* $\mathrm{height}(\mathfrak{p}) \geq 2$ *erfüllt ist, liegt $\mathfrak{p} \cap R^G$ im singulären Ort von* $\mathrm{Spec}(R^G)$.

Es sei A eine abelsche Varietät der Dimension g. Für jeden rationalen Punkt $x \in A$ ist das maximale Ideal $\mathfrak{m} \subset \mathscr{O}_{A,x}$ ein Primideal der Höhe g. Ist x ein 2-Torsionspunkt und $g \geq 2$, dann sind die Voraussetzungen der Proposition erfüllt und folglich ist $\mathscr{O}_{A/\iota,p(x)}$ kein regulärer lokaler Ring. Damit besitzen Kummer-Varietäten ab Dimension 2 stets singuläre Punkte. Im Fall $g = 1$ treten keine singulären Punkte auf, da der Quotient normal ist und nach dem Normalitätskriterium von Serre keine singulären Punkte in Kodimension 1 besitzen kann.

Beispiel 1.55. Wir berechnen für abelsche Varietäten der Dimension ≤ 1 explizit die zugehörigen Kummer-Varietäten. In diesen einfachen Fällen hängen die Kummer-Varietäten nur von $\dim(A)$, aber nicht von der konkreten abelschen Varietät A ab:

(i) Ist $\dim(A) = 0$, dann besteht A nur aus einem rationalen Punkt, welcher automatisch als neutrales Element fungiert. Es folgt $A/\iota = A$.

(ii) Ist E eine abelsche Varietät der Dimension 1, also eine elliptische Kurve, dann können wir eine Weierstraß-Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

für E wählen. Die rationalen Punkte von E bestehen aus den Nullstellen (λ, μ) dieser Gleichung und dem neutralen Element O, das nach Homogenisierung der Weierstraß-Gleichung dem Punkt $(0 : 1 : 0)$ entspricht. Die Vorzeicheninvolution operiert nach [52], Algorithmus III.2.3, auf rationalen Punkten durch $(\lambda, \mu) \mapsto (\lambda, -\mu - a_1\lambda - a_3)$ und $O \mapsto O$. Für jede k-Algebra L sei die Abbildung $E(L) \to \mathbb{P}^1_k(L)$ durch die Vorschrift $(\lambda, \mu) \mapsto (\lambda : 1)$ und $O \mapsto (1 : 0)$ gegeben. Diese Festlegung gibt eine natürliche Transformation $E(\,.\,) \to \mathbb{P}^1_k(\,.\,)$ und liefert nach dem Yoneda-Lemma einen wohldefinierten Morphismus von k-Schemata $f\colon E \to \mathbb{P}^1_k$. Der lokale Ringhomomorphismus zwischen den generischen Punkten vermittelt eine Körpererweiterung $k(x) = k(\mathbb{P}^1_k) \hookrightarrow k(E)$ der Funktionenkörper. Diese besitzt Erweiterungsgrad 2, da $k(E) = k(x)[y]/(y^2 + a_1xy + \ldots)$ gilt. Der Morphismus f ist ι-invariant, nach der universellen Eigenschaft des Quotienten erhält man daher, dass f als Komposition $E \xrightarrow{p} E/\iota \xrightarrow{h} \mathbb{P}^1_k$ geschrieben werden kann. Die Erweiterung $k(E/\iota) \subset k(E)$ ist ebenfalls quadratisch, also muss die Gleichheit $k(E/\iota) = k(\mathbb{P}^1_k)$ gelten. Der Morphismus h ist damit birational. Da E/ι keine singulären Punkte besitzt, ist h ein Isomorphismus (siehe [52], Cor. II.2.4.1). Damit haben wir $E/\iota \cong \mathbb{P}^1_k$ bewiesen.

1.4 Blow-ups

Es wird nun an die Operation des Blow-up und damit verbundene Begriffe erinnert, um diese im nächsten Kapitel zur Auflösung von Singularitäten anwenden zu können.

Definition 1.56. Es seien X ein Schema und Z ein abgeschlossenes Unterschema, definiert durch ein quasi-kohärentes Ideal $\mathscr{I} \subset \mathscr{O}_X$. Das *Blow-up von X mit Zentrum Z* ist das Schema $\mathrm{Bl}_Z(X) = \mathrm{Proj}(\bigoplus_{n\geq 0} \mathscr{I}^n)$. Bezeichnet $\pi\colon \mathrm{Bl}_Z(X) \to X$ den Strukturmorphismus, dann wird das Urbild $E = \pi^{-1}(Z)$ auch als *exzeptioneller Divisor* bezeichnet.

Die Bezeichnung legt bereits nahe, dass E ein Divisor ist. Das Blow-up besitzt sogar die folgende universelle Eigenschaft (siehe etwa [21], Def. 13.90, Prop. 13.92):

Proposition 1.57. *Es seien X und Z wie in der Definition. Ist $\psi\colon T \to X$ ein Morphismus von Schemata und $\psi^{-1}(Z)$ ein effektiver Cartier-Divisor, dann existiert ein eindeutiger Morphismus $h\colon T \to \mathrm{Bl}_Z(X)$, sodass $\psi = \pi \circ h$ faktorisiert.*

Weitere Eigenschaften von Blow-ups fasst die folgende Proposition zusammen (siehe z. B. [21], Prop. 13.91, 13.96):

Proposition 1.58. *Es seien $\pi\colon \mathrm{Bl}_Z(X) \to X$ das Blow-up von X mit Zentrum Z und $f\colon X' \to X$ ein Morphismus von Schemata.*

(i) Es existiert ein eindeutiger Morphismus $\mathrm{Bl}_Z(f)\colon \mathrm{Bl}_{f^{-1}(Z)}(X') \longrightarrow \mathrm{Bl}_Z(X)$, der das Diagramm

$$\begin{array}{ccc} \mathrm{Bl}_{f^{-1}(Z)}(X') & \xrightarrow{\mathrm{Bl}_Z(f)} & \mathrm{Bl}_Z(X) \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ X' & \xrightarrow{\quad f \quad} & X \end{array} \tag{1.9}$$

kommutativ macht.

(ii) Wenn f ein flacher Morphismus ist, so ist das Diagramm (1.9) kartesisch, d. h., es gilt $\mathrm{Bl}_{f^{-1}(Z)}(X') \cong X' \times_X \mathrm{Bl}_Z(X)$.

(iii) Ist $U = X \setminus Z$ das Komplement von Z, dann ist $\pi|_{\pi^{-1}(U)}\colon \pi^{-1}(U) \longrightarrow U$ ein Isomorphismus.

(iv) Es sei Z durch die Idealgarbe $\mathscr{I} \subset \mathscr{O}_X$ gegeben. Wir nehmen an, dass für jede affine offene Teilmenge $V \subset X$ in $H^0(V, \mathscr{I})$ ein reguläres Element existiert. In diesem Fall ist π ein birationaler Morphismus.

(v) Ist f eine abgeschlossene Einbettung, dann gilt dies auch für den Morphismus $\mathrm{Bl}_Z(f)$.

Die Bedingung in (iv) ist trivialerweise erfüllt, wenn X integer und $\mathscr{I} \neq 0$ gilt. Eine wichtige Anwendung von (ii) besteht darin, dass die Blow-up-Operation mit Lokalisierung bzw. Vervollständigung verträglich ist:

Korollar 1.59. *Es seien $X = \operatorname{Spec}(R)$, $I \subset R$ ein Ideal, $Z = V(I) \subset X$ und $\mathfrak{p} \subset R$ ein Primideal, das I enthält. Das Blow-up von $\operatorname{Spec}(R_\mathfrak{p})$ mit Zentrum $V(IR_\mathfrak{p})$ erhält man als Basiswechsel von $\operatorname{Bl}_Z(X) \to X$ entlang $\operatorname{Spec}(R_\mathfrak{p}) \to X$. Ist R noethersch, dann gilt die gleiche Aussage auch für die Vervollständigung $\hat{R}$ bzgl. $\mathfrak{p}$.*

Beweis. $R_\mathfrak{p}$ ist ein flacher R-Modul, da Lokalisierung ein exakter Funktor ist. Ist R ein noetherscher Ring, so ist nach Proposition 1.39 auch $\hat{R}$ flach über R. Folglich induzieren die kanonischen Ringhomomorphismen $R \to R_\mathfrak{p}$ und $R \to \hat{R}$ flache Morphismen von Schemata. □

Wenn Erzeuger des Ideals von Z bekannt sind, wird die Berechnung eines Blow-ups häufig in affinen Karten vorgenommen. Das folgende Resultat zeigt, wie eine affine Überdeckung konkret gefunden werden kann (siehe [25], Def. 4.13):

Proposition 1.60. *Ist $I = (g_1, \ldots, g_n)$ ein Ideal in einem integren noetherschen Ring R und gilt $g_i \neq 0$ für alle i, so erhält man das Blow-up von $\operatorname{Spec}(R)$ mit Zentrum $V(I)$ durch Verklebung von affinen Schemata der Form*

$$U_i = \operatorname{Spec}\left(R\left[\frac{g_1}{g_i}, \ldots, \frac{g_n}{g_i}\right]\right)$$

für $1 \leq i \leq n$. Die Verklebungsvorschrift folgt aus den Relationen $g_i/g_j = (g_j/g_i)^{-1}$ auf $D(g_i) \cap D(g_j)$.

Beispiel 1.61. Es sei $X = \mathbb{A}^n_k = \operatorname{Spec}(k[x_1, \ldots, x_n])$ der n-dimensionale affine Raum und $Z = V((x_1, \ldots, x_n))$ der Ursprung. Dann wird $\operatorname{Bl}_Z(X)$ von n offenen affinen Teilmengen der Form $U_i = \operatorname{Spec}(R_i)$ mit

$$R_i = k\left[x_i, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right]$$

überdeckt. Der exzeptionelle Divisor ist in $\operatorname{Spec}(R_i)$ durch $V(x_i)$ gegeben.

Definition 1.62. Es sei wie oben $\pi\colon \operatorname{Bl}_Z(X) \to X$ ein Blow-up und es sei $Y \subset X$ ein abgeschlossenes Unterschema, gegeben durch ein quasi-kohärentes Ideal $\mathscr{I} \subset \mathscr{O}_X$.

(*i*) Das (schematische) Urbild $Y^* = \pi^{-1}(Y)$ bzw. die Idealgarbe $\mathscr{I}^* = \mathscr{I} \cdot \mathscr{O}_{\operatorname{Bl}_Z(X)}$ heißt *totale Transformation* von Y bzw. $\mathscr{I}$ unter dem Blow-up π.

(*ii*) Das abgeschlossene Unterschema $Y^{\mathrm{str}} = \operatorname{Bl}_{Z \cap Y}(Y)$ von $\operatorname{Bl}_Z(X)$ heißt *strikte Transformation* von Y unter dem Blow-up π.

Die strikte Transformation wird auch häufig definiert als Abschluss $Y^{\mathrm{str}} = \overline{\pi^{-1}(Y \setminus Z)}$. Es bleibt noch die Frage nach dem Ideal von Y^{str} zu beantworten. Dazu führen wir den *Idealquotienten* ein:

Es sei $\mathscr{J} \subset \mathrm{Bl}_Z(X)$ das Ideal eines effektiven Cartier-Divisors, der auf einer offenen affinen Überdeckung U_i, $i \in I$, durch die Gleichung $h_i = 0$ gegeben ist. Weiter bezeichne $g\colon \mathscr{O}_{\mathrm{Bl}_Z(X)} \to \mathscr{O}_{\mathrm{Bl}_Z(X)}$ den Homomorphismus, der auf den U_i durch Multiplikation mit h_i gegeben ist. Wir definieren nun den Idealquotienten als

$$(\mathscr{I}^* : \mathscr{J}) = \ker\left(\mathscr{O}_{\mathrm{Bl}_Z(X)} \xrightarrow{g} \mathscr{O}_{\mathrm{Bl}_Z(X)} \longrightarrow \mathscr{O}_{\mathrm{Bl}_Z(X)}/\mathscr{I}^*\right).$$

Für das Ideal der strikten Transformation ist eine Beschreibung mittels Idealquotienten möglich. Das folgende Resultat stammt aus [25], S. 30:

Proposition 1.63. *In der Situation von Definition 1.62 ist durch*

$$\mathscr{I}^{\mathrm{str}} = \bigcup_{n \geq 0} (\mathscr{I}^* : \mathscr{I}_E^n)$$

das Ideal zu Y^{str} gegeben, wobei $\mathscr{I}_E$ das definierende Ideal des exzeptionellen Divisors E bezeichnet.

Es reicht, die Situation im Affinen zu betrachten: Es sei $X = \mathrm{Spec}(R)$ und $\mathrm{Spec}(S)$ ein offener affiner Teil des Blow-ups von X. Weiter sei $f\colon R \to S$ der zugehörige Ringhomomorphismus. Wir bezeichnen die Ideale der abgeschlossenen Unterschemata $Y \subset X$ und $Y^* \subset S$ mit I bzw. I^*. Als Cartier-Divisor ist E (zumindest nach Verkleinern der affinen Schemata) durch ein Hauptideal $(h) \subset S$ gegeben.

Proposition 1.64. *Ist $I = (b)$ ein Hauptideal und bezeichnet b^* das Bild von b in S, dann ist die strikte Transformation ebenfalls ein Hauptideal $I^{\mathrm{str}} = (b^{\mathrm{str}})$ mit $b^{\mathrm{str}} = h^{-m} \cdot b^*$. Dabei ist $m \geq 0$ der größte Exponent, für den b^* durch h^m teilbar ist.*

Das folgende Resultat ist Lemma 6.3 in [25]. Der Beweis obiger Proposition ergibt sich direkt aus der Aussage des Lemmas, wenn $a \in R$ ein Element mit $f(a) = h$ bezeichnet:

Lemma 1.65. *Es seien $f\colon R \to S$ ein Ringhomomorphismus, $a \in R$ ein Element und $I \subset R$ ein Ideal. Es bezeichne $f_a\colon R_a \to S_{f(a)}$ den durch die Lokalisierung induzierten Homomorphismus, $I^* = f(I) \cdot S$ und $(I \cdot R_a)^* = f_a(I \cdot R_a) \cdot S_{f(a)}$. In diesem Fall gilt*

$$\bigcup_{n \geq 0} (I^* : (f(a))^n) = (I \cdot R_a)^* \cap S. \tag{1.10}$$

Beweis. Ein Element $u \in S$ liegt genau dann in der linken Seite von (1.10), wenn $uf(a)^n$ für ein n in I^* liegt, also wenn $uf(a)^n = \sum_j \lambda_j f(x_j)$ für Elemente $x_j \in I$ und $\lambda_j \in S$ ge-

schrieben werden kann. Diese Gleichung können wir umschreiben zu $u = \sum_j \lambda_j f_a(x_j/a^n)$, was $u \in (I \cdot R_a)^*$ beweist. □

Beispiel 1.66. Es sei $Y \subset \mathbb{A}^n_k$ ein abgeschlossenes Unterschema, das den Ursprung enthält. Das Blow-up von Y im Ursprung erhält man, indem man die strikte Transformation Y^{str} bzgl. des Blow-ups von $\mathbb{A}^n_k$ im Ursprung bildet. Die Berechnung eines endlichen Erzeugendensystems der strikten Transformation eines Ideals ist im Allgemeinen sehr aufwendig. Für die strikte Transformation eines Hauptideals kann Proposition 1.64 genutzt werden. In der Regel bilden die strikten Transformationen der Erzeuger eines Ideals kein Erzeugendensystem der strikten Transformation des Ideals.

Das folgende Beispiel soll das praktische Vorgehen demonstrieren. Es zeigt auch, dass der exzeptionelle Divisor eines Blow-ups nicht zwangsläufig irreduzibel ist.

Beispiel 1.67 (A_2-Flächensingularität)**.** Es sei $f = x^2 + y^2 + z^3 \in \mathbb{C}[x, y, z]$. Wir betrachten das abgeschlossene Unterschema $X = \mathrm{V}(f) \subset \mathbb{A}^3_{\mathbb{C}}$, das am Punkt $(0, 0, 0)$ singulär ist. Wir bilden das Blow-up von $\mathbb{A}^3_{\mathbb{C}}$ mit Zentrum $\{(0, 0, 0)\}$, aufgefasst als reduziertes Schema, und betrachten darin das abgeschlossene Unterschema, welches durch die strikte Transformation des Ideals (f) gegeben ist. Dieses ist das Blow-up von X im singulären Punkt. Das Blow-up wird von drei affinen Schemata überdeckt:

- x-Karte: Durch Division von f durch x^2 ergibt sich die strikte Transformation, also

$$f^{\text{str}} = 1 + \left(\frac{y}{x}\right)^2 + x\left(\frac{z}{x}\right)^3 \in \mathbb{C}\left[x, \frac{y}{x}, \frac{z}{x}\right].$$

  Der exzeptionelle Divisor wird in diesem offenen affinen Unterschema durch die Gleichung $x = 0$ beschrieben, ist also das Spektrum des Rings

$$\begin{aligned}\mathbb{C}\left[\frac{y}{x}, \frac{z}{x}\right] / \left(1 + \left(\frac{y}{x}\right)^2\right) &\cong \mathbb{C}\left[\frac{y}{x}, \frac{z}{x}\right] / \left(1 + \sqrt{-1} \cdot \frac{y}{x}\right) \times \mathbb{C}\left[\frac{y}{x}, \frac{z}{x}\right] / \left(1 - \sqrt{-1} \cdot \frac{y}{x}\right) \\ &\cong \mathbb{C}\left[\frac{z}{x}\right] \times \mathbb{C}\left[\frac{z}{x}\right],\end{aligned}$$

  was der disjunkten Vereinigung von zwei affinen Räumen $\mathbb{A}^1_{\mathbb{C}}$ entspricht.

- y-Karte: Die Situation ist hier völlig symmetrisch zur x-Karte.

- z-Karte: Die strikte Transformation von f ist

$$f^{\text{str}} = \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 + z \in \mathbb{C}\left[\frac{x}{z}, \frac{y}{z}, z\right]$$

  mit exzeptionellem Divisor

$$\mathbb{C}\left[\frac{x}{z}, \frac{y}{z}\right] / \left(\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2\right) \cong \mathbb{C}\left[\frac{x}{z}, \frac{y}{z}\right] / \left(\left(\frac{x}{z} + \sqrt{-1} \cdot \frac{y}{z}\right)\left(\frac{x}{z} - \sqrt{-1} \cdot \frac{y}{z}\right)\right).$$

Hieraus ist ersichtlich, dass sich die beiden Komponenten des exzeptionellen Divisors in dieser Karte schneiden, nämlich im Punkt zum maximalen Ideal $(x/z, y/z)$.

In allen drei Karten ist das durch f^{str} gegebene abgeschlossene Unterschema glatt, somit löst bereits ein Blow-up die Singularität auf. Der exzeptionelle Divisor besteht aus zwei sich schneidenden irreduziblen Komponenten, wobei die Verklebung durch die offensichtlichen Relationen $x/z \cdot z/x = 1$ etc. gegeben ist. Beide Komponenten sind jeweils isomorph zum projektiven Raum $\mathbb{P}^1_{\mathbb{C}}$.

Definition 1.68. Es sei X ein reduziertes, eigentliches k-Schema. Eine *Auflösung der Singularitäten* von X ist ein eigentlicher birationaler Morphismus $f\colon X' \to X$, sodass X' regulär ist.

Bemerkung 1.69. Im Fall $\mathrm{char}(k) = 0$ bewies Hironaka in [27] die Existenz einer Auflösung der Singularitäten, welche durch eine Folge von geeigneten Blow-ups erhalten werden kann. Im Jahr 2017 veröffentlichte Hironaka auf seiner Homepage den Artikel [28], in dem die Existenz einer Auflösung von Singularitäten in positiver Charakteristik bewiesen wird. Die Korrektheit des Beweises ist noch nicht bestätigt.

Um Singularitäten zu klassifizieren, wird ein geeigneter Isomorphie-Begriff benötigt. Die lokalen Ringe singulärer Punkte verfügen dabei noch über zu viele Informationen, sodass etwa reguläre Punkte in unterschiedlichen Isomorphie-Klassen liegen würden. Anders verhält es sich bei den Vervollständigungen der lokalen Ringe (siehe Prop. 1.43).

Definition 1.70. Sind R_1 und R_2 lokale Ringe von singulären Punkten von reduzierten, eigentlichen k-Schemata, dann bezeichnen wir die Singularitäten als *formal isomorph*, wenn die vervollständigten Ringe $\hat{R}_1$ und $\hat{R}_2$ isomorph sind.

2 Klassische Kummer-Varietäten

In diesem Kapitel sei A eine g-dimensionale abelsche Varietät über einem Grundkörper k der Charakteristik $\mathrm{char}(k) \neq 2$. Wenn $g \geq 2$ gilt und k algebraisch abgeschlossen ist, weist die zugehörige Kummer-Varietät A/ι genau $2^{2g} = 4^g$ isolierte Singularitäten auf, die alle formal isomorph sind, d. h., die vervollständigten lokalen Ringe der singulären Punkte sind isomorph. In Abschnitt 2.1 werden einige Eigenschaften dieser Singularitäten ermittelt, in Abschnitt 2.2 wird die klassische Kummer-Konfiguration, die die Lage der Singularitäten zueinander widerspiegelt, beschrieben und verallgemeinert.

2.1 Eigenschaften der Singularitäten

Das Ziel dieses Abschnitts ist, den vervollständigten lokalen Ring der Singularität von A/ι am Bildpunkt des neutralen Elements zu bestimmen und hiermit einige Kennzahlen und Eigenschaften der Singularität zu ermitteln. Einige Resultate wie die Auflösung der Singularität sind bekannt, siehe z. B. [14], Abschnitt 2.2 im Fließtext, allerdings ist ein Beweis nicht auffindbar, weshalb dieser hier ergänzt wird.

2.1.1 Eigenschaften des lokalen Rings

Zur Bestimmung der Singularitäten wird die induzierte Wirkung der Vorzeicheninvolution ι auf dem Tangentialraum $T_e(A)$ und dessen Dualraum betrachtet. Wir beginnen mit der Beobachtung, dass ι auf dem Tangentialraum ebenfalls die Vorzeicheninvolution induziert (siehe etwa [6], Abs. I.3.2):

Lemma 2.1. *Es bezeichne ι die Vorzeicheninvolution und e das neutrale Element der abelschen Varietät A. Dann ist die Abbildung $T_e(\iota)\colon T_e(A) \to T_e(A)$ auf dem Tangentialraum durch $x \mapsto -x$ gegeben.*

Beweis. Die Komposition $f\colon A \xrightarrow{(\mathrm{id},\iota)} A \times A \xrightarrow{\mu} A$ ist konstant, faktorisiert also durch die abgeschlossene Einbettung $\{e\} \hookrightarrow A$. Entsprechend kann der Morphismus auf Halmen als Komposition $\mathscr{O}_{A,e} \to k \to \mathscr{O}_{A,e}$ geschrieben werden. Das Bild des maximalen Ideals ist daher das Nullideal und die Ableitung $T_e(f)$ ist die Nullabbildung. Die Rechnung

$$\begin{aligned} 0 = T_e(f) &= T_e(\mu \circ (\mathrm{id}_A, \iota)) = T_{(e,e)}(\mu) \circ T_e((\mathrm{id}_A, \iota)) \\ &= T_{(e,e)}(\mu) \circ (\mathrm{id}_{T_e(A)}, T_e(\iota)) = \mathrm{id}_{T_e(A)} + T_e(\iota) \end{aligned}$$

zeigt nun die Behauptung. Dabei wurde $T_p(\mathrm{id}_A) = \mathrm{id}_{T_p(A)}$ sowie $T_p(\beta\circ\alpha) = T_{\alpha(p)}(\beta)\circ T_p(\alpha)$ benutzt. □

Die folgende Aussage wird im Beweis von Theorem 10.6 in [3] für den Fall einer abelschen Fläche gezeigt, sie lässt sich jedoch genau so für g-dimensionale abelsche Varietäten beweisen.

Lemma 2.2. *Ist A eine abelsche Varietät der Dimension g, dann existiert ein Erzeugendensystem $u_1, \ldots, u_g$ von $\mathfrak{m} \subset \mathscr{O}_{A,e}$, auf dem die Vorzeicheninvolution durch $\iota^*(u_i) = -u_i$ für $i = 1, \ldots, g$ operiert.*

Beweis. Die Abbildung $T_e(\iota)\colon T_e(A) \to T_e(A)$ auf dem Tangentialraum ist nach Lemma 2.1 durch $x \mapsto -x$ gegeben, entsprechend erhält man den hierzu dualen Endomorphismus auf $T_e(A)^*$ durch $f \mapsto -f$. Da $T_e(A)^*$ als k-Vektorraum kanonisch isomorph zu $\mathfrak{m}/\mathfrak{m}^2$ ist, erhalten wir die induzierte k-lineare Abbildung

$$\bar{\iota}^*\colon \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{m}/\mathfrak{m}^2, \quad x \longmapsto -x.$$

Da $\mathscr{O}_{A,e}$ regulär ist, existiert ein Erzeugendensystem von $\mathfrak{m}$ aus g Elementen $u_1', \ldots, u_g'$. Dazu betrachten wir die Elemente $u_i = u_i' - \iota^*(u_i')$ für $1 \le i \le n$. Offenbar ist die Bedingung $\iota^*(u_i) = -u_i$ erfüllt. Es bleibt daher nur noch zu zeigen, dass $u_1, \ldots, u_g$ ein Erzeugendensystem von $\mathfrak{m}$ ist. Nach obiger Betrachtung gilt

$$\begin{aligned} \iota^*(u_i') &\equiv -u_i' \mod \mathfrak{m}^2, \\ u_i = u_i' - \iota^*(u_i') &\equiv 2u_i' \mod \mathfrak{m}^2 \end{aligned}$$

für $1 \le i \le g$. Da $2 \neq 0$ in k gilt, folgt nun aus dem Nakayama-Lemma, dass $u_1, \ldots, u_g$ das maximale Ideal $\mathfrak{m}$ erzeugen. □

Die Vervollständigung von $\mathscr{O}_{A,e}$ bzgl. $\mathfrak{m}$ ist ein vollständiger, noetherscher, regulärer, lokaler Ring, der den Restekörper k enthält, somit ein Potenzreihenring (Prop. 1.43). Wählt man das Parametersystem wie im Lemma, erhält man

$$\hat{\mathscr{O}}_{A,e} \cong k[\![u_1, \ldots, u_g]\!].$$

Hierauf operiert die Vorzeicheninvolution durch $\iota^*(u_i) = -u_i$ für alle i. Ist ein beliebiges Element $f \in k[\![u_1, \ldots, u_g]\!]$ invariant unter dieser Wirkung, so müssen bereits alle Summanden $f_{i_1,\ldots,i_g} u_1^{i_1} \cdots u_g^{i_g}$ invariant sein. Für alle Monome ist daher $i_1 + \ldots + i_g$ eine gerade Zahl und f kann als Potenzreihe in den Unbestimmten $u_i u_j$ für $1 \le i, j \le g$ dargestellt werden. Umgekehrt ist jede solche Potenzreihe invariant, also ist der Invariantenring $\hat{\mathscr{O}}_{A,e}^{\iota}$ durch $k[\![u_i u_j,\, 1 \le i, j \le g]\!]$ gegeben. Da nach Proposition 1.52 Lokalisierung/Vervollständigung

verträglich mit der Bildung des Invariantenrings ist, ist dieser Ring auch der gesuchte vervollständigte lokale Ring der Kummer-Varietät zu A am Bild des neutralen Elements, das für $g \geq 2$ ein singulärer Punkt ist.

Proposition 2.3. *Es bezeichne A eine g-dimensionale abelsche Varietät und A/ι die zugehörige Kummer-Varietät. Der vervollständigte lokale Ring $\hat{\mathcal{O}}^{\iota}_{A,e} = \hat{\mathcal{O}}_{A/\iota,p(e)}$ ist isomorph zum Unterring $k[\![u_i u_j,\, 1 \leq i,j \leq g]\!] \subset k[\![u_1,\ldots,u_g]\!]$. Insbesondere sind die Singularitäten aller g-dimensionalen Kummer-Varietäten formal isomorph.*

Die Darstellung einer invarianten Potenzreihe ist dabei nicht eindeutig. Zwei Potenzreihen beschreiben das gleiche Element des Invariantenrings, wenn man die auftretenden u_i in andere Paare aufteilen und so die eine Darstellung des Elements in die andere überführen kann. Die Relationen zwischen den Erzeugern $u_i u_j$ bilden den Kern des Homomorphismus

$$k[\![a_{\{i,j\}},\ 1 \leq i,j \leq g]\!] \longrightarrow k[\![u_i u_j,\ 1 \leq i,j \leq g]\!], \quad a_{\{i,j\}} \longmapsto u_i u_j.$$

Die Indizierung mit Mengen $\{i,j\}$ berücksichtigt dabei bereits den Umstand, dass die Reihenfolge der Faktoren im Produkt $u_i u_j$ keine Rolle spielt. Der Kern wird von den Polynomen der Form $a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,l\}}a_{\{j,m\}}$ mit $i,j,l,m \in \{1,\ldots,g\}$, erzeugt, was genau dem oben beschriebenen Aufteilen der u_i in andere Paare entspricht.

Es werden nun einige Kennzahlen der Singularität $\hat{\mathcal{O}}_{A/\iota,p(e)}$ ermittelt. Hierzu werden die folgenden Bezeichnungen verwendet:

$$\begin{aligned} S &= k[\![a_{\{i,j\}},\ 1 \leq i,j \leq g\,]\!], \\ J &= \left(a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,l\}}a_{\{j,m\}},\ i,j,l,m \in \{1,\ldots,g\}\right) \subset S, \\ R &= S/J \left(\cong \hat{\mathcal{O}}_{A/\iota,p(e)}\right). \end{aligned} \tag{2.1}$$

Weiter bezeichnen $\mathfrak{n} \subset S$, $\mathfrak{m} \subset R$ die maximalen Ideale.

Proposition 2.4. *Für den Ring R gelten die folgenden Aussagen:*

(*i*) *Die Einbettungsdimension beträgt* $\operatorname{edim}(R) = g(g+1)/2$*, die Anzahl der Unbestimmten $a_{\{i,j\}}$. Insbesondere ist R genau für $g \leq 1$ regulär.*

(*ii*) *Eine reguläre Folge der Länge g ist durch die Elemente $a_{\{1\}},\ldots,a_{\{g\}} \in R$ gegeben. Damit ist R ein Cohen–Macaulay-Ring.*

(*iii*) *Der Ring R ist genau dann ein Gorenstein-Ring, wenn $g = 1$ oder g eine gerade Zahl ist. Es gilt nämlich*

$$\dim_k\left(\operatorname{Ext}^g_R(k,R)\right) = \begin{cases} 1, & \text{wenn } g \text{ gerade oder } g = 1, \\ g, & \text{wenn } g \geq 3 \text{ ungerade.} \end{cases}$$

Beweis. (i): Wir betrachten die Linearkombination

$$\sum_{i,j} \lambda_{\{i,j\}} a_{\{i,j\}} = 0 \in \mathfrak{m}/\mathfrak{m}^2$$

mit Koeffizienten $\lambda_{\{i,j\}} \in k$. Dies bedeutet, dass über S die Aussage

$$\sum_{i,j} \lambda_{\{i,j\}} a_{\{i,j\}} \in \mathfrak{n}^2 + J = \mathfrak{n}^2$$

gilt, welche wegen der Regularität von S oder nach Vergleich der Grade wiederum nur erfüllt sein kann, wenn alle $\lambda_{\{i,j\}}$ verschwinden.

(ii): Wir fassen R als Unterring von $k[\![u_1, \ldots, u_g]\!]$ auf. Wenn eine formale Potenzreihe f nicht im Ideal $(u_1^2, \ldots, u_{i-1}^2)$ enthalten ist, dann gilt auch $f \cdot u_i^2 \notin (u_1^2, \ldots, u_{i-1}^2)$. Somit ist $a_{\{i\}}$ kein Nullteiler in $R/(a_{\{1\}}, \ldots, a_{\{i-1\}})$.

(iii): Es sei $\bar{R} = R/(a_{\{1\}}, \ldots, a_{\{g\}})$. Nach (1.7) gilt die Isomorphie

$$\mathrm{Ext}_R^g(k, R) \cong \mathrm{Hom}_R\left(k, \bar{R}\right)$$

von R-Moduln (und damit von k-Vektorräumen). Jeder R-Homomorphismus $\phi\colon k \to \bar{R}$ ist durch das Bild von $1 \in k$ eindeutig festgelegt und eine solche Festlegung liefert genau dann einen wohldefinierten R-linearen Homomorphismus, wenn

$$a_{\{i,j\}} \phi(1) = 0 \tag{2.2}$$

für alle i, j gilt. Für eine $2d$-elementige Teilmenge $I \subset \{1, \ldots, g\}$ benutzen wir nun die Kurzschreibweise

$$a_I = a_{\{i_1,i_2\}} \cdots a_{\{i_{2d-1},i_{2d}\}}$$

sowie $a_\emptyset = 1$. Das Element $a_I \in R$ ist wohldefiniert, da die Aufteilung der Indizes auf die Faktoren keine Rolle spielt. Weiter kann jedes Element aus $\bar{R}$ als k-Linearkombination von Elementen der Form a_I geschrieben werden, denn sobald $|\{i_1, i_2, i_3, i_4\}| < 4$ gilt, folgt $a_{\{i_1,i_2\}} a_{\{i_3,i_4\}} = 0$. Ist etwa

$$\phi(1) = \sum_{\substack{I \subset \{1,\ldots,g\} \\ |I| \equiv 0 \bmod 2}} \mu_I \, a_I \in \bar{R}$$

mit $\mu_I \in k$ gegeben, so ist Bedingung (2.2) gleichbedeutend damit, dass $\mu_I = 0$ für alle $I \subset \{1, \ldots g\}$ mit $|I| \leq g - 2$ gilt. Wenn g eine gerade Zahl ist, muss also

$$\phi(1) = \mu \cdot a_{\{1,2\}} \cdots a_{\{g-1,g\}}$$

mit $\mu \in k$ gelten und für jedes μ erhält man einen Homomorphismus. Ist $g > 1$ ungerade,

dann entsprechen die gesuchten R-Homomorphismen genau den Werten

$$\phi(1) \in k \cdot a_{\{1,\ldots,g\}\setminus\{1\}} + \ldots + k \cdot a_{\{1,\ldots,g\}\setminus\{g\}}$$

und somit gilt $\operatorname{Ext}^g_R(k,R) \cong k^g$ als k-Vektorräume. □

Wenn R ein Cohen–Macaulay-Ring und G eine endliche Gruppe von Ringautomorphismen ist, deren Ordnung in R invertierbar ist, dann ist wohlbekannt, dass der Invariantenring R^G die Cohen–Macaulay-Eigenschaft erbt (siehe Prop. 13 in [29]).

Für Quotienten von $\mathbb{A}^n_k$ nach einer endlichen Gruppe $G \subset \mathrm{GL}_n(k)$ kann die Gorenstein-Eigenschaft mithilfe von [55], Theorem 1, direkt an G abgelesen werden. Für jede endliche Untergruppe $G \subset \mathrm{GL}_n(k)$, die keine Elemente $A \in G$ mit $\operatorname{rank}(A-I) = 1$ enthält und deren Ordnung nicht von der Charakteristik von k geteilt wird, gilt: Der Ring $k[x_1,\ldots,x_n]^G$ ist genau dann ein Gorenstein-Ring, wenn $G \subset \mathrm{SL}_n(k)$ gilt.

Lässt man nun $G = \{-I, I\} \subset \mathrm{GL}_g(k)$ auf $k[u_1,\ldots,u_g]$ operieren, so ist die induzierte Gruppenwirkung auf der Vervollständigung $k[\![u_1,\ldots,u_g]\!]$ identisch mit der Wirkung auf dem komplettierten Halm $\hat{\mathscr{O}}_{A,e}$; folglich ist die Singularität $\hat{\mathscr{O}}_{A/\iota,e}$ für geradzahliges $g \geq 2$ ein Gorenstein-Ring.

Proposition 2.5. *Der Ring R ist genau dann ein vollständiger Durchschnitt, wenn $g \leq 2$ gilt. Man erhält*

$$\delta(R) = \frac{g(g-1)(g-2)(g+3)}{12}.$$

als Defekt der Vollständiger-Durchschnitt-Eigenschaft.

Beweis. Im Lichte von Proposition 1.46 kann mithilfe eines minimalen Erzeugendensystems des Ideals $J \subset S$ ermittelt werden, ob R ein vollständiger Durchschnitt ist. Dazu betrachten wir das Erzeugendensystem aus (2.1) genauer, eingeteilt in die drei Typen

$$\begin{aligned}
&1.)\ \ a^2_{\{i,j\}} - a_{\{i\}}a_{\{j\}},\ |\{i,j\}| = 2,\\
&2.)\ \ a_{\{i,j\}}a_{\{i,l\}} - a_{\{i\}}a_{\{j,l\}},\ |\{i,j,l\}| = 3,\\
&3.)\ \ a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,l\}}a_{\{j,m\}},\ |\{i,j,l,m\}| = 4.
\end{aligned}$$

Sind i,j,l,m paarweise verschieden, dann existieren bis auf Vorzeichen drei verschiedene Elemente des dritten Typs, nämlich zwei, in denen $a_{\{i,j\}}a_{\{l,m\}}$ als Summand auftritt, und ein Element, in dem $a_{\{i,j\}}$ gar nicht auftritt. Wegen

$$\big(a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,l\}}a_{\{j,m\}}\big) - \big(a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,m\}}a_{\{j,l\}}\big) = a_{\{i,m\}}a_{\{j,l\}} - a_{\{i,l\}}a_{\{j,m\}}$$

werden lediglich $2\binom{g}{4}$ Erzeuger (für jede vier-elementige Teilmenge zwei Elemente) des

dritten Typs benötigt, um das Ideal $J \subset S$ zu erzeugen. Außer diesen gibt es $\binom{g}{2}$ Elemente vom ersten und $g\binom{g-1}{2}$ Elemente vom zweiten Typ. Diese Zahlen summieren sich insgesamt zu $g^2(g+1)(g-1)/12$ Elementen, die für ein Erzeugendensystem von J ausreichen. Nach Wahl der Erzeuger des dritten Typs bilden diese Elemente ein minimales Erzeugendensystem von J: Nach dem Nakayama-Lemma reicht es zu zeigen, dass die Restklassen dieser Erzeuger von J im k-Vektorraum $J/\mathfrak{n}J$ linear unabhängig sind. Eine k-Linearkombination dieser Elemente ist ein homogenes Polynom vom Grad 2 und kann daher nicht in $\mathfrak{n}J$ liegen, außer wenn sie bereits in S trivial ist. Es sei die Linearkombination der Null

$$\begin{aligned} 0 \;=\; & \sum_{|\{i,j\}|=2} \mu_{\{i,j\}}(a_{\{i,j\}}^2 - a_{\{i\}}a_{\{j\}}) + \sum_{\substack{|\{j,l\}|=2 \\ i\notin\{j,l\}}} \mu_{(i,\{j,l\})}(a_{\{i,j\}}a_{\{i,l\}} - a_{\{i\}}a_{\{j,l\}}) \\ & + \sum_{|\{i,j,l,m\}|=4} \mu_{\{i,j,l,m\}}(a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,l\}}a_{\{j,m\}}) + \nu_{\{i,j,l,m\}}(a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,m\}}a_{\{j,l\}}) \end{aligned}$$

in S mit Koeffizienten in k gegeben. Die $\mu_{\{i,j\}}$ verschwinden, da $a_{\{i,j\}}^2$ sonst nicht wegfallen kann, mit gleichem Argument verschwinden die $\mu_{(i,\{j,l\})}$. Damit der Faktor $a_{\{i,j\}}a_{\{l,m\}}$ wegfällt, muss $\mu_{\{i,j,l,m\}} = -\nu_{\{i,j,l,m\}}$ gelten. Mithin sind auch diese Vorfaktoren null, da andernfalls die zweiten Summanden der Elemente des dritten Typs nicht ausgelöscht werden. Wir erhalten somit den Defekt

$$\delta(R) = \frac{g^2(g+1)(g-1)}{12} - \frac{g(g+1)}{2} + g = \frac{g(g-1)(g-2)(g+3)}{12} \;,$$

der nur für $g \leq 2$ verschwindet. □

In kleiner Dimension können die Aussagen, dass R regulär oder ein vollständiger Durchschnitt ist, auch durch bestimmte homologische Kennzahlen ausgedrückt werden:

Bemerkung 2.6. Für einen lokalen Ring R mit Restekörper k ist die *Poincaré-Reihe* durch

$$\mathrm{P}(t) = \sum_{j=0}^{\infty} b_j(R)t^j$$

definiert mit Koeffizienten $b_j(R) = \dim_k(\mathrm{Tor}_j^R(k,k))$. Die Poincaré-Reihe besitzt nach [23], Corollary 3.1.3, eine Produktdarstellung der Form

$$\mathrm{P}(t) \;=\; \prod_{i=0}^{\infty} \frac{(1+t^{2i+1})^{\epsilon_{2i}}}{(1-t^{2i+2})^{\epsilon_{2i+1}}}$$

für geeignete natürliche Zahlen ϵ_l, $l \geq 0$. Der Zahlenwert ϵ_l wird auch die *l-te Deviation* (engl. *deviation*: Abweichung) von R genannt. Es ist bekannt, dass ϵ_0 mit der Einbettungsdimension von R übereinstimmt, dass R genau dann regulär ist, wenn $\epsilon_1 = 0$ gilt, und

dass ϵ_2 genau für vollständige Durchschnitte verschwindet ([23], Def. 1.4.11, Thm. 1.4.13, Thm. 3.5.1). Ein lokaler Ring mit $\epsilon_0 = 0$ ist folglich ein Körper. Für R wie in (2.1) mit $g = \dim(R)$ gelten daher die Äquivalenzen

$$\epsilon_0 = 0 \Leftrightarrow g = 0, \quad \epsilon_1 = 0 \Leftrightarrow g \leq 1, \quad \epsilon_2 = 0 \Leftrightarrow g \leq 2.$$

Diese Folge von Äquivalenzen kann nicht weiter fortgesetzt werden: Nach [23], Theorem 3.5.1, ist die Bedingung $\epsilon_2 = 0$ äquivalent zu $\epsilon_3 = 0$. Wir wissen aber, dass R im Fall $g = 3$ kein vollständiger Durchschnitt ist, also $\epsilon_3 \neq 0$ gelten muss.

Eine weitere wichtige Größe zur Beschreibung eines lokalen Rings ist das *Hilbert–Samuel-Polynom*. Dazu sei daran erinnert, dass die *Länge* eines R-Moduls M die maximale Länge einer Kette von Untermoduln ist. Das Hilbert–Samuel-Polynom $P_R \in \mathbb{Q}[T]$ ist dadurch charakterisiert, dass

$$P_R(r) = \operatorname{length}_R\left(R/\mathfrak{m}^{r+1}\right)$$

für alle hinreichend großen $r \in \mathbb{N}$ gilt. Häufig wird $P_R(r)$ auch über die Länge von $R/\mathfrak{m}^r$ statt $R/\mathfrak{m}^{r+1}$ definiert, was aber weder den Grad noch den Leitkoeffizienten ändert. Der Grad von P_R stimmt mit $g = \dim(R)$ überein. Bezeichnet α den Leitkoeffizienten, dann ist die *Multiplizität* μ des maximalen Ideals definiert als $\mu = g!\,\alpha$.

Proposition 2.7. *Das Hilbert–Samuel-Polynom von R wie in* (2.1) *ist durch*

$$P_R(r) = \frac{1}{2^{g+1}} + \sum_{l=0}^{g} \frac{1}{2^{l+1}} \binom{g-l+2r}{g-l}$$

gegeben. Es gibt die korrekte Länge von $R/\mathfrak{m}^{r+1}$ sogar für jedes $r \in \mathbb{N}$. Die Multiplizität des singulären Punktes von $\operatorname{Spec}(R)$ *beträgt $\mu = 2^{g-1}$.*

Zur Vorbereitung des Beweises werden zwei Identitäten mit Binomialkoeffizienten nachgerechnet, welche für die Beschreibung des Hilbert–Samuel-Polynoms benötigt werden. Zumindest die erste der beiden Gleichungen ist wohlbekannt als Summenregel im Pascalschen Dreieck.

Lemma 2.8. *Es gelten die beiden Summenformeln*

$$\sum_{j=0}^{m} \binom{g-1+j}{g-1} = \binom{g+m}{g} \quad \text{für } m, g \in \mathbb{N},\ g \geq 1,$$

$$\sum_{j=0}^{2m} (-1)^j \binom{g-1+j}{g-1} = \sum_{j=0}^{m} \binom{(g-1)+2j-1}{(g-1)-1} \quad \text{für } m, g \in \mathbb{N},\ g \geq 2.$$

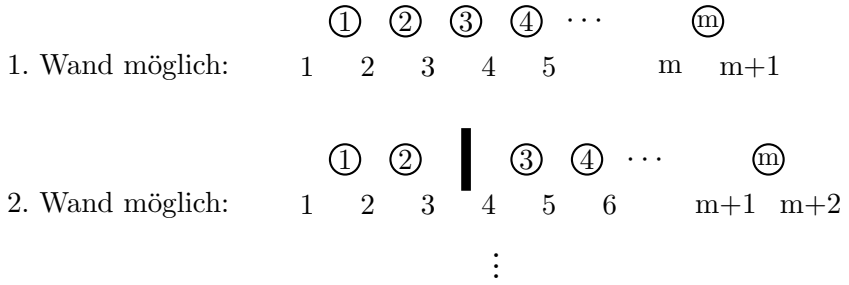


Abbildung 3: Veranschaulichung der Zählung in (2.3)

Beweis. Wir verfahren mit vollständiger Induktion nach m. Der Induktionsanfang für $m = 0$ und festes g ist in beiden Fällen trivial. Die erste Gleichung folgt aus der Additionsregel im Pascalschen Dreieck: Gilt die Aussage bereits für $m-1$, dann ist

$$\sum_{j=0}^{m} \binom{g-1+j}{g-1} = \binom{g-1+m}{g-1} + \binom{g+(m-1)}{g} = \binom{g+m}{g}.$$

Ähnlich folgt die zweite Gleichung: Wieder sei g fest gewählt und die Aussage gelte für $m-1$. Es gilt

$$\binom{(g-1)+2m}{g-1} - \binom{(g-1)+2m-1}{g-1} = \binom{(g-1)+2m-1}{(g-1)-1}$$

und damit lässt sich durch die Rechnung

$$\begin{aligned}\sum_{j=0}^{2m}(-1)^j\binom{g-1+j}{g-1} &= \sum_{j=0}^{2(m-1)}(-1)^j\binom{g-1+j}{g-1} + \binom{(g-1)+2m-1}{(g-1)-1} \\ &= \sum_{j=0}^{m-1}\binom{(g-1)+2j-1}{(g-1)-1} + \binom{(g-1)+2m-1}{(g-1)-1}.\end{aligned}$$

die linke Seite der Gleichung in die rechte Seite umformen. □

Beweis von Proposition 2.7. Da R eine lokale k-Algebra ist und aus diesem Grund jeder einfache R-Modul isomorph zum Restekörper k ist, stimmt die Länge von $R/\mathfrak{m}^{r+1}$ mit der Dimension als k-Vektorraum überein. Wir fassen $R \cong k[\![u_i u_j,\ 1 \le i,j \le g]\!]$ als Unterring des formalen Potenzreihenrings in g Unbestimmten auf. Als k-Vektorraum ist $R/\mathfrak{m}^{r+1}$ nichts anderes als der Raum aller Polynome, deren Grad höchstens $2r$ beträgt und die nur aus Monomen von geradzahligem Grad bestehen.

Der Vektorraum der homogenen Polynome von Grad m in g Unbestimmten hat Dimension $\binom{g-1+m}{g-1}$. Diese Tatsache kann man sich mit dem folgenden Modell kombinatorisch veranschaulichen (siehe auch Abb. 3): Angenommen, es sind m Kugeln in einer Reihe an-

geordnet, welche durch Einfügen von $g-1$ Wänden in g Mengen aufgeteilt werden sollen. Dabei ist die leere Menge durch Aufstellen von zwei Trennwänden nebeneinander erlaubt. Für die erste Wand gibt es $m+1$ mögliche Positionen. Für die zweite Wand existieren nun $m+2$ mögliche Positionen, da durch die erste Wand ein weiteres Objekt hinzugekommen ist. Für die letzte Wand existieren schließlich $m+g-1$ Möglichkeiten. Insgesamt erhält man, da die Abfolge des Platzierens der Wände irrelevant ist,

$$\frac{(m+1)(m+2)\cdots(m+g-1)}{(g-1)!} = \binom{g-1+m}{g-1} \tag{2.3}$$

verschiedene Aufteilungen. Die Anzahl der Kugeln in den g Teilmengen entspricht den Exponenten der g Unbestimmten eines Monoms vom Grad m und man erhält auf diese Weise alle Monome.

Es reicht nun zu zeigen, dass die Gleichung

$$\sum_{j=0}^{r} \binom{g-1+2j}{g-1} = \frac{1}{2^{g+1}} + \sum_{l=0}^{g} \frac{1}{2^{l+1}} \binom{g-l+2r}{g-l} \tag{2.4}$$

erfüllt ist. Es sei r fest gewählt. Der Beweis verläuft über Induktion nach g. Im Fall $g=1$ ergeben beide Seiten den Wert $r+1$. Für den Induktionsschritt sei die Aussage für $g-1$ erfüllt. Mit den genannten Additionsregeln erhält man

$$\begin{aligned}
\sum_{j=0}^{r} \binom{g-1+2j}{g-1} &= \frac{1}{2} \sum_{j=0}^{2r} \left(1+(-1)^j\right) \binom{g-1+j}{g-1} \\
&= \frac{1}{2} \sum_{j=0}^{2r} \binom{g-1+j}{g-1} + \frac{1}{2} \sum_{j=0}^{2r} (-1)^j \binom{g-1+j}{g-1} \\
&= \frac{1}{2} \binom{g+2r}{g} + \frac{1}{2} \sum_{j=0}^{r} \binom{(g-1)+2j-1}{(g-1)-1} \\
&= \frac{1}{2} \binom{g+2r}{g} + \frac{1}{2} \left(\frac{1}{2^g} + \sum_{l=0}^{g-1} \frac{1}{2^{l+1}} \binom{(g-1)-l+2r}{(g-1)-l} \right) \\
&= \frac{1}{2^{0+1}} \binom{g-0+2r}{g-0} + \frac{1}{2^{g+1}} + \sum_{l=1}^{g} \frac{1}{2^{l+1}} \binom{g-l+2r}{g-l},
\end{aligned}$$

womit die Gleichung (2.4) gezeigt ist. Das Monom höchsten Grades von P_R ist im Summanden für $l=0$ enthalten, da hier die größte Anzahl an Faktoren auftritt, die die Unbestimmte r enthalten. Der Leitkoeffizient ist $\alpha = 2^{g-1}/g!$ und die Multiplizität des maximalen Ideals ist in diesem Fall also $\mu = 2^{g-1}$. □

2.1.2 Auflösung der Singularität

Es bezeichne $S_1 = k[a_{\{i,j\}},\ 1 \le i \le j \le g]$ den Polynomring in $g(g+1)/2$ Unbestimmten, $J_1 \subset S_1$ das Ideal, das von den gleichen Polynomen wie J in (2.1) erzeugt wird, und $R_1 = S_1/J_1$. Es gelten also $\hat{S}_1 = S$ und $\hat{R}_1 = R$ für die Vervollständigungen bzgl. des maximalen Ideals $\mathfrak{m} = (a_{\{i,j\}},\ 1 \le i, j \le g)$.

Es sei $\tilde{X} \to \mathrm{Spec}(S_1) \cong \mathbb{A}_k^{g(g+1)/2}$ das Blow-up mit dem Ursprung als Zentrum. Dieses wird von den offenen affinen Teilmengen

$$U_{\{l,m\}} = \mathrm{Spec}\left(k\left[a_{\{l,m\}},\ \frac{a_{\{i,j\}}}{a_{\{l,m\}}},\ 1 \le i, j \le g\right]\right)$$

mit $1 \le l, m \le g$ überdeckt. Das Blow-up $\tilde{Y} \to \mathrm{Spec}(R_1)$ mit dem singulären Punkt als Zentrum erhält man hieraus als die strikte Transformation des abgeschlossenen Unterschemas $\mathrm{Spec}(R_1) \subset \mathrm{Spec}(S_1)$ mit offener affiner Überdeckung durch

$$V_{\{l,m\}} = \mathrm{Spec}\left(k\left[a_{\{l,m\}},\ \frac{a_{\{i,j\}}}{a_{\{l,m\}}},\ 1 \le i, j \le g\right] / J_{\{l,m\}}\right), \tag{2.5}$$

wobei $J_{\{l,m\}}$ die strikte Transformation des Ideals J_1 in $U_{\{l,m\}}$ bezeichnet.

Es ist im Allgemeinen falsch, dass die strikte Transformation eines Ideals von den strikten Transformationen eines Erzeugendensystems dieses Ideals erzeugt wird. Wenn das Erzeugendensystem jedoch eine *Macaulay-Basis* ist, kann man so verfahren. Dieser Begriff wird nun genauer erläutert.

Es sei $A = k[x_1, \ldots, x_n]$ der Polynomring in n Unbestimmten, welcher zusammen mit der kanonischen Graduierung („Totalgrad“) als graduierter Ring aufgefasst wird. Für ein Polynom $0 \neq f \in A$ bezeichne $\mathrm{in}(f)$ die homogene Komponente kleinsten Grades von f. Per Konvention wird $\mathrm{in}(0) = 0$ festgelegt. Weiter definieren wir für ein Ideal $I \subset A$ das *initiale Ideal*

$$\mathrm{in}(I) = (\mathrm{in}(f) \mid f \in I) \subset A.$$

Definition 2.9. Es sei $I \subset k[x_1, \ldots, x_n]$ ein Ideal. Polynome $f_1, \ldots, f_r \in I$ bilden eine *Macaulay-Basis von I*, wenn das Ideal $\mathrm{in}(I)$ von den Elementen $\mathrm{in}(f_1), \ldots, \mathrm{in}(f_r)$ erzeugt wird.

Ist ein Erzeugendensystem eines Ideals zugleich eine Macaulay-Basis, so kann nach [25], Proposition 6.6, das Ideal der strikten Transformation bzgl. Blow-up einfach ermittelt werden:

Proposition 2.10. *Es sei ein Ideal $I = (f_1, \ldots, f_r) \subset k[x_1, \ldots, x_n]$ gegeben, sodass die Erzeuger f_i eine Macaulay-Basis bilden. Die strikte Transformation I^{str} von I bzgl. eines Blow-ups in einem regulären Zentrum wird in den affinen Karten von den Elementen $f_1^{\mathrm{str}}, \ldots, f_r^{\mathrm{str}}$ erzeugt.*

Im Allgemeinen ist es aufwendig, für ein beliebiges Erzeugendensystem eines Ideals zu überprüfen, ob es sich um eine Macaulay-Basis handelt. Wenn das Erzeugendensystem aus homogenen Polynomen besteht, ist die Eigenschaft leicht einzusehen. Wir benutzen die bekannte Charakterisierung von homogenen Idealen in graduierten Ringen (siehe z. B. [21], S. 367):

Lemma 2.11. *Es seien A ein graduierter Ring und $\mathfrak{a} \subset A$ ein Ideal. Äquivalent sind:*

(i) Das Ideal $\mathfrak{a}$ kann von homogenen Elementen erzeugt werden.

(ii) Ist $f \in \mathfrak{a}$, dann sind auch die homogenen Komponenten von f in $\mathfrak{a}$ enthalten.

Hiermit folgt nun leicht der Nachweis einer Macaulay-Basis bei homogenen Idealen:

Lemma 2.12. *Es sei $I \subset k[x_1, \ldots, x_n]$ ein homogenes Ideal, also $I = (f_1, \ldots, f_r)$ für homogene Polynome f_i. Dann bilden $f_1, \ldots, f_r$ eine Macaulay-Basis von I.*

Beweis. Es sei $f \in I$. Da I homogen ist, sind auch alle homogenen Komponenten von f enthalten, insbesondere gilt daher $\mathrm{in}(f) \in I$ und folglich $\mathrm{in}(I) \subset I$. Andererseits gilt $f_i = \mathrm{in}(f_i)$ und es ergibt sich die umgekehrte Inklusion $I \subset \mathrm{in}(I)$. □

Die Erzeuger des Ideals J_1 bilden also eine Macaulay-Basis, sodass deren strikte Transformationen ein Erzeugendensystem von J_1^{str} bilden. Zunächst werden die offenen Unterschemata $V_{\{m\}}$ aus (2.5) untersucht: Wegen der Relation

$$\frac{a_{\{i,j\}}}{a_{\{m\}}} = \frac{a_{\{m,i\}}}{a_{\{m\}}} \cdot \frac{a_{\{m,j\}}}{a_{\{m\}}},$$

in $\Gamma(V_{\{m\}}, \mathscr{O}_{V_{\{m\}}})$, die aus der strikten Transformation von $a_{\{i,j\}}a_{\{m\}} - a_{\{m,i\}}a_{\{m,j\}} \in J_1$ hervorgeht, werden im Koordinatenring von $V_{\{m\}}$ nur die Elemente $a_{\{m\}}$ und $a_{\{m,i\}}/a_{\{m\}}$ mit $i \neq m$ als Erzeuger benötigt. Zwischen diesen Elementen gibt es keine Relationen: Dazu fassen wir R_1 als Unterring $R_1 \cong k\,[u_i u_j,\ 1 \leq i, j \leq g]$ auf. Angenommen, es gäbe ein Polynom f in g Unbestimmten mit $f(u_m^2, u_1/u_m, \ldots, u_g/u_m) = 0$. Nach Multiplikation mit u_m^{2N} für N groß genug ist

$$0 = (u_m^2)^N \cdot f(u_m^2, \frac{u_1}{u_m}, \ldots, \frac{u_g}{u_m}) = P(u_1, \ldots, u_g) \tag{2.6}$$

für ein Polynom P in g Unbestimmten über k. Da die u_i algebraisch unabhängig sind, ist P das Nullpolynom und damit ebenso f. Es gilt somit

$$\Gamma\left(V_{\{m\}}, \mathscr{O}_{V_{\{m\}}}\right) = k\left[a_{\{m\}}, \frac{a_{\{1,m\}}}{a_{\{m\}}}, \ldots, \frac{a_{\{g,m\}}}{a_{\{m\}}}\right]$$

und hieran wird ersichtlich, dass $V_{\{m\}}$ regulär ist. Der exzeptionelle Divisor E ist in $V_{\{m\}}$

durch die Gleichung $a_{\{m\}} = 0$ gegeben, entsprechend ergibt sich

$$\begin{aligned} E \cap V_{\{m\}} &= \operatorname{Spec}\left(k\left[\frac{a_{\{1,m\}}}{a_{\{m\}}}, \ldots, \frac{a_{\{g,m\}}}{a_{\{m\}}}\right]\right) \\ &= \operatorname{Spec}\left(k\left[\frac{u_1}{u_m}, \ldots, \frac{u_g}{u_m}\right]\right) \cong \mathbb{A}_k^{g-1}. \end{aligned}$$

Nun liegt eine Standardsituation vor, bei der sich die g Kopien von $\mathbb{A}_k^{g-1}$ aus $V_{\{1\}}, \ldots, V_{\{g\}}$ zu einem projektiven Raum $\mathbb{P}_k^{g-1}$ verkleben lassen.

Für die offenen affinen Teilmengen $V_{\{l,m\}}$ mit $l \neq m$ ist eine ähnliche Analyse möglich: Wegen der Relation

$$\frac{a_{\{i,j\}}}{a_{\{l,m\}}} = \frac{a_{\{i,m\}}}{a_{\{l,m\}}} \cdot \frac{a_{\{j,m\}}}{a_{\{l,m\}}} \cdot \frac{a_{\{l\}}}{a_{\{l,m\}}},$$

welche als strikte Transformation von

$$a_{\{l,m\}}\left(a_{\{i,j\}}a_{\{l,m\}} - a_{\{i,m\}}a_{\{j,l\}}\right) + a_{\{i,m\}}\left(a_{\{l,m\}}a_{\{j,l\}} - a_{\{j,m\}}a_{\{l\}}\right) \in J_1$$

entsteht, bilden die Elemente der Form $a_{\{j,m\}}/a_{\{l,m\}}$ mit $j \neq l$ zusammen mit $a_{\{l\}}/a_{\{l,m\}}$ ein Erzeugendensystem der k-Algebra $\Gamma(V_{\{l,m\}}, \mathscr{O}_{V_{\{l,m\}}})$. Zwischen diesen Erzeugern gilt die Relation

$$\frac{a_{\{m\}}}{a_{\{l,m\}}} \cdot \frac{a_{\{l\}}}{a_{\{l,m\}}} = 1,$$

außer dieser Relation bestehen jedoch keine weiteren Relationen zwischen den Erzeugern, analog zum Argument in (2.6). Es ergibt sich also

$$\Gamma(V_{\{l,m\}}, \mathscr{O}_{V_{\{l,m\}}}) = k\left[a_{\{l,m\}}, \frac{a_{\{1,m\}}}{a_{\{l,m\}}}, \ldots, \frac{a_{\{g,m\}}}{a_{\{l,m\}}}, \left(\frac{a_{\{m\}}}{a_{\{l,m\}}}\right)^{-1}\right]$$

und folglich ist $V_{\{l,m\}}$ regulär. Der exzeptionelle Divisor ist in $V_{\{l,m\}}$ durch die Gleichung $a_{\{l,m\}} = 0$ gegeben, also gilt

$$E \cap V_{\{l,m\}} = \operatorname{Spec}\left(k\left[\frac{a_{\{1,m\}}}{a_{\{l,m\}}}, \ldots, \frac{a_{\{g,m\}}}{a_{\{l,m\}}}, \left(\frac{a_{\{m\}}}{a_{\{l,m\}}}\right)^{-1}\right]\right),$$

was einer offenen Teilmenge des affinen Raums $\mathbb{A}_k^{g-1}$ entspricht. Diese wird mit dem offenen Unterschema $D(a_{\{l,m\}}/a_{\{m\}})$ von $E \cap V_{\{m\}}$ identifiziert via

$$\frac{a_{\{i,m\}}}{a_{\{m\}}} = \frac{a_{\{i,m\}}}{a_{\{l,m\}}} \cdot \left(\frac{a_{\{m\}}}{a_{\{l,m\}}}\right)^{-1},$$

die offenen Unterschemata der Form $V_{\{l,m\}}$ tragen daher keine neue Information über den exzeptionellen Divisor bei.

Insgesamt ist nun gezeigt, dass durch ein Blow-up des singulären Punktes von $\mathrm{Spec}(R_1)$ bereits eine Auflösung der Singularität erhalten wird und der exzeptionelle Divisor isomorph zu einem projektiven Raum $\mathbb{P}_k^{g-1}$ ist. Wir können das Ergebnis direkt auf Kummer-Varietäten anwenden:

Proposition 2.13. *Es sei k zusätzlich algebraisch abgeschlossen. Jede Kummer-Varietät $X = A/\iota$ besitzt für $g \geq 2$ genau 2^{2g} singuläre Punkte, die durch ein Blow-up mit dem singulären Ort als Zentrum aufgelöst werden können. Der exzeptionelle Divisor besteht dabei aus 2^{2g} disjunkten projektiven Räumen $\mathbb{P}_k^{g-1}$.*

Wir wollen nun auch die Selbstschnittzahl für die Komponenten des exzeptionellen Divisors bestimmen.

Proposition 2.14. *Es gelten die Voraussetzungen aus Proposition 2.13. Für jede Komponente E des exzeptionellen Divisors ist die Selbstschnittzahl $(E^g) = (-2)^{g-1}$.*

Beweis. Es bezeichne $\tilde{X}$ das Blow-up der Kummer-Varietät $X = A/\iota$ mit dem singulären Ort als Zentrum und $f\colon E \to \tilde{X}$ die abgeschlossene Einbettung. Wir fassen die Selbstschnittzahl (E^g) als Selbstschnittzahl der assoziierten Garbe $(\mathscr{O}_{\tilde{X}}(E)^g)$ auf. Die Idealgarbe von E ist durch $\mathscr{O}_{\tilde{X}}(-E)$ gegeben, sodass wir eine kurze exakte Sequenz der Form

$$0 \longrightarrow \mathscr{O}_{\tilde{X}}(-E) \longrightarrow \mathscr{O}_{\tilde{X}} \longrightarrow \mathscr{O}_E \longrightarrow 0$$

erhalten. Nach Tensorieren mit der invertierbaren Garbe $\mathscr{O}_{\tilde{X}}(E)$ ergibt sich hieraus die exakte Sequenz

$$0 \longrightarrow \mathscr{O}_{\tilde{X}} \longrightarrow \mathscr{O}_{\tilde{X}}(E) \longrightarrow \mathscr{O}_E(E) \longrightarrow 0$$

und es gilt $\mathscr{O}_E(E) = \mathscr{O}_E \otimes \mathscr{O}_{\tilde{X}}(E) \cong f^*(\mathscr{O}_{\tilde{X}}(E))$. Nach [3], Lemma 1.9 und 1.10, gilt nun

$$\left(\mathscr{O}_{\tilde{X}}(E)^{g-1} \cdot \mathscr{O}_{\tilde{X}}(E)\right)_{\tilde{X}} = \left(\mathscr{O}_{\tilde{X}}(E)^{g-2} \cdot \mathscr{O}_E(E)\right)_{\tilde{X}} = \left(\mathscr{O}_E(E)^{g-1}\right)_E,$$

wobei die Indizes $\tilde{X}$ bzw. E anzeigen, auf welchem Schema die Schnittzahl betrachtet wird. Da $E \cong \mathbb{P}_k^{g-1}$, ist die invertierbare Garbe $\mathscr{O}_E(E)$ isomorph zu einer Garbe der Form $\mathscr{O}_{\mathbb{P}_k^{g-1}}(n)$ für ein $n \in \mathbb{Z}$. Da die Schnittform multilinear ist, folgt

$$(\mathscr{O}_{\mathbb{P}_k^{g-1}}(n)^{g-1}) = n^{g-1}(\mathscr{O}_{\mathbb{P}_k^{g-1}}(1)^{g-1}) = n^{g-1},$$

da sich $g-1$ Hyperebenen in allgemeiner Lage in $\mathbb{P}_k^{g-1}$ in einem Punkt schneiden. Es bleibt also zu zeigen, dass $\mathscr{O}_E(E)$ isomorph zu $\mathscr{O}_{\mathbb{P}_k^{g-1}}(-2)$ ist.

Wie bei der Berechnung der Auflösung der Singularität oben können wir X durch $\mathrm{Spec}(R_1)$ und E durch den exzeptionellen Divisor des Blow-ups im singulären Punkt ersetzen. Das Blow-up wird von den offenen affinen Teilmengen der Form $V_{\{l,m\}}$ überdeckt und

E ist in $V_{\{l,m\}}$ durch die Gleichung $a_{\{l,m\}} = 0$ gegeben. Wir können dies auch formulieren als $\mathscr{O}_{\tilde{X}}(E)|_{V_{\{l,m\}}} = a_{\{l,m\}}^{-1}\mathscr{O}_{V_{\{l,m\}}}$. Es sei $n \in \{1, \ldots, g\}$ fest gewählt. Wir betrachten den zu $\mathscr{O}_{\tilde{X}}(E)$ isomorphen $\mathscr{O}_{\tilde{X}}$-Modul $\mathscr{L} = a_{\{n\}}\mathscr{O}_{\tilde{X}}(E)$. Wir haben somit

$$\mathscr{L}|_{V_{\{n\}}} \cong \mathscr{O}_{V_{\{n\}}}, \qquad \mathscr{L}|_{V_{\{m,n\}}} \cong \mathscr{O}_{V_{\{m,n\}}},$$

da $a_{\{n\}} \cdot a_{\{n,m\}}^{-1}$ invertierbar im Koordinatenring von $V_{\{m,n\}}$ ist. Für $l, m \neq n$ ergibt sich

$$\mathscr{L}|_{V_{\{l,m\}}} \cong a_{\{n\}}a_{\{l,m\}}^{-1}\mathscr{O}_{V_{\{l,m\}}} \cong \left(\frac{a_{\{l,n\}}}{a_{\{l,m\}}} \cdot \frac{a_{\{m,n\}}}{a_{\{l,m\}}}\right)\mathscr{O}_{V_{\{l,m\}}},$$

wobei der Fall $l = m$ erlaubt ist. Damit ist $\mathscr{L}|_{V_{\{l,m\}}}^{-1}$ durch ein quadratisches Polynom im Koordinatenring von $E \cap V_{\{l,m\}}$ gegeben. Hieraus folgt $f^*(\mathscr{L}) \cong \mathscr{O}_{\mathbb{P}_k^{g-1}}(-2)$. □

Die Selbstschnittzahl kann nach [46], S. 63, auch aus der Multiplizität des zugehörigen singulären Punktes abgelesen werden:

Proposition 2.15 (Ramanujam)**.** *Es seien X ein g-dimensionales integres, projektives k-Schema, $x \in X$ ein Punkt und $I \subset \mathscr{O}_{X,x}$ ein Ideal, das primär für das maximale Ideal ist. Weiter seien $f\colon \tilde{X} \to X$ ein eigentlicher birationaler Morphismus, $\tilde{X}$ regulär und integer, sodass $I\mathscr{O}_{\tilde{X}}$ eine invertierbare Idealgarbe auf $\tilde{X}$ und einen effektiven Divisor D definiert. Für die Selbstschnittzahl von D gilt dann*

$$(D^g) = (-1)^{g-1}\,\mu\,(I, \mathscr{O}_{X,x})\,,$$

wobei $\mu\,(I, \mathscr{O}_{X,x})$ die Multiplizität des Ideals im lokalen Ring bezeichnet.

Für $X = A/\iota$, x ein singulärer Punkt, $I = \mathfrak{m}$ und $f\colon \tilde{X} \to X$ das Blow-up von X mit dem singulären Ort als Zentrum sind die Voraussetzungen der Proposition erfüllt. Nach Proposition 2.7 beträgt die Multiplizität des maximalen Ideals 2^{g-1}. Folglich ist $(E^g) = (-2)^{g-1}$ für $g \geq 2$.

2.2 Die Kummer-Konfiguration

Es sei hier $k = \mathbb{C}$ der Körper der komplexen Zahlen. Es ist ein klassisches Resultat, dass die Kummer-Flächen von abelschen Flächen, die eine irreduzible Prinzipalpolarisation besitzen, in den projektiven Raum $\mathbb{P}_k^3$ eingebettet werden können. Dort existieren zu den 16 singulären Punkten der Kummer-Fläche 16 Ebenen, sodass jeder der Punkte auf sechs der Ebenen liegt und jede der Ebenen sechs singuläre Punkte der Kummer-Fläche enthält. Dieses Resultat soll hier für höhere Dimension verallgemeinert werden. Die Existenz der allgemeineren $(4^g, 2^{g-1}(2^g - 1))$-Konfiguration ist wohlbekannt (siehe

z. B. [13], Abs. 10.3), ein Beweis ist in der Fachliteratur jedoch nicht auffindbar. Neben einer ausführlicheren Beweisskizze wird in diesem Abschnitt ebenso die von Kummer-Flächen bekannte Inzidenz-Relation verallgemeinert und aus dieser ein Resultat über die Lage von Paaren von singulären Punkten hergeleitet.

Definition 2.16. Es bezeichne A eine abelsche Varietät. Die *duale abelsche Varietät* A^* zu A ist die Zusammenhangskomponente des neutralen Elements $\mathrm{Pic}^0_{A/\mathbb{C}}$ des Picard-Schemas $\mathrm{Pic}_{A/\mathbb{C}}$. Eine *Polarisation* ist eine Isogenie $\phi_{\mathscr{L}}\colon A \to A^*$ der Form $\phi_{\mathscr{L}}(x) = t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ für eine invertierbare Garbe $\mathscr{L}$. Wenn $\phi_{\mathscr{L}}$ ein Isomorphismus ist, spricht man von einer *Prinzipalpolarisation.*

Das Picard-Schema $\mathrm{Pic}_{A/\mathbb{C}}$ existiert nach [33], Theorem 9.4.8. Dass $\mathrm{Pic}^0_{A/\mathbb{C}}$ auch tatsächlich eine abelsche Varietät ist, ergibt sich aus [33], Proposition 9.5.3 (irreduzibel), Theorem 9.5.4 (projektiv) und Corollary 9.5.14 (reduziert). Zu den abelschen Varietäten, die mit einer Prinzipalpolarisation ausgestattet werden können, zählen die Jacobi-Varietäten $J(C)$ von glatten Kurven C ([41], Thm. 6.6). Nicht jede abelsche Varietät kann mit einer Prinzipalpolarisation versehen werden.

Definition 2.17. Es seien a, b zwei natürliche Zahlen und M, N zwei Mengen der Kardinalität a. Eine (a,b)*-Konfiguration* ist eine Relation $\mathcal{R} \subset M \times N$, sodass jedes $m \in M$ mit genau b Elementen von N und jedes $n \in N$ mit genau b Elementen von M in Relation steht.

Jede (a,b)-Konfiguration kann als $(a \times a)$-Matrix verdeutlicht werden: Nach Wahl von Aufzählungen der Elemente $m_1, \ldots, m_a \in M$ und $n_1, \ldots, n_a \in N$ definieren wir

$$\alpha_{ij} = \begin{cases} 1, & \text{wenn } m_i \sim n_j, \\ 0, & \text{wenn } m_i \nsim n_j. \end{cases}$$

Die Matrix (α_{ij}) wird auch als *Inzidenz-Matrix* bezeichnet.

Es sei A eine g-dimensionale abelsche Varietät, versehen mit einer Prinzipalpolarisation, die durch einen symmetrischen irreduziblen Divisor D bzw. die Garbe $\mathscr{L} = \mathscr{O}_A(D)$ gegeben ist. Nach [4], Theorem 4.8.1, ist $h^0(A, \mathscr{L}^2) = 2^g$ und $\mathscr{L}^2$ basispunktfrei, sodass durch $\mathscr{L}^2$ ein Morphismus $A \to \mathbb{P}^{2^g-1}_{\mathbb{C}}$ erhalten wird. Dieser faktorisiert durch den Quotienten $A \to A/\iota$, gefolgt von einer abgeschlossenen Einbettung $A/\iota \to \mathbb{P}^{2^g-1}_{\mathbb{C}}$.

Die Kummer-Fläche kann so also in $\mathbb{P}^3_{\mathbb{C}}$ eingebettet werden. Das folgende Theorem beschreibt die klassische $(16,6)$-Konfiguration (für einen Beweis siehe z. B. [20], Cor. 2.18 und Prop. 4.23):

Theorem 2.18. *Es existieren 16 Ebenen in* $\mathbb{P}^3_{\mathbb{C}}$*, die zusammen mit den 16 Bildern der singulären Punkte in* $\mathbb{P}^3_{\mathbb{C}}$ *bzgl. der Relation „*$\in$*“ eine* $(16,6)$*-Konfiguration bilden.*

Indem wir die Ebenen durch ihre Schnitte mit der Kummer-Fläche ersetzen, erhalten wir eine $(16,6)$-Konfiguration bestehend aus den singulären Punkten und Divisoren auf A/ι. Diese Sichtweise hat den Vorteil, dass die Konfiguration direkt auf der Kummer-Varietät betrachtet werden kann.

Die Besonderheit der oben beschriebenen $(16,6)$-Konfiguration besteht darin, dass es eine weitere Möglichkeit gibt, die Inzidenz-Relation zu verdeutlichen: Die 16 singulären Punkte und Ebenen können derart mit den Einträgen einer (4×4)-Matrix identifiziert werden, dass jeder Punkt (bzw. jede Ebene) a_{ij} mit den sechs Ebenen (bzw. Punkten) in Relation steht, die in der gleichen Zeile oder Spalte wie a_{ij} stehen, wobei a_{ij} selbst ausgenommen ist. In der folgenden Darstellung sind exemplarisch die Einträge, die mit einem ausgewählten Eintrag „$*$“ in Relation stehen, mit einem „$\circ$“ markiert:

$$\begin{pmatrix} * & \circ & \circ & \circ \\ \circ & \cdot & \cdot & \cdot \\ \circ & \cdot & \cdot & \cdot \\ \circ & \cdot & \cdot & \cdot \end{pmatrix} \qquad \begin{pmatrix} \cdot & \cdot & \circ & \cdot \\ \circ & \circ & * & \circ \\ \cdot & \cdot & \circ & \cdot \\ \cdot & \cdot & \circ & \cdot \end{pmatrix}$$

Diese Veranschaulichung wird auch als *Inzidenz-Diagramm* bezeichnet. Sie wurde bereits zu Beginn des 20. Jahrhunderts von Hudson erwähnt (siehe [30], §5). Um das Inzidenz-Diagramm zu verallgemeinern, betrachten wir das quadratische Tableau als die Menge $M = \{0,1,2,3\}^2$. Zwei Tupel $(a_1,a_2),(b_1,b_2) \in M$ stehen genau dann in Relation zueinander, wenn sie in genau einem Eintrag übereinstimmen.

Die Relation lässt sich in natürlicher Weise für g-Tupel verallgemeinern:

Definition 2.19. Es seien g eine natürliche Zahl und $M = \{0,1,2,3\}^g$. Die *verallgemeinerte Inzidenzrelation* auf M ist wie folgt definiert: Zwei Tupel $a, b \in M$ stehen genau dann in Relation zueinander, wenn ihre Einträge an einer ungeraden Anzahl an Positionen übereinstimmen.

Lemma 2.20. *Es sei $a = (a_1, \ldots, a_g) \in M$ ein fest gewähltes Element. Es existieren genau $2^{g-1}(2^g - 1)$ Tupel in M, deren Einträge mit denen von a an einer ungeraden Anzahl an Positionen übereinstimmen.*

Beweis. Es existieren $\binom{g}{i}3^{g-i}$ mögliche Tupel $b \in M$, die mit dem gegebenen a an genau i Positionen übereinstimmen: Für die $g - i$ verschiedenen Einträge gibt es jeweils drei Möglichkeiten und es gibt $\binom{g}{i}$ Möglichkeiten, an welchen i Positionen die Einträge übereinstimmen. Es ist also die Gleichheit

$$\sum_{\substack{i=1,\ldots,g \\ i \text{ ungerade}}} \binom{g}{i} 3^{g-i} = 2^{g-1}(2^g - 1)$$

zu zeigen. Dies kann direkt durch Umformen der linken Seite gezeigt werden:

$$\begin{aligned}\sum_{\substack{i=1,\dots,g\\ i \text{ ungerade}}} \binom{g}{i} 3^{g-i} &= \sum_{i=0}^{g} \binom{g}{i} 3^{g-i} \cdot \frac{1-(-1)^i}{2} \\ &= \frac{1}{2} \cdot \left(\sum_{i=0}^{g} \binom{g}{i} 3^{g-i} - \sum_{i=0}^{g} \binom{g}{i} (-1)^i 3^{g-i} \right) \\ &= \frac{1}{2} \cdot ((1+3)^g - (3-1)^g) = \frac{2^g}{2}(2^g - 1) = 2^{g-1}(2^g - 1).\end{aligned}$$

□

Definition 2.21. Eine $(4^g, 2^{g-1}(2^g - 1))$-Konfiguration, die über die verallgemeinerte Inzidenzrelation beschrieben werden kann, heißt *Konfiguration vom Typ* $(^*)$.

Die Namensgebung ist angelehnt an Definition 1.9 in [20]. Für Kummer-Varietäten X der Dimension $g \leq 1$ existiert trivialerweise eine Konfiguration vom Typ $(^*)$, bestehend aus den Bildern der 2-Torsionspunkte und bestimmten Unterschemata: Ist $X = \{0\}$ nulldimensional, dann existiert lediglich ein Unterschema in Kodimension 1, nämlich das leere Schema. Der eindeutige Punkt von X ist nicht darin enthalten und umgekehrt enthält das leere Schema den Punkt nicht. Es liegt also eine $(1,0)$-Konfiguration vor. Im Fall, dass $X = \mathbb{P}^1_k$ die Kummer-Varietät einer elliptischen Kurve E ist, bezeichne x_1, x_2, x_3, x_4 die Bilder der 2-Torsionspunkte von E in X. Die Teilmengen $\{x_i\}$ für $1 \leq i \leq 4$, aufgefasst als reduzierte abgeschlossene Unterschemata, dienen als ausgezeichnete Divisoren. Offensichtlich ist x_i genau in $\{x_i\}$ enthalten, wir haben folglich eine $(4,1)$-Konfiguration. Abbildung 4 zeigt zu den Konfigurationen die verallgemeinerte Inzidenzrelation. Jedes der Felder entspricht einem Punkt bzw. einem der ausgezeichneten Divisoren, grau schattiert sind die Felder, die in Relation mit dem „X“-markierten Feld stehen.

Um zu zeigen, dass auch für Kummer-Varietäten A/ι der Dimension $g \geq 3$ eine Konfiguration vom Typ $(^*)$ existiert, brauchen wir die Bedingung, dass es einen symmetrischen irreduziblen Divisor D auf A gibt, der eine Prinzipalpolarisation definiert. Davon ausgehend können wir den Beweis für Kummer-Flächen in [4], Proposition 10.2.5 und Corollary 10.2.6, adaptieren. Dazu rekapitulieren wir zunächst einige Resultate über komplexe abelsche Varietäten.

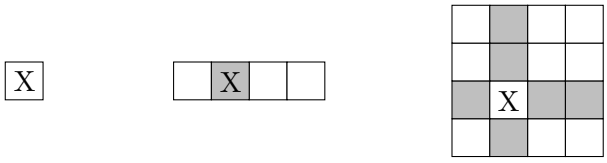


Abbildung 4: Kummer-Konfigurationen: $(1,0)$, $(4,1)$ und $(16,6)$

Jede g-dimensionale komplexe abelsche Varietät kann als komplexer Torus $\mathbb{C}^g/\Lambda$ aufgefasst werden für ein Gitter $\Lambda \subset \mathbb{C}^g$. Ein Gitter ist dabei definiert als diskrete Untergruppe, die isomorph zu $\mathbb{Z}^{\oplus 2g}$ ist. Nach dem *Appell–Humbert-Theorem* ([42], S. 20/21) kann jedes Element $\mathscr{L} \in \mathrm{Pic}(A)$ als ein Paar (H, χ) aufgefasst werden, bestehend aus einer Hermiteschen Form $\mathrm{H}\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ und einer Abbildung $\chi\colon \Lambda \to S^1 \subset \mathbb{C}$, die die folgenden Bedingungen erfüllen: Für die Imaginärteile $E(v,w) = \operatorname{Im} \mathrm{H}(v,w)$ gilt $E(\Lambda,\Lambda) \subset \mathbb{Z}$ und χ erfüllt für alle $\lambda, \mu \in \Lambda$ die Gleichung

$$\chi(\lambda+\mu) = \chi(\lambda)\,\chi(\mu)\exp(\pi i\, E(\lambda,\mu)). \tag{2.7}$$

Insbesondere kann eine Polarisation von A, welche durch eine invertierbare Garbe $\mathscr{L}$ repräsentiert wird, als solches Paar angesehen werden. Beschreibt $\mathscr{L}$ eine Prinzipalpolarisation, dann existiert eine $\mathbb{Z}$-Basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ von Λ, sodass E durch die symplektische Matrix

$$M = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \tag{2.8}$$

gegeben ist, wobei I_g die Einheitsmatrix in $\mathrm{GL}_g(\mathbb{C})$ bezeichnet (siehe [4], S.46). Jeder 2-Torsionspunkt von A ist nun die Restklasse eines Vektors der Form

$$v = \frac{1}{2}\sum_{i=1}^{g} a_i'\lambda_i + a_i''\mu_i$$

mit $a_i', a_i'' \in \{0,1\}$. Wir können a_i', a_i'' auch als Elemente von $\mathbb{F}_2$ ansehen, da $\bar{v}$ nur von der Parität der Koeffizienten abhängt. Es bezeichne $e_i' = \overline{\frac{1}{2}\lambda_i}$, $e_i'' = \overline{\frac{1}{2}\mu_i}$ die Restklassen. Indem wir die Koeffizienten a_i', a_i'' als Koordinaten bzgl. der Basis $(e_i', e_i'', 1 \le i \le g)$ ansehen, können wir die 2-Torsionspunkte von A mit den Elementen des Vektorraums $\left(\mathbb{F}_2^2\right)^g = \{(a_1, \ldots, a_g) \mid a_i = (a_i', a_i'') \in \mathbb{F}_2^2\}$ identifizieren.

Aus der Form der Matrix M ist ersichtlich, dass sich $\mathbb{C}^g$ in die reellen Untervektorräume $V_1 = \langle \lambda_1, \ldots, \lambda_g \rangle$ und $V_2 = \langle \mu_1, \ldots, \mu_g \rangle$ zerlegen lässt, sodass $E(v_i, v_i) = 0$ für alle Vektoren $v_i \in V_i$ gilt. Wir schreiben $v = v_1 + v_2$ mit $v_i \in V_i$. Die durch $\chi_0(v) = \exp(\pi i\, E(v_1, v_2))$ definierte Abbildung $\chi_0\colon \mathbb{C}^g \to S^1$ erfüllt die Bedingung (2.7) und nach dem Appell–Humbert-Theorem existiert eine invertierbare Garbe $\mathscr{L}_0 \in \mathrm{Pic}(A)$, die dem Paar (H, χ_0) entspricht. Weiter gilt nach [4], Lemma 3.1.2, dass sich $\mathscr{L}$ und $\mathscr{L}_0$ lediglich um eine Translation unterscheiden, also dass $\mathscr{L}_0 \cong t_c^*\mathscr{L}$ gilt.

Es sei nun $\mathscr{L}$ eine symmetrische, ample Garbe auf A, die eine Prinzipalpolarisation definiert und die die assoziierte Garbe eines irreduziblen Divisors D' ist. Es sei $\mathscr{L}_0$ wie oben und es bezeichne $D = t_c^* D'$ den translatierten Divisor, zu dem $\mathscr{L}_0$ assoziierte Garbe ist. Ohne Einschränkung können wir annehmen, dass $\mathscr{L} = t^*_{e_1'+e_1''+\ldots+e_g'+e_g''}\mathscr{L}_0$ gilt (siehe

[4], Lemma 4.6.1). Für jeden 2-Torsionspunkt x von A sei $D_x = t^*_{x+e'_1+e''_1+\ldots+e'_g+e''_g} D$ sowie $H_{p(x)} = p(D_x)$ das Bild der Quotientenabbildung $p\colon A \to A/\iota$.

Proposition 2.22. *Es seien $y_1 = p(x_1), y_2 = p(x_2)$ zwei singuläre Punkte der Kummer-Varietät A/ι. Wir identifizieren $x_1 = (a_1, \ldots, a_g)$, $x_2 = (b_1, \ldots, b_g) \in (\mathbb{F}_2^2)^g$. Die folgenden beiden Aussagen sind äquivalent:*

(i) Der Punkt y_1 liegt auf H_{y_2}.

(ii) Für eine ungerade Anzahl an Indizes i gilt $a_i = b_i$.

Beweis. Es reicht zu zeigen, dass die Aussage für den Punkt $y_1 = p(0)$ gilt, da die Translation um einen singulären Punkt sowohl die Menge der singulären Punkte als auch die der Divisoren H_y in sich selbst überführt. Die Aussage (i) ist genau dann erfüllt, wenn $0 \in D_{x_2}$ gilt. Nach Definition von D_{x_2} heißt das, dass der 2-Torsionspunkt $0+x_2+e'_1+e''_1+\ldots+e'_g+e''_g$ auf D liegt. Wir können $x_2 = \sum(a'_i e'_i + a''_i e''_i)$ schreiben. Nach [4], Proposition 4.7.2, gilt für jeden 2-Torsionspunkt $x = \frac{1}{2}\lambda \in A$ die Gleichung

$$(-1)^{\mathrm{mult}_x(D)} = (-1)^{\mathrm{mult}_0(D)} \chi_0(\lambda), \tag{2.9}$$

also insbesondere für den Punkt

$$0 + x_2 + e'_1 + e''_1 + \ldots + e'_g + e''_g = \sum_{i=1}^{g} \overline{\frac{1}{2}\left((a'_i+1)\lambda_i + (a''_i+1)\mu_i\right)}.$$

Wenn D an x lokal durch $f \in \mathscr{O}_{A,x}$ gegeben ist, kann die Multiplizität $\mathrm{mult}_x(D)$ als höchster Exponent n definiert werden, sodass $f \in \mathfrak{m}_x^n$ gilt. Es ist bekannt, dass die Multiplizität $\mathrm{mult}_x(D)$ für einen 2-Torsionspunkt $x \in D$ stets ungerade ist (siehe [13], Abs. 10.3). Ebenso ist bekannt, dass $\mathrm{mult}_0(D)$ eine gerade Zahl ist, da die Theta-Funktion von $\mathscr{L}_0$ eine gerade Funktion ist ([4], Lemma 3.2.4 und Bemerkung auf S. 93). Die Gleichung (2.9) liefert daher das folgende Kriterium: Der Punkt $x_1 = 0$ liegt genau dann auf D_{x_2}, wenn die Bedingung

$$-1 = \exp\left(\pi\, i \left\langle \begin{pmatrix} 1+a'_1 \\ \ldots \\ 1+a'_g \end{pmatrix}, \begin{pmatrix} 1+a''_1 \\ \ldots \\ 1+a''_g \end{pmatrix} \right\rangle\right)$$

erfüllt ist. Dabei bezeichnet $\langle\ .\ ,\ .\ \rangle$ das Standardskalarprodukt auf $\mathbb{F}_2^g$, denn die Form E aus der Definition von χ_0 ist durch die Matrix M wie in (2.8) gegeben. Das Skalarprodukt besitzt den Wert

$$g + \sum_{i=1}^{g}(a'_i + a''_i) + \sum_{i=1}^{g} a'_i a''_i \in \mathbb{F}_2. \tag{2.10}$$

Es bezeichne l_1 die Anzahl der Vektoren $a_i = (a_i', a_i'') \in \mathbb{F}_2^2$, die genau einen von Null verschiedenen Eintrag besitzen, und l_2 die Anzahl der a_i mit $a_i = (0,0)$. In diesem Fall wird (2.10) zu

$$g + (2g - 2l_2 - l_1) + (g - l_1 - l_2) = 4g - 2l_1 - 3l_2$$

und dieser Wert ist genau dann $1 \in \mathbb{F}_2$, wenn l_2 ungerade ist, also wenn Bedingung (ii) der Proposition erfüllt ist. □

Korollar 2.23. *Es sei $g \geq 2$. Mit der Relation „$\in$“ bilden die singulären Punkte $y \in A/\iota$ und die Divisoren H_y eine $(4^g, 2^{g-1}(2^g - 1))$-Konfiguration vom Typ (*).*

Beweis. Aus der Proposition ist ersichtlich, dass die Rollen von Punkten und Divisoren vertauscht werden können. Wir identifizieren $\mathbb{F}_2^2$ mit $\{0,1,2,3\}$ und erhalten eine Konfiguration vom Typ (*). Nach Lemma 2.20 liegt jeder Punkt y_1 auf genau $2^{g-1}(2^g - 1)$ verschiedenen H_y. □

Für den Fall $g = 3$ ist die Inzidenzrelation der Kummer-Konfiguration in Abbildung 5 dargestellt. Übereinstimmung in einer ungeraden Anzahl an Einträgen bedeutet in diesem Fall, gemeinsam in einer oder drei Querschnittsebenen, nicht aber in genau zwei Querschnitten des Würfels zu liegen.

Die Zahl der Punkte, die auf einem Paar von Divisoren liegt, ist ebenfalls konstant:

Korollar 2.24. *Es sei $n = 2^{g-1}(2^{g-1} - 1)$. Jedes Paar von singulären Punkten liegt auf n Divisoren der Form H_y. Je zwei Divisoren der Form H_y haben genau n singuläre Punkte gemeinsam.*

Die Aussage ist auch für $g = 1$ richtig, wenn „singulärer Punkt“ durch „Bild eines 2-Torsionspunkts“ ersetzt wird. Für $g = 2$ erhält man die bekannte Aussage, dass je zwei Ebenen der Konfiguration genau zwei singuläre Punkte gemeinsam haben und je zwei singuläre Punkte im Schnitt von genau zwei der Ebenen liegen. Für $g = 3$ ist $n = 12$. Im Schnitt von drei Divisoren können unterschiedlich viele singuläre Punkte liegen, wie man bereits im zweidimensionalen Fall sehen kann.

Beweis. Wir beweisen die Aussage mit vollständiger Induktion und schließen den Fall $g = 1$ wie oben beschrieben mit ein. Da hier die vier Divisoren selbst die vier Punkte sind,

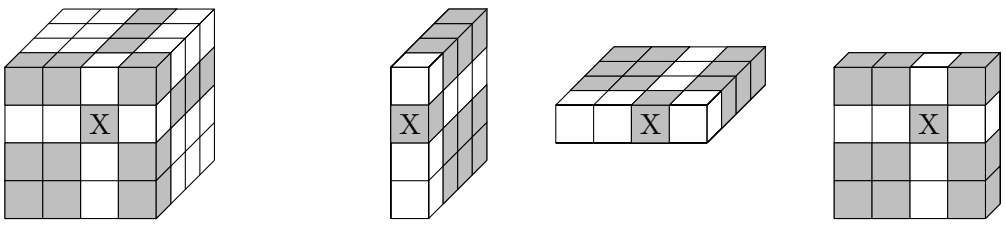


Abbildung 5: $(64, 28)$-Konfiguration, Darstellung mit Würfel-Querschnitten

kann im Schnitt zweier verschiedener Divisoren kein Punkt liegen, in Übereinstimmung mit der Behauptung.

Es sei nun $g \geq 2$ fest gewählt und wir nehmen an, dass die Aussage für $g-1$ stimmt. Wir identifizieren die singulären Punkte und die Divisoren mit $\{0,1,2,3\}^g$ und der verallgemeinerten Inzidenzrelation. Es seien $a = (a_1, \ldots, a_g)$ und $b = (b_1, \ldots, b_g)$ zwei Elemente. Es werden nun alle Tupel $c = (c_1, \ldots, c_g)$ gezählt, deren Einträge sowohl mit a als auch mit b an einer ungeraden Zahl an Positionen übereinstimmen. Wir definieren außerdem a', b' und c' als das $(g-1)$-Tupel, das man erhält, wenn man den ersten Eintrag weglässt.

1. Fall: $a_1 = b_1$. Es gibt drei mögliche Wahlen für c_1, sodass $c_1 \neq a_1$ gilt. Ist dies der Fall, dann muss die Inzidenzrelation durch die anderen $g-1$ Einträge erfüllt sein. Nach Induktionsvoraussetzung gibt es $2^{g-2}(2^{g-2}-1)$ solcher $(g-1)$-Tupel. Wenn $c_1 = a_1$ gilt, muss es eine gerade Anzahl an Übereinstimmungen zwischen c' und a' bzw. c' und b' geben. Diese Zahl ergibt sich, indem man von der Gesamtzahl 4^{g-1} die Zahl der Tupel abzieht, die mit a' bzw. b' an einer ungeraden Anzahl von Einträgen gleich sind, und die Zahl der Tupel wieder addiert, die mit a' und b' eine ungerade Anzahl an Übereinstimmungen haben, da diese sonst zweimal abgezogen wurde. Insgesamt erhält man

$$\begin{aligned} &3 \cdot 2^{g-2}(2^{g-2}-1) + \left(4^{g-1} - 2 \cdot 2^{g-2}(2^{g-1}-1) + 2^{g-2}(2^{g-2}-1)\right) \\ &= 3 \cdot 4^{g-2} - 3 \cdot 2^{g-2} + 4^{g-1} - 4^{g-1} + 2^{g-1} + 4^{g-2} - 2^{g-2} \\ &= 4 \cdot 4^{g-2} - 2 \cdot 2^{g-2} = 2^{g-1}(2^{g-1}-1) \end{aligned}$$

mögliche Tupel c, womit die Aussage in diesem Fall bewiesen ist.

2. Fall: $a_1 \neq b_1$. Wenn $c_1 \neq a_1$, $c_1 \neq b_1$ gilt, müssen c' und a' sowie c' und b' jeweils für eine ungerade Anzahl an Indizes die gleichen Einträge besitzen. Da es für c_1 dabei zwei verschiedene Möglichkeiten gibt, gibt es genau $2^{g-1}(2^{g-2}-1)$ solcher Tupel c. Wenn $c_1 = a_1$ gilt, muss c' mit b' in ungerader Anzahl, mit a' in gerader Anzahl der Einträge übereinstimmen. Die Bedingung kann auch so verstanden werden, dass es eine ungerade Anzahl von gleichen Einträgen bei c' und b', aber nicht gleichzeitig bei c' und a' gibt. Somit erhält man nach Induktionsvoraussetzung $2^{g-2}(2^{g-1}-1) - 2^{g-2}(2^{g-2}-1)$ geeignete Tupel. Die gleiche Zahl erhält man im Fall $c_1 = b_1$. Insgesamt gibt es also

$$2^{g-1}(2^{g-2}-1) + 2^{g-1}(2^{g-1}-1) - 2^{g-1}(2^{g-2}-1) = 2^{g-1}(2^{g-1}-1)$$

Möglichkeiten für c. □

Für Kummer-Flächen, eingebettet in $\mathbb{P}^3_{\mathbb{C}}$, gibt es noch eine weitere Interpretation des Inzidenzdiagramms, welche ausführlich in [20] behandelt wird, aber auch bereits 1905 in [30], §5, auftritt. Diese wird nun kurz zusammengefasst, um sie zumindest teilweise auf Kummer-Dreifaltigkeiten zu übertragen.

Durch die homogenen Koordinaten $(a_0 : a_1 : a_2 : a_3)$ werden nicht nur die Punkte in $\mathbb{P}^3_{\mathbb{C}}(\mathbb{C})$ beschrieben, sondern auch die Ebenen. Diese sind durch Gleichungen der Form $a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3$ festgelegt, die ebenfalls eindeutig bis auf Multiplikation mit Einheiten in $\mathbb{C}$ sind.

Wir betrachten die Automorphismen $\phi_A, \phi_B, \psi_A, \psi_B$ von $\mathbb{P}^3_{\mathbb{C}}$, die durch

$$\begin{aligned}
\phi_A((a_0 : a_1 : a_2 : a_3)) &= (a_3 : a_2 : a_1 : a_0), \quad & \psi_A((a_0 : a_1 : a_2 : a_3)) &= (-a_0 : a_1 : a_2 : -a_3) \\
\phi_B((a_0 : a_1 : a_2 : a_3)) &= (a_2 : a_3 : a_0 : a_1), \quad & \psi_B((a_0 : a_1 : a_2 : a_3)) &= (-a_0 : a_1 : -a_2 : a_3)
\end{aligned}$$

gegeben sind. Wir schreiben auch $\phi_A = (03)(12)$, $\phi_B = (02)(13)$ in Zykelschreibweise und $\psi_A = v_{03}$, $\psi_B = v_{02}$ für Vorzeichenwechsel an den im Index genannten Positionen. Die Untergruppe $G = \langle \phi_A, \phi_B, \psi_A, \psi_B \rangle \subset \mathrm{Aut}(\mathbb{P}^3_{\mathbb{C}})$ ist abelsch, da auf homogenen Koordinaten $v_{03} = v_{12}$ und $v_{02} = v_{13}$ gilt, und isomorph zu $(\mathbb{Z}/2\mathbb{Z})^4$. Wir definieren $\phi_C = \phi_A\phi_B$ und $\psi_C = \psi_A\psi_B$.

Es sei nun $P = (a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3_{\mathbb{C}}(\mathbb{C})$ ein fest gewählter Punkt, dessen G-Bahn aus 16 verschiedenen Punkten besteht und der die Bedingungen

$$\begin{aligned}
&a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0, \\
&a_i a_j \neq \pm a_k a_l, \\
&a_i^2 + a_j^2 \neq a_k^2 + a_l^2 \quad \text{für } \{i,j,k,l\} = \{0,1,2,3\}
\end{aligned} \tag{2.11}$$

erfüllt. Fassen wir P als Ebene auf, erhalten wir durch die G-Wirkung entsprechend 16 verschiedene Ebenen. Die Elemente von G können in der Form

1	$\phi_A\psi_B$	$\phi_B\psi_C$	$\phi_C\psi_A$
$\phi_A\psi_C$	ψ_A	ϕ_C	$\phi_B\psi_B$
$\phi_B\psi_A$	$\phi_C\psi_C$	ψ_B	ϕ_A
$\phi_C\psi_B$	ϕ_B	$\phi_A\psi_A$	ψ_C

angeordnet werden, wobei der Eintrag in Position (i, j) das Produkt der Elemente an den Positionen $(i, 1)$ und $(1, j)$ ist. Insbesondere ist G das direkte Produkt aus der ersten Zeile und der ersten Spalte des Tableaus. Dass die $(16, 6)$-Konfiguration einer Kummer-Fläche über ein solches Tableau beschrieben werden kann, ist Theorem 1.45 aus [20]:

Theorem 2.25. *Es sei $P \in \mathbb{P}^3_{\mathbb{C}}(\mathbb{C})$ ein Punkt, dessen G-Bahn aus 16 verschiedenen Punkten besteht und dessen Koordinaten die Bedingungen* (2.11) *erfüllen. Mithilfe des obigen Tableaus können wir die Elemente $\sigma \in G$ mit den 16 Punkten $\sigma(P)$ und den dazu dualen 16 Ebenen identifizieren.*

(i) Die 16 Punkte und Ebenen bilden bzgl. „$\in$“ eine $(16,6)$-Konfiguration vom Typ $(^*)$.

(ii) Jede $(16,6)$-Konfiguration vom Typ $(^*)$, bestehend aus Punkten und Ebenen in $\mathbb{P}^3_{\mathbb{C}}$ bzgl. „$\in$“, ist bis auf einen Automorphismus von $\mathbb{P}^3_{\mathbb{C}}$ von dieser Form.

Eine ähnliche Gruppe von Automorphismen, die durch Permutation und Vorzeichenwechsel von Koordinaten operieren, kann auch im projektiven Raum $\mathbb{P}^7_{\mathbb{C}}$ gefunden werden. Dazu seien die Automorphismen ϕ_i, ψ_j für $i, j \in \{0, \dots, 7\}$ so definiert wie in der Liste angegeben:

$$\begin{aligned}
\phi_0 &= 1 & \psi_0 &= 1\\
\phi_1 &= (01)(23)(45)(67), & \psi_1 &= v_{0123},\\
\phi_2 &= (02)(13)(46)(57), & \psi_2 &= v_{0145},\\
\phi_3 &= (03)(12)(47)(56), & \psi_3 &= v_{0167},\\
\phi_4 &= (04)(15)(26)(37), & \psi_4 &= v_{0246},\\
\phi_5 &= (05)(14)(27)(36), & \psi_5 &= v_{0257},\\
\phi_6 &= (06)(17)(24)(35), & \psi_6 &= v_{0347},\\
\phi_7 &= (07)(16)(25)(34), & \psi_7 &= v_{0356}.
\end{aligned}$$

Jeder dieser Automorphismen ist sein eigenes Inverses. Die Automorphismen der Form ϕ_i bilden eine abelsche Gruppe: Die Automorphismen ϕ_1, ϕ_2, ϕ_4 kommutieren und es gilt $\phi_1\phi_2 = \phi_3$, $\phi_4\phi_i = \phi_{i+4}$ für $i \leq 3$, was die Abgeschlossenheit zeigt. Gleiches gilt für die Automorphismen der Form ψ_j: Es gilt $\psi_2\psi_4 = \psi_6$, $\psi_1\psi_{2j} = \psi_{2j+1}$ für $j \leq 3$ und ψ_1, ψ_2, ψ_4 kommutieren. Ebenso gilt $\phi_i\psi_j = \psi_j\phi_i$ für alle i, j, da die Koordinaten, in denen ein Vorzeichenwechsel stattfindet, entweder nur untereinander oder nur mit den Koordinaten ohne Vorzeichenwechsel vertauscht werden. Die von den ϕ_i und ψ_j erzeugte Untergruppe $G \subset \mathrm{Aut}(\mathbb{P}^7_{\mathbb{C}})$ ist daher isomorph zu $\{\phi_i,\ 0 \leq i \leq 7\} \times \{\psi_j,\ 0 \leq j \leq 7\} \cong (\mathbb{Z}/2\mathbb{Z})^6$. Wir können G auch als direktes Produkt

$$G = \{1, \phi_3\psi_2, \phi_2\psi_6, \phi_1\psi_4\} \times \{1, \phi_3\psi_4, \phi_2\psi_2, \phi_1\psi_6\} \times \{1, \phi_4, \psi_1, \phi_4\psi_1\} \tag{2.12}$$

schreiben. Wir ordnen die Elemente von G in einem Würfel aus $4\times4\times4$ Blöcken so an wie in Abbildung 6 dargestellt. In der Abbildung sind die vier aufeinander liegenden Ebenen des Würfels gezeigt. Das neutrale Element erhält die Position $(1,1,1)$, die drei Untergruppen von G aus (2.12) weisen davon ausgehend in die verschiedenen Raumdimensionen (grau schattierte Felder). Man sieht leicht, dass das Element an Position (i,j,k) nun das Produkt der drei Elemente an den Positionen $(i,1,1)$, $(1,j,1)$ und $(1,1,k)$ ist.

1	$\phi_3\psi_4$	$\phi_2\psi_2$	$\phi_1\psi_6$
$\phi_3\psi_2$	ψ_6	ϕ_1	$\phi_2\psi_4$
$\phi_2\psi_6$	$\phi_1\psi_2$	ψ_4	ϕ_3
$\phi_1\psi_4$	ϕ_2	$\phi_3\psi_6$	ψ_2

ϕ_4	$\phi_7\psi_4$	$\phi_6\psi_2$	$\phi_5\psi_6$
$\phi_7\psi_2$	$\phi_4\psi_6$	ϕ_5	$\phi_6\psi_4$
$\phi_6\psi_6$	$\phi_5\psi_2$	$\phi_4\psi_4$	ϕ_7
$\phi_5\psi_4$	ϕ_6	$\phi_7\psi_6$	$\phi_4\psi_2$

ψ_1	$\phi_3\psi_5$	$\phi_2\psi_3$	$\phi_1\psi_7$
$\phi_3\psi_3$	ψ_7	$\phi_1\psi_1$	$\phi_2\psi_5$
$\phi_2\psi_7$	$\phi_1\psi_3$	ψ_5	$\phi_3\psi_1$
$\phi_1\psi_5$	$\phi_2\psi_1$	$\phi_3\psi_7$	ψ_3

$\phi_4\psi_1$	$\phi_7\psi_5$	$\phi_6\psi_3$	$\phi_5\psi_7$
$\phi_7\psi_3$	$\phi_4\psi_7$	$\phi_5\psi_1$	$\phi_6\psi_5$
$\phi_6\psi_7$	$\phi_5\psi_3$	$\phi_4\psi_5$	$\phi_7\psi_1$
$\phi_5\psi_5$	$\phi_6\psi_1$	$\phi_7\psi_7$	$\phi_4\psi_3$

Abbildung 6: Anordnung der Automorphismen im Würfel (Querschnitte)

Wir stellen wie in (2.11) Bedingungen an die Koordinaten der Punkte $P \in \mathbb{P}^3_{\mathbb{C}}$. Diese lauten:

(i) $a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 \neq 0$.

(ii) $a_i^2+a_j^2+a_k^2+a_l^2 \neq a_{i'}^2+a_{j'}^2+a_{k'}^2+a_{l'}^2$, wann immer es ein λ gibt mit $\psi_\lambda = v_{ijkl} = v_{i'j'k'l'}$.

(iii) $a_ia_{i'}+a_ja_{j'} \neq \pm(a_ka_{k'}+a_la_{l'})$, wann immer es ein λ gibt mit $\phi_\lambda = (ii')(jj')(kk')(ll')$.

Wir erhalten auf diese Weise eine $(64, 28)$-Konfiguration aus Punkten und Hyperebenen in $\mathbb{P}^7_{\mathbb{C}}$, die als Kandidat für die Verallgemeinerung von Theorem 2.25 angesehen werden kann.

Proposition 2.26. *Es sei $P \in \mathbb{P}^7_{\mathbb{C}}(\mathbb{C})$ ein Punkt, dessen G-Bahn aus 64 verschiedenen Punkten besteht und dessen Koordinaten die genannten Bedingungen erfüllen. Mithilfe der Zuordnung in Abbildung 6 können wir die Elemente $\sigma \in G$ mit den 64 Punkten $\sigma(P)$ und den 64 Hyperebenen, die den Punkten $\sigma\phi_4\psi_1(P)$ entsprechen, identifizieren. Die 64 Punkte und Hyperebenen bilden bzgl. „$\in$“ eine $(64, 28)$-Konfiguration vom Typ $(^*)$.*

Beweis. Es reicht, die Aussage für einen ausgewählten Block des Würfels zu beweisen, da die Multiplikation mit einem Element von G lediglich Querschnitte des Würfels permutiert und die Inzidenzrelation erhält. Es liegt daher nahe, den Punkt P zu wählen, der ja dem neutralen Element 1 entspricht, und zu überprüfen, auf welchen Hyperebenen er liegt. Durch Nachrechnen verifiziert man, dass es sich um die 28 behaupteten Hyperebenen handelt. □

Der Hauptunterschied zur Konfiguration in $\mathbb{P}^3_{\mathbb{C}}$ liegt darin, dass Hyperebenen und Punkte nicht auf die gleiche Weise mit den Elementen von G identifiziert werden. Das Vorschalten des Automorphismus $\phi_4\psi_1$ ist nötig, da bei der Inzidenzrelation im Würfel der ausgewählte Punkt mit seiner dualen Hyperebene in Relation stehen muss.

Es sei A eine abelsche Dreifaltigkeit mit irreduzibler Prinzipalpolarisation, gegeben durch die symmetrische Garbe $\mathscr{L}$. Wir bezeichnen mit $f\colon A/\iota \to \mathbb{P}^7_{\mathbb{C}}$ die abgeschlossene Einbettung, die von $\mathscr{L}^2$ induziert wird. Die folgende Proposition dient zur Definition der *Coble-Quartik*. Ein Beweis findet sich in [15] (Prop. 7 in §IX.5 und anschl. Bem.).

Proposition 2.27. *Bezeichnet $A = Jac(X)$ die Jacobi-Varietät einer glatten nichthyperelliptischen Kurve X vom Geschlecht 3, dann ist $f(A/\iota)$ der singuläre Ort einer eindeutigen Hyperfläche $C_4 \subset \mathbb{P}^7_{\mathbb{C}}$. Bei geeigneter Koordinatenwahl ist C_4 die Verschwindungsmenge eines homogenen Polynoms $F \in \mathbb{C}[x_0, \ldots, x_7]$ der Form*

$$\begin{aligned}
F = \quad & r \cdot (x_0^4 + x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 + x_6^4 + x_7^4) \\
& + s_1 \cdot (x_0^2x_1^2 + x_2^2x_3^2 + x_4^2x_5^2 + x_6^2x_7^2) + t_1 \cdot (x_0x_2x_4x_6 + x_1x_3x_5x_7) \\
& + s_2 \cdot (x_0^2x_2^2 + x_1^2x_3^2 + x_4^2x_6^2 + x_5^2x_7^2) + t_2 \cdot (x_0x_1x_4x_5 + x_2x_3x_6x_7) \\
& + s_3 \cdot (x_0^2x_3^2 + x_1^2x_2^2 + x_4^2x_7^2 + x_5^2x_6^2) + t_3 \cdot (x_0x_3x_4x_7 + x_1x_2x_5x_6) \\
& + s_4 \cdot (x_0^2x_4^2 + x_1^2x_5^2 + x_2^2x_6^2 + x_3^2x_7^2) + t_4 \cdot (x_0x_1x_2x_3 + x_4x_5x_6x_7) \\
& + s_5 \cdot (x_0^2x_5^2 + x_1^2x_4^2 + x_2^2x_7^2 + x_3^2x_6^2) + t_5 \cdot (x_0x_2x_5x_7 + x_1x_3x_4x_6) \\
& + s_6 \cdot (x_0^2x_6^2 + x_1^2x_7^2 + x_2^2x_4^2 + x_3^2x_5^2) + t_6 \cdot (x_0x_1x_6x_7 + x_2x_3x_4x_5) \\
& + s_7 \cdot (x_0^2x_7^2 + x_1^2x_6^2 + x_2^2x_5^2 + x_3^2x_4^2) + t_7 \cdot (x_0x_3x_5x_6 + x_1x_2x_4x_7).
\end{aligned}$$

Die Gleichung von F ist invariant unter den Vorzeichenwechseln und Vertauschungen der Unbestimmten, die durch die Automorphismen $\phi_i\psi_j$ vermittelt werden, daher induzieren sie Automorphismen der Coble-Quartik. Das Ideal $I = (\partial F/\partial x_i,\ 0 \le i \le 7)$, dessen Verschwindungsmenge die Kummer-Dreifaltigkeit ist, bleibt ebenfalls invariant: Die ψ_j können höchstens einen Vorzeichenwechsel bei den Erzeugern von I bewirken, während die ϕ_i die Erzeuger permutieren. Somit können die Elemente $\phi_i\psi_j$ auch als Automorphismen der Kummer-Varietät angesehen werden. Da von einem Automorphismus singuläre Punkte wieder auf singuläre Punkte abgebildet werden, operieren die Automorphismen $\phi_i\psi_j$ schließlich auch auf den 64 singulären Punkten der Kummer-Dreifaltigkeit.

Wenn die Koordinaten eines singulären Punktes x die Bedingungen von Proposition 2.26 erfüllen und die Bahn aus 64 Punkten besteht, dann bilden die Punkte und die dualen Hyperebenen eine Konfiguration vom Typ (*). Inwieweit die Bedingungen die Situation einschränken und ob sie überhaupt erfüllt sein können, konnte leider nicht geklärt werden.

Frage 2.28. Lässt sich auch die $(64, 28)$-Konfiguration für die Singularitäten von Kummer-Dreifaltigkeiten in $\mathbb{P}^7_{\mathbb{C}}$ als Bahn eines Punktes realisieren?

3 Wilde Kummer-Varietäten

Ziel dieses Kapitels ist eine Untersuchung von Kummer-Varietäten über einem algebraisch abgeschlossenen Körper der Charakteristik $p = 2$. Eine Quotientensingularität wird als *wild* bezeichnet, wenn die Ordnung der operierenden Gruppe aufgefasst als Element des Grundkörpers nicht invertierbar ist; daher liegt es nahe, zur Unterscheidung von klassischen Kummer-Varietäten wie in Kapitel 2 auch von wilden Kummer-Varietäten zu sprechen.

Wilde Kummer-Flächen wurden bereits 1974 von Shioda in [51] und 1978 von Katsura in [32] beschrieben, für Kummer-Varietäten der Dimension $g \geq 3$ ist hingegen nur wenig bekannt. Der Hauptteil des Kapitels besteht darin, für die Kummer-Varietäten von Produkten elliptischer Kurven eine explizite Beschreibung einer offenen Umgebung eines singulären Punktes anzugeben. Mit der Verallgemeinerung eines Arguments von Katsura in [32], das die Theorie der formalen Gruppen benutzt, kann dieser Spezialfall noch etwas ausgedehnt werden: Es wird gezeigt, dass die Bestimmung der Singularitäten von allgemeineren *gewöhnlichen* Kummer-Varietäten, d. h., die von gewöhnlichen abelschen Varietäten stammen, bereits durch die Betrachtung von Produkten elliptischer Kurven abgedeckt ist.

3.1 Kummer-Flächen

Als Motivation für die Untersuchung von wilden Kummer-Varietäten dient uns die Analyse von Shioda [51] und Katsura [32] von Kummer-Flächen, deren Hauptresultate in diesem Abschnitt rekapituliert werden. Anders als in Kapitel 2 treten hier mehrere Fälle auf, die sich qualitativ unterschiedlich verhalten.

Der Grundkörper k sei in diesem Abschnitt stets algebraisch abgeschlossen.

Definition 3.1. Es gelte $\mathrm{char}(k) = p > 0$.

(*i*) Eine abelsche Varietät A der Dimension g wird *gewöhnlich* genannt, wenn die Gruppe $\ker(p_A)(k)$ aus genau p^g Elementen besteht.

(*ii*) Eine elliptische Kurve E wird *supersingulär* genannt, wenn sie keinen Punkt der Ordnung p besitzt.

(*iii*) Eine abelsche Varietät A wird *supersingulär* genannt, wenn es eine Isogenie von A zu einem Produkt supersingulärer elliptischer Kurven gibt. Ist A sogar isomorph zu einem solchen Produkt, so heißt A auch *superspeziell*.

Es folgen zwei Bemerkungen zur Definition:

Bemerkung 3.2. Für supersinguläre elliptische Kurven existiert eine Reihe äquivalenter Definitionen. Eine elliptische Kurve E ist nach [52], Theorem V.3.1, genau dann supersingulär, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Morphismus p_E ist rein inseparabel und die j-Invariante $j(E)$ liegt in $\mathbb{F}_{p^2}$.
- Die Verschiebung $V_{E/k}$ ist rein inseparabel.
- Der Endomorphismenring $\mathrm{End}(E)$ ist eine Ordnung in einer Quaternionenalgebra.

Wir werden sehen, dass es im Fall $p = 2$ bis auf Isomorphie nur eine supersinguläre elliptische Kurve E gibt. Für diese gilt $j(E) = 0$.

Bemerkung 3.3. Supersinguläre abelsche Flächen können auch dadurch charakterisiert werden, dass sie keinen Punkt der Ordnung p besitzen. Für höher-dimensionale abelsche Varietäten ist diese Aussage falsch, da hier nicht-supersinguläre abelsche Varietäten ohne Punkte der Ordnung p existieren.

Für wilde Kummer-Flächen hat Katsura 1976 Auflösungen der Singularitäten ermittelt sowie die Rationalität der Kummer-Flächen von supersingulären abelschen Flächen gezeigt. Seine Hauptresultate, die Theoreme A, B und C aus [32], werden hier wiedergegeben:

Theorem 3.4. *Es sei A eine abelsche Fläche über dem Grundkörper k und es gelte* $\mathrm{char}(k) = 2$. *Weiter seien $X = A/\iota$ die Kummer-Varietät von A und $s = |\ker(2_A)(k)|$.*

(i) Die Fläche X ist genau dann rational, wenn A eine supersinguläre abelsche Fläche ist. Dies ist wiederum genau dann der Fall, wenn die Singularität von X ein elliptischer Doppelpunkt ist.

(ii) Die minimale Desingularisierung von X ist genau dann eine $K3$-Fläche, wenn A nicht supersingulär ist. Äquivalent hierzu ist, dass die Singularitäten von X rational sind.

(iii) Die Singularitäten von X sind rationale Doppelpunkte vom Typ D_4, wenn $s = 4$, und vom Typ D_8, wenn $s = 2$ gilt. Im Fall $s = 1$ besitzt X einen elliptischen Doppelpunkt vom Typ $(19)_0$, *wenn A superspeziell ist, andernfalls besitzt X einen elliptischen Doppelpunkt vom Typ* $(4)^{(1)}_{0,1}$.

Für den Fall, dass A das Produkt von zwei elliptischen Kurven ist, gehen die genannten Beobachtungen (außer der Auflösung des elliptischen Doppelpunkts) auf Shioda in [51] und Artin in [2] zurück. Die Klassifikation und Benennung der Auflösungsgraphen der elliptischen Doppelpunkte geht auf Wagreich in [54], Theorem 3.8, zurück.

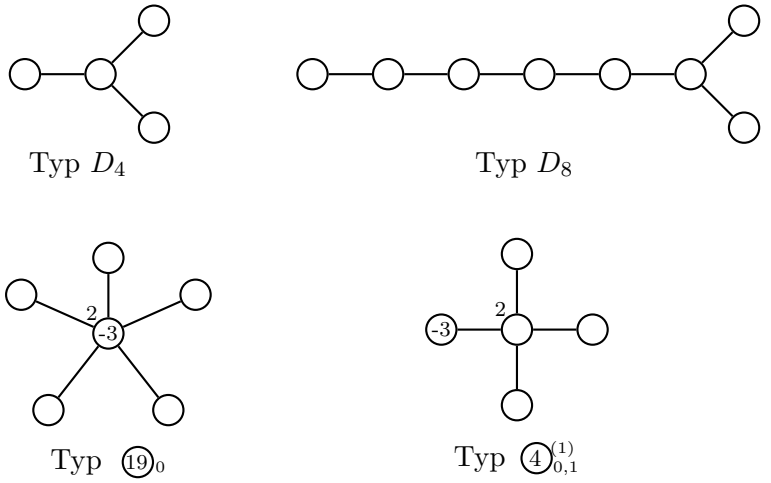


Abbildung 7: Duale Graphen zur Auflösung der Singularitäten

In Abbildung 7 sind die dualen Graphen zur minimalen Auflösung der Singularitäten dargestellt. Eine Auflösung von Singularitäten $\pi\colon \tilde{X} \to X$ heißt minimal, wenn jede Auflösung von Singularitäten $Y \to X$ durch π faktorisiert. Die Knoten im Graphen entsprechen rationalen Kurven, eine Kante zwischen zwei Knoten zeigt an, dass sich die entsprechenden Kurven schneiden. Ist im Knoten eine Zahl eingetragen, handelt es sich dabei um die Selbstschnittzahl der entsprechenden Kurve. Wenn keine Zahl eingetragen ist, beträgt sie -2. Steht neben einem Knoten eine Zahl, dann ist damit die Multiplizität der Kurve im Fundamentalzykel gemeint; diese hat den Wert 1, wenn keine Zahl genannt wird. Der Fundamentalzykel Z_0 der Auflösung einer Flächensingularität $x \in X$ ist dabei der eindeutig bestimmte effektive Divisor auf $\tilde{X}$, der die Bedingung $(Z_0 \cdot E_i) \leq 0$ für jede irreduzible Komponente E_i von $\pi^{-1}(\{x\})$ erfüllt und minimal mit dieser Eigenschaft ist (vgl. [54], Def. 2.2).

Bemerkung 3.5. Durch diese Graphen sind die zugehörigen Singularitäten allerdings noch nicht festgelegt. Für rationale Doppelpunkte hat Artin in [1] klassifiziert, welche Singularitäten die jeweiligen Auflösungsgraphen der ADE-Klassifikation besitzen (siehe Tabelle 1). Für Kummer-Flächen hat Schröer in [48], Propositionen 5.1 und 5.2, bewiesen, dass die rationalen Doppelpunkte D_4^1 und D_8^2 auftreten. Dieses Resultat wird im nächsten Abschnitt ebenfalls in Beispiel 3.35 erhalten. Für die elliptischen Doppelpunkte, welche im Quotienten von supersingulären abelschen Flächen auftreten, sind die vervollständigten lokalen Ringe ebenfalls bekannt: Ist die abelsche Fläche A isomorph zum Produkt zweier supersingulärer elliptischer Kurven, so ist die Singularität von A/ι durch den Ring

$$k[\![s,t,z]\!]/(z^2 + s^2t^2z + s^4t + st^4)$$

gegeben (siehe [32], Prop. 8). Wenn die supersinguläre abelsche Fläche A nicht isomorph

A_n:	$z^{n+1} + xy$	für $n \geq 1$
D^0_{2n}:	$z^2 + x^2y + xy^n$	für $n \geq 2$
D^r_{2n}:	$z^2 + x^2y + xy^n + xy^{n-r}z$	für $n \geq 2$, $1 \leq r \leq n-1$
D^0_{2n+1}:	$z^2 + x^2y + y^nz$	für $n \geq 2$
D^r_{2n+1}:	$z^2 + x^2y + y^nz + xy^{n-r}z$	für $n \geq 2$, $1 \leq r \leq n-1$
E^0_6:	$z^2 + x^3 + y^2z$	
E^1_6:	$z^2 + x^3 + y^2z + xyz$	
E^0_7:	$z^2 + x^3 + xy^3$	
E^1_7:	$z^2 + x^3 + xy^3 + x^2yz$	
E^2_7:	$z^2 + x^3 + xy^3 + y^3z$	
E^3_7:	$z^2 + x^3 + xy^3 + xyz$	
E^0_8:	$z^2 + x^3 + y^5$	
E^1_8:	$z^2 + x^3 + y^5 + xy^3z$	
E^2_8:	$z^2 + x^3 + y^5 + xy^2z$	
E^3_8:	$z^2 + x^3 + y^5 + y^3z$	
E^4_8:	$z^2 + x^3 + y^5 + xyz$	

Tabelle 1: Rationale Doppelpunkte in Charakteristik 2 nach Artin [1]

zu einem solchen Produkt ist, dann ist die Singularität durch $k[\![x,y,z]\!]/(f)$ mit

$$f = z^2 + x^2bz + x^4y + xb^2, \qquad b = (q^4+q)x + y^2$$

gegeben für ein geeignetes $q \in k$ (siehe [48], Prop. 5.3).

Dass auch bei den genannten elliptischen Doppelpunkten der duale Graph zur Festlegung der Singularität nicht ausreicht, wird im Folgenden kurz ausgeführt.

Definition 3.6. Es sei X eine irreduzible, normale, eigentliche Fläche über k mit einem singulären Punkt $x \in X$. Es sei Γ der duale Auflösungsgraph, dessen Knoten mit der Selbstschnittzahl, dem Geschlecht und der Multiplizität der entsprechenden Kurven versehen sind. Die Singularität x heißt *taut*, wenn jede normale Flächen-Singularität mit gleichem gewichteten dualen Graphen selbst bereits formal isomorph zu x ist.

Es seien $\pi\colon \tilde{X} \to X$ die minimale Auflösung von x und $E_1, \ldots, E_n$ die irreduziblen Komponenten von $\pi^{-1}(\{x\})$, aufgefasst als reduzierte Schemata. Wir nehmen weiter an, dass die E_i regulär sind, dass sich keine drei E_i in einem Punkt schneiden und dass sich im Fall $E_i \cap E_j \neq \emptyset$ die Komponenten transversal schneiden. Nach [49], Lemma 1.8, ist dann die folgende Bedingung notwendig für Tautheit:

Lemma 3.7. *Wenn $x \in X$ taut ist und die obigen Annahmen gelten, dann schneidet jede irreduzible Komponente E_i höchstens drei weitere Komponenten.*

Diese Bedingung ist bei den genannten elliptischen Doppelpunkten offenkundig verletzt.

3.2 Produkte elliptischer Kurven

Es seien $E_1, \ldots, E_g$ elliptische Kurven über einem algebraisch abgeschlossenen Körper k der Charakteristik $p = 2$, weiter sei

$$A = E_1 \times \cdots \times E_g$$

das Produkt dieser Kurven. Auf A ist die Vorzeicheninvolution $\iota\colon A \to A$ als Diagonalwirkung auf den Faktoren gegeben, d. h., ι ist Produkt der Involutionen $\iota_r\colon E_r \to E_r$ auf den Faktoren. Die Voraussetzung $k = \bar{k}$ wird nur dafür benötigt, geeignete Weierstraß-Gleichungen der elliptischen Kurven zu erhalten.

Die abelsche Varietät A wird nun in Hinblick auf die Singularitäten der zugehörigen Kummer-Varietät untersucht. Dazu werden offene affine Unterschemata von A/ι berechnet, die genau einen der singulären Punkte enthalten (wenn $g \geq 2$ gilt). Dies geschieht, indem die induzierte Wirkung von ι auf dem Koordinatenring einer geeigneten offenen affinen Umgebung eines 2-Torsionspunktes von A betrachtet und die invarianten Elemente hierin berechnet werden. Während dies im Allgemeinen schwierig zu bewerkstelligen ist, kann das Problem hier dank der speziellen Form der Diagonalwirkung auf ein Problem der modularen Invariantentheorie reduziert werden.

3.2.1 Die Diagonalwirkung auf den Faktoren

Wir betrachten zunächst eine elliptische Kurve E mit $j_E = j(E) \neq 0$. Es sei $\alpha \in k$ ein Element mit $\alpha^6 = j_E^{-1}$. Die Weierstraß-Gleichung $y^2 + \alpha xy = x^3 + \beta x$ mit Koeffizienten α und $\beta = \alpha j_E^{-1}$ definiert eine Kurve mit nicht-verschwindender Diskriminante und j-Invariante j_E, also eine zu E isomorphe elliptische Kurve. Wir nehmen daher an, dass E durch obige Gleichung gegeben ist. Bezeichnet $O = (0 : 1 : 0)$ das neutrale Element in homogenen Koordinaten, dann ist $U = E \setminus \{O\}$ ein offenes affines Unterschema von E mit affinem Koordinatenring

$$R_{j_E} = \Gamma\left(U, \mathscr{O}_E\right) = k\left[x, y\right] / (y^2 + \alpha xy + x^3 + \beta x).$$

Da lediglich das neutrale Element entfernt wurde, welches ein Fixpunkt unter der Vorzeicheninvolution ι ist, handelt es sich bei U um eine ι-invariante offene affine Teilmenge. Auf rationalen Punkten $E(k)$ operiert ι durch

$$(x, y) \longmapsto (x, y + \alpha x)$$

und ist damit festgelegt (vgl. [52], Alg. III.2.3). Der Punkt $(0, 0) \in U$, der dem maximalen Ideal $(x, y) \subset R_{j_E}$ entspricht, ist ein 2-Torsionspunkt von E, insbesondere ist E also eine

gewöhnliche elliptische Kurve. Auf R_{j_E} erhält man die induzierte ι-Wirkung durch $x \mapsto x$, $y \mapsto y + \alpha x$. Es wird sich als wichtig herausstellen, dass durch diese Abbildungsvorschrift auch eine lineare Gruppenwirkung auf $\mathbb{A}^2_k = \operatorname{Spec}(k[x,y])$ gegeben ist, die auf $\operatorname{Spec}(R_{j_E})$ die ι-Wirkung induziert.

Nun sei E eine elliptische Kurve mit $j_E = 0$. Diese kann durch die Weierstraß-Gleichung $y^2 + y = x^3$ definiert werden. Wir gehen zur homogenen Gleichung $Y^2Z + YZ^2 = X^3$ über und erhalten auf $E(k)$ die Operation von ι durch

$$(X : Y : Z) \longmapsto (X : Y + Z : Z).$$

Der Punkt $O = (0 : 1 : 0)$ ist der einzige Fixpunkt von ι, somit ist E supersingulär. Dehomogenisiert man die Weierstraß-Gleichung durch Einführung der neuen Koordinaten $x = X/Y$, $z = Z/Y$, dann ergibt sich das offene affine Unterschema

$$U' = \operatorname{Spec}\left(k\left[x,z\right]/(z + z^2 + x^3)\right),$$

in dem nur der rationale Punkt $(0 : 0 : 1)$ nicht enthalten ist. Diese offene Umgebung des neutralen Elements ist nicht ι-invariant, da $(0 : 1 : 1) \in U'$ von ι auf den Punkt $(0 : 0 : 1)$ abgebildet wird. Um eine ι-invariante offene affine Umgebung zu erhalten, muss aber lediglich dieser Punkt (und damit der Orbit von $(0 : 0 : 1)$) aus U' entfernt werden, was durch Lokalisieren an $z + 1$ realisiert wird. Man erhält den Ring

$$R_0 = k\left[x, z, (z+1)^{-1}\right]/(z + z^2 + x^3),$$

dessen Spektrum die gewünschte Umgebung U des Fixpunktes $(0 : 1 : 0)$ bildet. Der durch ι induzierte k-Algebrenautomorphismus $\iota^* \colon R_0 \to R_0$ ist durch

$$x \longmapsto \frac{x}{z+1}, \qquad z \longmapsto \frac{z}{z+1}$$

gegeben. Das Element $(z+1)^{-1}$ wird nach dieser Festlegung von ι^* auf $z + 1$ abgebildet. Das folgende Lemma gibt eine einfachere Beschreibung von R_0, die mit lediglich zwei Erzeugern auskommt.

Lemma 3.8. *Die k-Algebra R_0 wird von $x^2(z+1)^{-1}$ und $x(z+1)^{-1}$ erzeugt. Durch*

$$\Phi \colon S = k\left[v,w\right]/(w^2 + v^2w + v) \longrightarrow R_0$$
$$v \longmapsto \frac{x^2}{z+1}, \qquad w \longmapsto \frac{x}{z+1}$$

ist ein Isomorphismus von k-Algebren gegeben.

Beweis. Die Wohldefiniertheit kann leicht nachgerechnet werden durch

$$\begin{aligned}\Phi(w^2+v^2w+v) &= \frac{x^2}{(z+1)^2}+\frac{x^4}{(z+1)^2}\cdot\frac{x}{z+1}+\frac{x^2}{z+1}\\ &= \frac{x^2}{(z+1)^3}\cdot\left(z+x^3+z^2\right)=0.\end{aligned}$$

Dass die Festlegung automatisch einen Homomorphismus liefert, ist durch die universelle Eigenschaft des Polynomrings sichergestellt. Die Surjektivität von Φ kann ebenfalls nachgerechnet werden: So gelten etwa

$$\Phi\left(vw+1\right)=\frac{1}{z+1},\quad \Phi\left(vw+v^3\right)=z,\quad \Phi\left(w(vw+v^3+1)\right)=x,$$

womit Erzeuger von R_0 (als k-Algebra) im Bild liegen.

Es bleibt nun noch zu zeigen, dass Φ injektiv ist. Das Polynom

$$w^2+v^2w+v\in k[v][w]=k[v,w]$$

ist irreduzibel nach Eisensteinkriterium (wähle das Primelement v), also ein Primelement im zweidimensionalen faktoriellen Ring $k[v,w]$. Entsprechend ist S integer und nach dem Hauptidealsatz von Krull eindimensional. Da R_0 und damit $S/\ker(\Phi)$ integre Ringe sind, muss $\ker(\Phi)\subset S$ ein Primideal sein. Folglich gilt entweder $\ker(\Phi)=0$ oder $\ker(\Phi)$ ist ein maximales Ideal. Der letztgenannte Fall kann nicht auftreten, da R_0 kein Körper ist. □

Durch $\Phi^{-1}\circ\iota^*\circ\Phi\colon S\to S$ erhält man die induzierte Involutionswirkung auf S. Diese wird der Einfachheit halber ebenfalls mit ι^* bezeichnet.

Lemma 3.9. *Die induzierte Involution auf der k-Algebra S ist gegeben durch*

$$v\longmapsto v,\qquad w\longmapsto w+v^2.$$

Diese Wirkung wird zwar nicht von einer linearen Wirkung auf $\mathbb{A}^2_k$ induziert, aber kann noch als eng verwandt angesehen werden.

Beweis. Das Element $x\cdot x(z+1)^{-1}\in R_0$ ist invariant, da die Involution die Faktoren des Produkts vertauscht. Weiterhin gilt

$$\begin{aligned}w+v^2 &= \Phi^{-1}\left(\frac{x}{z+1}+\frac{x^4}{z^2+1}\right)=\Phi^{-1}\left(\frac{x(z+1+x^3)}{z^2+1}\right)\\ &= \Phi^{-1}\left(\frac{x(z^2+1)}{z^2+1}\right)=\Phi^{-1}\left(\iota^*\left(\frac{x}{z+1}\right)\right)=\Phi^{-1}\circ\iota^*\circ\Phi(w)=\iota^*(w),\end{aligned}$$

wobei $z^2=z+x^3$ ausgenutzt wurde. □

Ist nun $A = E_1 \times \cdots \times E_g$ und sind $E_1, \ldots, E_r$ gewöhnliche elliptische Kurven und $E_{r+1}, \ldots, E_g$ supersingulär, dann ist das Spektrum des Rings

$$R = R_{j_1} \otimes \ldots \otimes R_{j_r} \otimes R_0^{\otimes g-r}$$

mit $j_n = j_{E_n}$ ein offenes affines Unterschema von A, das nach Konstruktion genau einen 2-Torsionspunkt von A enthält. Um die Gruppenoperation der Vorzeicheninvolution in der Notation einfacher zu halten, wird der Ring R_{j_E} mit dem isomorphen Ring

$$k\,[x, y]\,/(y^2 + xy + \alpha^{-3}x^3 + \alpha^{-1}\beta x)$$

mit der induzierten Involutionswirkung $x \mapsto x$, $y \mapsto y + x$ identifiziert, ebenso wird R_0 durch S ersetzt. Wir erhalten dadurch die folgende Situation:

Lemma 3.10. *Es seien k ein algebraisch abgeschlossener Körper der Charakteristik $p = 2$ und $A = E_1 \times \ldots \times E_g$ Produkt elliptischer Kurven über k, wobei die Faktoren $E_1, \ldots, E_r$ gewöhnlich und $E_{r+1}, \ldots, E_g$ supersingulär seien. Dann ist durch das Spektrum des Ringes*

$$R = k\,[x_1, y_1, \ldots, x_r, y_r, v_{r+1}, w_{r+1}, \ldots, v_g, w_g]\,/I,$$

wobei das Ideal I von Polynomen der Form

$$\begin{aligned} &y_i^2 + x_i y_i + \gamma_i x_i^3 + \delta_i x_i, \quad 1 \leq i \leq r \\ &w_j^2 + v_j^2 w_j + v_j, \quad r+1 \leq j \leq g \end{aligned}$$

erzeugt wird, eine offene affine ι-invariante Umgebung genau eines 2-Torsionspunktes von A gegeben. Dabei hängen die Parameter

$$\gamma_i = j_{E_i}^{\frac{1}{2}} \quad \textit{und} \quad \delta_i = j_{E_i}^{-1}$$

nur von der elliptischen Kurve E_i ab. Die Vorzeicheninvolution $\iota\colon A \to A$ induziert eine $\mathbb{Z}/2\mathbb{Z}$-Wirkung auf der k-Algebra R, welche durch

$$\begin{aligned} &x_i \longmapsto x_i, \quad y_i \longmapsto y_i + x_i, \qquad 1 \leq i \leq r, \\ &v_j \longmapsto v_j, \quad w_j \longmapsto w_j + v_j^2, \quad r+1 \leq j \leq g \end{aligned}$$

festgelegt ist.

Der Einfachheit halber bezeichnen wir den Erzeuger von $\mathbb{Z}/2\mathbb{Z}$ ebenfalls mit ι und verzichten auf eine Unterscheidung zwischen Vorzeicheninvolution und induzierter Wirkung in der Notation.

Wir betrachten den Ring R aus Lemma 3.10 und die Gruppenwirkung etwas genauer. Es sei $\hat{R}$ die Vervollständigung von R am Ursprung. Für die Erzeuger des Ideals I gilt

$$\frac{\partial}{\partial x_i}(y_i^2 + x_i y_i + \gamma_i x_i^3 + \delta_i x_i) = y_i + \gamma_i x_i^2 + \delta_i \in \hat{R}^\times,$$
$$\frac{\partial}{\partial v_j}(w_j^2 + v_j^2 w_j + v_j) = 1 \in \hat{R}^\times,$$

sodass nach dem Satz über implizite Funktionen (siehe [7], S. A.IV.37) eindeutige formale Potenzreihen $x_i(y_i)$ und $v_j(w_j)$ existieren, die die entsprechenden Relationen in $\hat{R}$ erfüllen. Es folgt

$$\hat{R} \cong k[\![y_1, \ldots, y_r, w_{r+1}, \ldots, w_g]\!]$$

und die Wirkung der Vorzeicheninvolution auf $\hat{R}$ ist nach [45], Proposition 2.1, nicht linear:

Proposition 3.11. *Es sei k ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und $S = k[\![u_1, \ldots, u_g]\!]$ versehen mit der Wirkung einer Gruppe G, deren Ordnung ein Vielfaches von p ist. Wenn der Morphismus $\operatorname{Spec}(S) \to \operatorname{Spec}(S^G)$ nur am maximalen Ideal $\mathfrak{m} \subset S$ verzweigt ist, dann ist es nicht möglich, Koordinaten für S zu wählen, sodass G auf der k-Algebra S linear operiert.*

Die Strategie besteht daher darin, möglichst lange mit einer einfacheren Gruppenwirkung zu arbeiten, die möglichst nahe an eine lineare Wirkung herankommt. Die folgende Beobachtung zeigt, dass man sich bei speziellen Diagonalwirkungen in positiver Charakteristik auf eine Wirkung auf dem affinen Raum zurückziehen kann:

Proposition 3.12. *Es seien k ein Körper der Charakteristik $p > 0$ und $G \cong \mathbb{Z}/p\mathbb{Z}$ zyklisch der Ordnung p. Auf dem Polynomring $S = k[A_1, B_1, \ldots, A_g, B_g]$ operiere die Gruppe $G = \langle\sigma\rangle$ durch*

$$\sigma(A_i) = A_i, \qquad \sigma(B_i) = B_i + A_i^{e_i}, \tag{3.1}$$

für natürliche Zahlen $e_i \geq 1$. Weiter seien Polynome $f_i \in S$ der Form

$$f_i = B_i^p - A_i^{(p-1)e_i} B_i + P_i(A_i) \tag{3.2}$$

mit Polynomen $P_i \in A_i\, k[A_i]$ gegeben und es bezeichne $I = (f_1, \ldots, f_g) \subset S$ das von den f_i erzeugte Ideal. Dann wird durch die G-Wirkung auf S eine Wirkung auf dem Quotienten S/I induziert und die Restklassenabbildung definiert einen surjektiven Homomorphismus $\phi\colon S^G \to (S/I)^G$ von k-Algebren. Insbesondere gilt

$$S^G/I \cap S^G \cong (S/I)^G. \tag{3.3}$$

Beweis. Da $\sigma(f_i) = f_i$ erfüllt ist, folgt $\sigma(I) = I$ und man erhält durch (3.1) eine wohldefinierte G-Wirkung auf dem Quotienten S/I. Somit ist auch der Homomorphismus ϕ wohldefiniert, da $\sigma(h + I) = \sigma(h) + I$.

Es sei $h + I \in S/I$ ein beliebiges Element. Dieses besitzt einen Repräsentanten $h_0 \in S$, sodass in jedem Monom von h_0 alle Unbestimmten $B_1, \ldots, B_g$ höchstens mit Exponent $p - 1$ auftreten, also sodass

$$\deg_{B_i}(h_0) \leq p - 1$$

für alle $1 \leq i \leq g$ gilt. Dieser Repräsentant kann etwa erhalten werden, indem in h alle höheren Potenzen der B_i sukzessiv mittels der Relation $B_i^p = A_i^{(p-1)e_i} B_i + P_i$ verkleinert werden. Das Polynom

$$\sigma(h_0) = h_0(A_1, B_1 + A_1^{e_1}, \ldots, A_g, B_g + A_g^{e_g})$$

erfüllt ebenso wie h_0 die Eigenschaft $\deg_{B_i}(\sigma(h_0)) \leq p - 1$. Gleiches gilt entsprechend für die Differenz $\sigma(h_0) - h_0 \in S$. Weiterhin ist $h_0 + I \in S/I$ genau dann invariant unter der Gruppenwirkung, wenn $\sigma(h_0) - h_0 \in I$ in S gilt. Wenn sogar $\sigma(h_0) - h_0 = 0$ gilt, dann ist $h_0 \in S$ invariant und $h + I = \phi(h_0)$ im Bild von ϕ.

Für die Surjektivität von ϕ reicht es nun zu zeigen, dass ein Element $h \in I$, das für jedes i die Bedingung $\deg_{B_i}(h) \leq p - 1$ erfüllt, automatisch das Nullpolynom ist. Im Folgenden werden I und S als k-Vektorräume betrachtet und geeignete Basen gesucht. Dazu sei für $1 \leq i \leq g$ die Menge M_i definiert als

$$M_i = \{A_i^r,\ A_i^r B_i,\ \ldots,\ A_i^r B_i^{p-1},\ \left(B_i^p + A_i^{(p-1)e_i} B_i + P_i\right) A_i^r B_i^s \mid r, s, \geq 0\},$$

deren Elemente eine Basis des k-Vektorraums $k[A_i, B_i]$ bilden. Folglich bilden die Elemente der Menge

$$M = M_1 \cdot \ldots \cdot M_g = \{m_1 \cdot \ldots \cdot m_g \mid m_i \in M_i,\ 1 \leq i \leq g\}$$

eine Vektorraumbasis von $S = k[A_1, B_1] \otimes \ldots \otimes k[A_g, B_g]$. Der Untervektorraum I besitzt ein Erzeugendensystem bestehend aus allen Elementen der Form

$$\left(B_i^p + A_i^{(p-1)e_i} B_i + P_i\right) A_1^{r_1} B_1^{s_1} \cdot \ldots \cdot A_g^{r_g} B_g^{s_g}$$

mit $1 \leq i \leq g$ und Exponenten $r_1, s_1, \ldots, r_g, s_g \geq 0$. Da man die Faktoren $A_j^{r_j} B_j^{s_j}$ in diesem Ausdruck in der Basis M_j schreiben kann, erhält man ein weiteres Erzeugendensystem von I, bestehend aus den Elementen der Form

$$\left(B_i^p + A_i^{(p-1)e_i} B_i + P_i\right) A_i^{r_i} B_i^{s_i} \cdot m_1^{(i)} \cdot \ldots \cdot \hat{m}_i \cdot \ldots \cdot m_g^{(i)} \tag{3.4}$$

mit $1 \leq i \leq g$, $r_i, s_i \geq 0$ und $m_j^{(i)} \in M_j$ für $1 \leq j \leq g$. Dabei bedeutet $\hat{m}_i$ die Auslassung des Faktors im Produkt. Dieses Erzeugendensystem von I besteht aus genau den Elementen von M, die mindestens einen Faktor m_d mit $\deg_{B_d}(m_d) \geq p$ enthalten.

Ist nun $h \in I$ mit $\deg_{B_i}(h) \leq p-1$ für alle i, dann kann h einerseits als Linearkombination des Erzeugendensystems (3.4) von I geschrieben werden, andererseits lässt sich h auch als Linearkombination der anderen Elemente von M, nämlich von Basiselementen der Form $m_1 \cdot \ldots \cdot m_g$ mit

$$m_i \in \{A_i^r,\ A_i^r B_i, \ldots, A_i^r B_i^{p-1} \mid r \geq 0\}$$

darstellen. Aus der Eindeutigkeit der Darstellung bzgl. der Basis M von S ergibt sich wie gewünscht $h = 0$. Damit ist nun gezeigt, dass $\sigma(h_0 + I) = h_0 + I \in S/I$ genau dann gilt, wenn $\sigma(h_0) = h_0 \in S$ invariant ist; jedes Element von $(S/I)^G$ ist folglich Restklasse eines invarianten Elements aus S^G. □

Der Beweis der Proposition gibt das folgende Korollar:

Korollar 3.13. *Jedes (invariante) Element $h + I \in S/I$ besitzt einen eindeutigen (invarianten) Repräsentanten $h_0 \in S$ mit $deg_{B_i}(h_0) \leq p-1$ für alle $1 \leq i \leq g$.*

Bemerkung 3.14. Es ist wohlbekannt, dass für eine endliche Gruppe G, deren Ordnung nicht von der Charakteristik des Grundkörpers geteilt wird, stets die Isomorphie (3.3) gilt: Es seien S eine k-Algebra mit G-Wirkung und $I \subset S$ ein Ideal, das durch G in sich selbst überführt wird. Dazu betrachten wir den Homomorphismus

$$f\colon S \longrightarrow S^G, \qquad x \longmapsto \frac{1}{\operatorname{ord}(G)} \sum_{\sigma \in G} \sigma(x),$$

und das kommutative Diagramm von k-Vektorräumen

$$\begin{array}{ccc} S & \xrightarrow{\ \pi\ } & S/I \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \bar{f}} \\ S^G & \xrightarrow[\ q\ ]{} & (S/I)^G \end{array}$$

mit surjektiven Homomorphismen π, f und $\bar{f}$. Aus der Kommutativität ergibt sich nun mit

$$\operatorname{Im}(q) = \operatorname{Im}(q \circ f) = \operatorname{Im}\left(\bar{f} \circ \pi\right) = (S/I)^G$$

unmittelbar die Aussage.

Für wilde Gruppenoperationen, d. h. p teilt $|G|$, ist die Isomorphie (3.3) im Allgemeinen nicht gegeben. Dazu geben wir hier ein einfaches Beispiel.

Beispiel 3.15. Wir betrachten den Polynomring $S = \mathbb{F}_2[X, Y]$ mit der Wirkung der symmetrischen Gruppe $G = S_2$, die die Unbestimmten vertauscht. Außerdem definieren wir das G-invariante Hauptideal $I = (X + Y) \subset S$. Im Ring S/I ist jedes Element $f + I$ invariant, d. h. $f(X, Y) - f(Y, X) \in I$, da jedes Monom eine Relation der Form

$$\begin{aligned} X^n Y^m + X^m Y^n &= X^m Y^m \left(X^{n-m} + Y^{n-m}\right) \\ &= X^m Y^m (X + Y) \left(\sum_{a=0}^{n-m-1} X^a Y^{n-m-1-a} \right) \in I \end{aligned}$$

erfüllt, wobei ohne Einschränkung $m \leq n$ angenommen wurde und die Konvention gilt, dass die leere Summe den Wert 0 besitzt. Andererseits gilt nach dem Hauptsatz über symmetrische Polynome $S^G = \mathbb{F}_2[X+Y,\, XY]$. Die Klasse $X+I \in (S/I)^G$ liegt nicht im Bild der Restklassenabbildung $S^G \to (S/I)^G$. Andernfalls würden Polynome $g(X, Y), h(XY) \in S$ existieren, sodass $X = h(XY) + (X + Y)g(X, Y)$ in S geschrieben werden könnte. Ein Koeffizientenvergleich der linearen Terme zeigt aber, dass das nicht sein kann. Folglich ist die Restklassenabbildung nicht surjektiv auf den Invariantenringen.

In diesem Beispiel ist die G-Wirkung auf dem Quotienten trivial, was eine sehr spezielle Situation darstellt. Da die Berechnung von Invariantenringen ein schwieriges Problem darstellt, fehlt es an weiteren Beispielen, die bei der Einordnung von Proposition 3.12 helfen.

Frage 3.16. Ist die Isomorphie aus Proposition 3.12 bei wilden Gruppenoperationen eher die Ausnahme oder doch bereits unter milden Bedingungen erfüllt?

3.2.2 Die Erzeuger des Invariantenrings

In der Situation von Lemma 3.10 soll nun der Invariantenring R^ι ermittelt werden. Wir verwenden die Notation

$$\begin{aligned} &S = k\left[x_1, y_1, \ldots, x_r, y_r, v_{r+1}, w_{r+1}, \ldots, v_g, w_g\right], \\ &P_i(x_i) = \gamma_i x_i^3 + \delta_i x_i \;\text{ mit }\; \gamma_i = j_{E_i}^{\frac{1}{2}},\;\; \delta_i = j_{E_i}^{-1} \;\text{ für }\; 1 \leq i \leq r, \\ &I = \left(y_i^2 + x_i y_i + P_i(x_i),\; w_j^2 + v_j^2 w_j + v_j,\; 1 \leq i \leq r < j \leq g\right) \subset S, \\ &R = S/I, \end{aligned} \tag{3.5}$$

und haben dabei sowohl auf R als auch auf S die Involutionswirkung durch

$$x_i \longmapsto x_i, \quad y_i \longmapsto y_i + x_i, \quad v_j \longmapsto v_j, \quad w_j \longmapsto w_j + v_j^2. \tag{3.6}$$

Die Zahl $r \in \mathbb{N}$ ist die Anzahl der gewöhnlichen elliptischen Kurven, die als Faktoren in $A = E_1 \times \ldots \times E_g$ auftreten. Der Fall $r = 0$ ist erlaubt, es treten dann keine x_i, y_i als

Unbestimmte auf. Ebenso erlaubt ist der Fall $r = g$.

Zur Unterscheidung bezeichne $\iota\colon R \to R$ die Involution auf R und $\tilde{\iota}\colon S \to S$ den Automorphismus von S. Nach Proposition 3.12 ist jedes invariante Element von R nun die Restklasse eines invarianten Polynoms aus S. Weiter folgt aus Korollar 3.13, dass nur Elemente aus S, deren Grad bzgl. der Unbestimmten y_i, w_j höchstens 1 beträgt, betrachtet werden müssen. Tatsächlich können wir diese Elemente eindeutig mit den jeweiligen Restklassen in R identifizieren.

Zuerst betrachten wir den Fall, dass keine supersinguläre elliptische Kurve als Faktor der abelschen Varietät A auftritt. Die ι-Wirkung stammt dann von einer linearen Gruppenwirkung auf dem Spektrum des Rings $S = k[x_1, y_1, \ldots, x_g, y_g]$. In diesem konkreten Fall sind bereits Erzeugendensysteme des Invariantenrings $S^{\tilde{\iota}}$ bekannt: Für den Fall $p = 2$, der ja hier betrachtet wird, gab Richman 1990 in [47], Proposition 2, ein Erzeugendensystem an. Dass dieses auch für beliebiges $p \geq 2$ den Invariantenring erzeugt, konnten Campbell und Hughes in [9], S. 4, verifizieren. Shank und Wehlau konnten dieses Resultat noch dahingehend verbessern, dass sie in [50], Corollary 4.4, bestätigen konnten, dass es sich um ein minimales Erzeugendensystem handelt. Sie bewiesen das folgende Theorem:

Theorem 3.17. *Es seien $K = \mathbb{F}_p$ und $G = \langle\sigma\rangle$ zyklische Gruppe der Ordnung p sowie $S_K = K[x_1, y_1, \ldots, x_g, y_g]$ mit G-Wirkung gegeben durch $\sigma(x_i) = x_i$, $\sigma(y_i) = y_i + x_i$ für $1 \leq i \leq g$. Dann ist durch die Elemente*

$$
\begin{aligned}
&x_i \quad \text{für } 1 \leq i \leq g,\\
&x_i y_j - x_j y_i \quad \text{für } 1 \leq i < j \leq g,\\
&\mathrm{N}(y_i) \quad \text{für } 1 \leq i \leq g,\\
&\mathrm{Tr}\left(y_1^{a_1} \cdots y_g^{a_g}\right) \text{ für } 0 \leq a_1, \ldots, a_g \leq p-1 \text{ und } \textstyle\sum_i a_i > 2(p-1)
\end{aligned}
$$

ein minimales Erzeugendensystem des Invariantenrings S_K^G gegeben. Dabei bezeichnen $\mathrm{N}(X) = \prod_{\sigma\in G} \sigma(X)$ die Norm und $\mathrm{Tr}(X) = \sum_{\sigma\in G} \sigma(X)$ die Spur des Elements $X \in S_K$.

Dass die Aussage über dem Primkörper $K = \mathbb{F}_p$ getroffen wird, gibt eine größere Allgemeinheit des Resultats: Ist $K \subset L$ eine beliebige Körpererweiterung und tensoriert man die exakte Sequenz

$$0 \longrightarrow S_K^G \longrightarrow S_K \xrightarrow{\sigma-\mathrm{id}} S_K$$

von K-Vektorräumen mit dem flachen K-Modul L, so ergibt sich

$$0 \longrightarrow S_K^G \otimes L \longrightarrow S_L \xrightarrow{\sigma-\mathrm{id}} S_L,$$

also ist $S_K^G \otimes L = S_L^G$.

Mithilfe von Proposition 3.12 erhält man nun aus dem Theorem direkt ein Erzeugendensystem des Invariantenrings R^ι.

Theorem 3.18. *Es sei k ein Körper der Charakteristik $p = 2$, weiter seien die Ringe S und R sowie das Ideal $I \subset S$ definiert wie in* (3.5)*, wobei $r = g$ gelte (keine supersingulären Faktoren). Dann gilt: Der Invariantenring R^ι der $\mathbb{Z}/2\mathbb{Z}$-Wirkung* (3.6) *wird als k-Algebra von den Elementen der Form*

$$\mathrm{Tr}\,(y_{i_1} \cdot \ldots \cdot y_{i_m}) \in R \tag{3.7}$$

erzeugt, wobei $\{i_1, \ldots, i_m\} \subset \{1, \ldots, g\}$ alle nicht-leeren Teilmengen durchläuft.

Beweis. Die Elemente $\mathrm{N}(y_i)$ werden als Erzeuger nicht mehr benötigt, da in R die Gleichheit $\mathrm{N}(y_i) = y_i^2 + x_i y_i = P_i(x_i)$ gilt. Die anderen Erzeuger aus Theorem 3.17 sind abgedeckt durch $x_i = \mathrm{Tr}(y_i)$ und $x_i y_j + x_j y_i = \mathrm{Tr}(y_i y_j) + \mathrm{Tr}(y_i)\mathrm{Tr}(y_j)$. □

In der Situation von Theorem 3.18 kann der Invariantenring R^ι auch ohne das Resultat aus Theorem 3.17 berechnet werden. Dies wird im Folgenden ausgeführt und ein Erzeugendensystem durch elementare Rechnung ermittelt. Zuvor ist es jedoch nützlich, die Elemente des Erzeugendensystems (3.7) genauer zu betrachten.

Definition 3.19. Für jede Teilmenge $\emptyset \neq M \subset \{1, \ldots, g\}$ definieren wir das homogene Polynom $f_M \in k[x_1, y_1, \ldots, x_g, y_g]$ durch

$$f_M = \sum_{d=0}^{|M|-1} \sum_{\substack{N \subset M, \\ |N|=d}} \prod_{m \in M \setminus N} x_m \prod_{n \in N} y_n, \tag{3.8}$$

d. h., die Menge M gibt an, welche Indizes auftreten, ihre Kardinalität $|M|$ ist der Totalgrad von f_M und d gibt den y-Totalgrad der Monome an.

Mit Ausnahme des Monoms $\prod_{i \in M} y_i$ tritt in f_M jedes Monom Q genau einmal auf, das homogen vom Grad $|M|$ ist, in dem nur Indizes aus M auftreten und das für jedes $i \in M$ die Gleichung

$$\deg_{x_i}(Q) + \deg_{y_i}(Q) = 1$$

erfüllt. Insbesondere sind diese Grade durch 1 beschränkt. Es folgt

$$f_M = \prod_{i \in M} (y_i + x_i) - \prod_{i \in M} y_i = \mathrm{Tr}\left(\prod_{i \in M} y_i \right),$$

da in der Spur genau die gleichen Monome auftreten. Also sind die Polynome f_M invariant unter der Involutionswirkung.

Durch Bilden der formalen partiellen Ableitung kann ein bestimmter Index $i \in M$ aus f_M eliminiert werden: Es ist leicht zu sehen, dass für $|M| \geq 2$ die Gleichheit

$$\frac{\partial f_M}{\partial y_i} = f_{M \setminus \{i\}} \tag{3.9}$$

gilt. Die partielle Ableitung ist null, wenn $i \notin M$. Diese Operation wird im Beweis für einen Induktionsschritt genutzt werden.

Alternativer Beweis von Theorem 3.18. Es sei $K = k(x_1, \ldots, x_g)$ der Körper der rationalen Funktionen in g Unbestimmten und weiter sei

$$B = K[y_1, \ldots, y_g] / (y_i^2 + x_i y_i + P_i(x_i), 1 \leq i \leq g),$$

versehen mit der K-linearen $\mathbb{Z}/2\mathbb{Z}$-Wirkung von $\iota\colon B \to B$, $\iota(y_i) = y_i + x_i$. Der Ring B ist als K-Vektorraum isomorph zum 2^g-dimensionalen Vektorraum

$$V = \{f \in K[y_1, \ldots y_g] \,|\, \deg_{y_i}(f) \leq 1 \text{ für alle } 1 \leq i \leq g\},$$

da jedes Element aus B einen eindeutigen Repräsentanten aus V besitzt (analog zum Beweis von Prop. 3.12). Wenn wir mit den ausgezeichneten Repräsentanten arbeiten, können wir ι nicht nur als K-Algebra-Automorphismus auffassen, sondern auch als lineare Abbildung $\iota\colon V \to V$. Der Grad des Repräsentanten bzgl. y_i wird durch ι nicht verändert und damit liegt insbesondere das Bild von ι wieder in V.

Es sei $v_1, \ldots, v_r \in V$ eine Basis von V^ι, dem Eigenraum zum Eigenwert 1 von ι. Wir fassen diese Vektoren als Elemente der K-Algebra B auf und betrachten die Elemente

$$v_1, \ldots, v_r,\ y_g v_1, \ldots, y_g v_r \in B. \tag{3.10}$$

Diese bzw. ihre Repräsentanten in V sind linear unabhängig. Um dies einzusehen, nehmen wir an, dass Skalare $\lambda_i, \mu_i \in K$ existieren, die die Bedingung

$$\mu_1 v_1 + \ldots + \mu_r v_r + \lambda_1 y_g v_1 + \ldots + \lambda_r y_g v_r \in \left(y_i^2 + x_i y_i + P_i(x_i), 1 \leq i \leq g\right)$$

in $K[y_1, \ldots, y_g]$ bzw. in B die Gleichung

$$0 = \mu_1 v_1 + \ldots + \mu_r v_r + \lambda_1 y_g v_1 + \ldots + \lambda_r y_g v_r \tag{3.11}$$

erfüllen. Durch Anwenden von ι auf beide Seiten der Gleichung erhält man

$$\begin{aligned} 0 &= \mu_1 v_1 + \ldots + \mu_r v_r + \lambda_1 (y_g + x_g) v_1 + \ldots + \lambda_r (y_g + x_g) v_r \\ &= \lambda_1 x_g v_1 + \ldots + \lambda_r x_g v_r \ + \underbrace{\mu_1 v_1 + \ldots + \mu_r v_r + \lambda_1 y_g v_1 + \ldots + \lambda_r y_g v_r}_{=0} \end{aligned}$$

und damit eine Linearkombination der Null, in der nur die Vektoren $v_1, \ldots, v_r$ auftreten. Da diese nach Voraussetzung linear unabhängig sind, müssen die Koeffizienten $x_g \lambda_i$ verschwinden, mithin gilt $\lambda_i = 0$ für $1 \leq i \leq r$. Mit gleichem Argument in (3.11) verschwinden nun auch die Koeffizienten $\mu_1, \ldots, \mu_r \in K$.

Wegen der linearen Unabhängigkeit der Vektoren aus (3.10) muss $r \leq 2^{g-1}$ gelten. Die umgekehrte Inklusion gilt ebenfalls: Dazu müssen 2^{g-1} linear unabhängige invariante Elemente von V gefunden werden. Mit diesen ist dann zugleich eine Basis von V^ι gefunden. Kandidat für ein solches System sind die Elemente der Form

$$f_{M\cup\{g\}} = \mathrm{Tr}\left(y_g \cdot \prod_{i\in M} y_i\right),$$

wobei $M \subset \{1,\ldots,g-1\}$ alle Teilmengen (diesmal einschließlich der leeren Menge) durchläuft. Wir beweisen die lineare Unabhängigkeit im Anschluss in Lemma 3.20.

Jedes invariante Element $f \in V$ kann also eindeutig als Linearkombination

$$f = \sum_{M\subset\{1,\ldots,g-1\}} \frac{\mu_{M\cup\{g\}}}{\nu_{M\cup\{g\}}} \cdot f_{M\cup\{g\}} \tag{3.12}$$

mit Polynomen $\mu_{M\cup\{g\}},\ \nu_{M\cup\{g\}} \in k[x_1,\ldots,x_g]$ geschrieben werden. Wir sind nun an dem Fall interessiert, in dem f aus $k[x_1,y_1,\ldots,x_g,y_g]$ stammt. Dabei ist es durchaus möglich, dass nicht-konstante Nenner auftreten. Es ist aber notwendig, dass in (3.12) nach Kürzen $\nu_{M\cup\{g\}} = 1$ oder $\nu_{M\cup\{g\}} = x_g$ erreicht werden kann: Wir wählen eine Menge M' mit maximaler Kardinalität, sodass der Koeffizient $\mu_{M'\cup\{g\}}$ nicht verschwindet. Dann ist $f_{M'\cup\{g\}}$ das einzige Basiselement in der Summe (3.12), das das Monom $x_g \cdot \prod_{i\in M'} y_i$ enthält, und folglich muss $\nu_{M'\cup\{g\}}$ ein Teiler von x_g sein. Dieses Argument können wir mit dem Element

$$f + \frac{\mu_{M'\cup\{g\}}}{\nu_{M'\cup\{g\}}} \cdot f_{M'\cup\{g\}}$$

anstelle von f wiederholen und erhalten sukzessiv die Nenner der weiteren Koeffizienten in der Darstellung (3.12).

Wir schreiben das invariante Polynom f als Summe von Polynomen $f = h_1 + h_2$, wobei

$$\begin{aligned} h_1 &= \sum_{M\subset\{1,\ldots,g-1\}} \mu_{M\cup\{g\}} \cdot f_{M\cup\{g\}} \quad \text{mit} \quad \mu_{M\cup\{g\}} \in k\left[x_1,\ldots,x_g\right], \\ h_2 &= \sum_{M\subset\{1,\ldots,g-1\}} \frac{\xi_{M\cup\{g\}}}{x_g} \cdot f_{M\cup\{g\}} \quad \text{mit} \quad \xi_{M\cup\{g\}} \in k\left[x_1,\ldots,x_{g-1}\right] \end{aligned}$$

bezeichnen. Alle nicht-konstanten Nenner werden also in einem Summanden zusammengefasst. Es wird nun das Polynom h_2 und seine formale partielle Ableitung nach y_g betrachtet. Es gilt

$$\frac{\partial h_2}{\partial y_g} = \frac{1}{x_g} \cdot \left(\sum_{M\subset\{1,\ldots,g-1\}} \xi_{M\cup\{g\}} \cdot \frac{\partial f_{M\cup\{g\}}}{\partial y_g}\right) = 0,$$

denn die Summanden in der Klammer enthalten als ausgeschriebene Polynome weder x_g noch y_g, wie aus (3.9) ersichtlich wird; entsprechend kann x_g nicht auf andere Art gekürzt werden. Die formale partielle Ableitung von h_2 kann so nur dann ein Polynom sein, wenn es sich dabei um das Nullpolynom handelt. Damit gelten $\deg_{y_g}(h_2) \leq 0$, da sonst die Ableitung nicht verschwinden würde, sowie $\deg_{x_g}(h_2) \leq 0$, da $\deg_{x_g}(f_{M\cup\{g\}}) = 1$ und durch x_g dividiert wird. Insgesamt ist daher

$$h_2 \in k\left[x_1, \ldots, x_{g-1}, y_1, \ldots, y_{g-1}\right] \cap V^\iota$$

gezeigt. Diese Reduktion auf den Fall von $g-1$ Paaren von Unbestimmten (x_i, y_i) können wir als Induktionsschritt verwenden.

Um den Beweis von Theorem 3.18 abzuschließen, ist dementsprechend noch der Induktionsanfang, also der Beweis für den Fall $g = 1$ zu erbringen. Es sei nun daher $g = 1$. Der Untervektorraum V^ι der invarianten Elemente ist nach obiger Betrachtung eindimensional, also identisch mit $K = k(x_1)$. Somit ist $R^\iota = k[x_1]$ der gesuchte Invariantenring, welcher von $x_1 = f_{\{1\}} = \mathrm{Tr}(y_1)$ als k-Algebra erzeugt wird. □

Lemma 3.20. *Die 2^{g-1} Elemente der Form $f_{M\cup\{g\}}$ mit $M \subset \{1, \ldots, g-1\}$ sind linear unabhängig über K.*

Beweis. Für jede Teilmenge $M \subset \{1, \ldots, g-1\}$ sei ein $\lambda_{M\cup\{g\}} \in K$ gegeben, sodass die Gleichung

$$\sum_M \lambda_{M\cup\{g\}} \cdot f_{M\cup\{g\}} = 0 \tag{3.13}$$

erfüllt ist. Wir nehmen an, dass nicht alle Koeffizienten in (3.13) verschwinden. In diesem Fall können wir eine Menge M' finden, für die $\lambda_{M'\cup\{g\}} \neq 0$ gilt und die mit dieser Eigenschaft maximal ist, d. h., es soll $|M'| \geq |M|$ für alle M mit $\lambda_{M\cup\{g\}} \neq 0$ erfüllt sein. Der Fall $M' = \emptyset$ kann nicht auftreten, da dies implizieren würde, dass genau ein Koeffizient nicht verschwindet. Wir schreiben $M' = \{i_1, \ldots, i_m\}$. Das Polynom $f_{M'\cup\{g\}}$ ist das einzige Polynom in obiger Linearkombination, das das Monom $y_{i_1} \cdots y_{i_m}$ enthält. Dieses kann in der Linearkombination nur wegfallen, wenn $\lambda_{M'\cup\{g\}} = 0$ gilt, im Widerspruch zur Wahl von M'. □

Korollar 3.21. *Jedes $f \in R^\iota$ kann in der Form*

$$f = \sum_{\substack{M\subset\{1,\ldots,g\}\\ M\neq\emptyset}} \lambda_M f_M \tag{3.14}$$

mit Polynomen $\lambda_M \in k\left[x_1, \ldots, x_g\right]$ geschrieben werden. Insbesondere ist R^ι ein endlicherzeugter $k[x_1, \ldots, x_g]$-Modul.

Beispiel 3.22. Für kleine Dimension g erhält man die folgenden Erzeuger von R^ι:

$$\begin{aligned} g=1: &\quad x_1 \\ g=2: &\quad x_1,\ \ x_2,\ \ x_1y_2+x_2y_1+x_1x_2 \\ g=3: &\quad x_1y_2y_3+x_2y_1y_3+x_3y_1y_2+x_2x_3y_1+x_1x_3y_2+x_1x_2y_3+x_1x_2x_3, \\ &\quad x_i,\ \ x_iy_j+x_jy_i+x_ix_j,\ \ 1\le i,j\le 3,\ i\neq j. \end{aligned}$$

Die Summanden x_ix_j können dabei auch weggelassen werden. Im Fall $g=2$ stimmen die gefundenen Erzeuger dann mit den in [31], Proposition 2.2, ermittelten invarianten Erzeugern überein. Den Fall $g=1$ können wir direkt als Ausdruck von $E/\iota=\mathbb{P}^1_k$ deuten, der Fall $g=0$ ist trivial.

Auf diesen Ergebnissen aufbauend, kann der Invariantenring R^ι auch für den Fall, dass in der ursprünglichen abelschen Varietät $A=E_1\times\ldots\times E_g$ supersinguläre Faktoren auftreten, angegeben werden:

Proposition 3.23. *Es gelten die Bezeichnungen aus* (3.5)*. Der Invariantenring R^ι wird als k-Algebra von den Elementen*

$$\begin{aligned} &v_{r+1},\ldots,v_g, \\ &f_{M\cup N}=\operatorname{Tr}\left(\prod_{i\in M}y_i\cdot\prod_{j\in N}w_j\right) \end{aligned}$$

erzeugt, wobei $M\subset\{1,\ldots,r\}$, $N\subset\{r+1,\ldots,g\}$ alle Teilmengen durchläuft.

Wegen $\operatorname{Tr}(w_j)=v_j^2$ können die invarianten Elemente v_j nicht als Spur ausgedrückt werden. Dies zeigt auch zugleich, dass das genannte Erzeugendensystem nicht minimal ist.

Beweis. Wir betrachten die k-Algebren

$$S_1=S,\quad S_2=k\left[x_1,y_1,\ldots,x_r,y_r,\,v_{r+1}^2,w_{r+1},\ldots,v_g^2,w_g\right]$$

und die k-Vektorräume

$$V_n=\{f\in S_n\mid \deg_{y_i}(f)\le 1,\ \deg_{w_j}(f)\le 1 \text{ für alle } 1\le i\le r<j\le g\}\subset S_n$$

mit der $\mathbb{Z}/2\mathbb{Z}$-Wirkung gegeben durch

$$\begin{aligned} \iota(x_i)&=x_i, \quad \iota(y_i)=y_i+x_i, \\ \iota(v_j^n)&=v_j^n, \quad \iota(w_j)=w_j+v_j^2. \end{aligned}$$

Nach Korollar 3.13 besitzt jedes Element von $R=S/I$ einen eindeutigen Repräsentanten in V_1. Es wird wie zuvor der Untervektorraum V_1^ι der invarianten Elemente bestimmt.

Dazu seien $f_1 \in V_1$ ein beliebiges Polynom und $L \subset \{r+1, \ldots, g\}$ eine Teilmenge. Wir bezeichnen mit $h_L \in V_1$ die Summe aller Monome Q von f_1, die die Bedingung

$$j \in L \iff \deg_{v_j}(Q) \equiv 1 \bmod 2$$

erfüllen. Das Polynom h_L ist also die Summe aller Monome von f_1, in denen die Unbestimmten v_j mit $j \in L$ mit ungeradem Exponenten auftreten, während die anderen v_i mit geradem Exponenten erscheinen. Wir können f_1 als Summe der h_L schreiben und erhalten

$$f_1 = \sum_L h_L = \sum_L \left(\prod_{j \in L} v_j \right) \tilde{h}_L$$

für geeignete Polynome $\tilde{h}_L \in V_2$. Da $\iota(V_2) = V_2$ und $\iota(v_j) = v_j$ gelten, ist $f_1 \in V_1$ genau dann invariant unter ι, wenn die Polynome $\tilde{h}_L \in V_2$ invariant sind. Wäre ein $\tilde{h}_L$ nicht invariant, könnte der Fehlerterm $\iota(\tilde{h}_L) - \tilde{h}_L$ nicht mehr ausgelöscht werden, da der Vorfaktor $\prod v_j$ nur einmal auftritt. Die Operation von ι auf V_2 ist dabei genau von der Form, für die in Theorem 3.18 die invarianten Elemente ermittelt wurden. Nach Korollar 3.21 kann jedes invariante Element $f_2 \in V_2^\iota$ in der Form

$$f_2 = \sum_{\substack{M \subset \{1,\ldots,r\} \\ N \subset \{r+1,\ldots,g\}}} \lambda_{M \cup N} \cdot f_{M \cup N}$$

mit Polynomen $\lambda_{M \cup N} \in k[x_1, \ldots, x_r, v_{r+1}^2, \ldots, v_g^2]$ geschrieben werden. Wir erinnern daran, dass die Elemente $x_i = f_{\{i\} \cup \emptyset}$ ebenfalls von der Form $f_{M \cup N}$ sind. Somit bilden die Polynome $f_{M \cup N}$ und v_j ein Erzeugendensystem der k-Algebra R^ι. □

3.2.3 Die Relationen zwischen den Erzeugern

Da es sich beim Invariantenring R^ι um eine endlich erzeugte k-Algebra handelt, von der ein Erzeugendensystem bekannt ist, stellt sich die Frage nach den Relationen zwischen diesen Erzeugern. Hierbei wird die folgende Notation verwendet:

Notation 3.24. Für Teilmengen $M \subset \{1, \ldots, r\}$ und $M' \subset \{r+1, \ldots, g\}$ seien

$$\begin{aligned} y_M = \prod_{i \in M} y_i\,, \quad & x_M = \prod_{i \in M} x_i\,, \\ w_{M'} = \prod_{i \in M'} w_i\,, \quad & v_{M'}^2 = \prod_{i \in M'} v_i^2, \\ P_{M \cup M'} = \prod_{i \in M \cup M'} P_i \quad & \text{für} \quad P_i \in k\left[x_1, \ldots x_r, v_{r+1}, \ldots, v_g\right]. \end{aligned}$$

Die Polynome $P_i \in k[x_i]$ waren bisher nur als Bestandteil der Weierstraß-Gleichungen der

gewöhnlichen elliptischen Kurven eingeführt. Für $i \in M'$ setzen wir $P_i = v_i$. Dadurch kann für gewöhnliche wie supersinguläre elliptische Kurven die Weierstraß-Gleichung als $\mathrm{N}(y_i) = P_i$ geschrieben werden. Leere Produkte erhalten wie üblich per Konvention den Wert 1.

Für die spezielle Gruppenoperation aus Theorem 3.17, eine lineare Operation auf dem Spektrum eines Polynomrings, sind die Relationen zwischen den Erzeugern des Invariantenrings im Allgemeinen unbekannt. Campbell und Wehlau konnten 2014 in [10] die Relationen für den Fall $p = 2$ bestimmen. Die Kandidaten für ein Erzeugendensystem sind durch die folgenden Identitäten gegeben ([10], Prop. 3.2, 3.4):

Lemma 3.25. *Es sei der Polynomring $S_K = K[x_1, y_1, \ldots, x_g, y_g]$ über einem Körper der Charakteristik $p = 2$ gegeben sowie die $\mathbb{Z}/2\mathbb{Z}$-Wirkung durch $\iota(x_i) = x_i$, $\iota(y_i) = y_i + x_i$ für $1 \leq i \leq g$. In S_K sind die folgenden Gleichungen erfüllt:*

$$(i) \quad \sum_{L \subsetneq A} x_{A \setminus L} \operatorname{Tr}(y_L) = 0, \tag{3.15}$$

$$(ii) \quad \operatorname{Tr}(y_A) \operatorname{Tr}(y_B) = \sum_{L \subsetneq A \cap B} x_{(A \cap B) \setminus L} \operatorname{N}(y_L) \operatorname{Tr}\left(y_{(A \cup B) \setminus L}\right) + \operatorname{N}(y_{A \cap B}) \sum_{M \subsetneq A \setminus B} x_{(A \setminus B) \setminus M} \operatorname{Tr}\left(y_{M \cup (B \setminus A)}\right), \tag{3.16}$$

dabei sind $A, B \subset \{1, \ldots, g\}$ beliebige Teilmengen.

Für die erste Gleichung, welche im Abstract des Artikels fehlerhaft wiedergegeben ist, wird der Beweis aus [10] gegeben. Für die zweite Gleichung wird ein kombinatorischer Beweis gegeben.

Beweis. (i): Mit (3.8) und der oben eingeführten Notation ergibt sich

$$\operatorname{Tr}(y_A) = \sum_{L \subsetneq A} x_{A \setminus L}\, y_L.$$

Da die Spur additiv ist, erhält man nach nochmaligem Anwenden

$$0 = \operatorname{Tr}(\operatorname{Tr}(y_A)) = \operatorname{Tr}\left(\sum_{L \subsetneq A} x_{A \setminus L}\, y_L\right) = \sum_{L \subsetneq A} x_{A \setminus L} \operatorname{Tr}(y_L).$$

(ii): Es sei $C = A \cap B$. Durch Ausmultiplizieren des Ausdrucks auf der linken Seite und der Produkte auf der rechten Seite erhält man Summen von Monomen der Form

$$\underbrace{y_{c_1}^2 \cdots y_{c_n}^2 \cdot y_{c_{n+1}} \cdots y_{c_{n+m}}}_{\text{Indizes aus } C} \cdot \underbrace{y_{a_1} \cdots y_{a_s}}_{\text{Indizes aus } A \setminus C} \cdot \underbrace{y_{b_1} \cdots y_{b_t}}_{\text{Indizes aus } B \setminus C} \tag{3.17}$$

mit $n, m, s, t \geq 0$ und paarweise verschiedenen Faktoren. Für jedes dieser Monome wird nun gezählt, wie oft es auf der linken und auf der rechten Seite der Gleichung (3.16) auftritt.

Wir zeigen zunächst, dass in jedem Monom dabei immer das gleiche Polynom in den x_i Teil des Koeffizienten ist, weshalb es nicht weiter berücksichtigt werden muss: Da für linke Seite und beide Summen auf der rechten Seite gilt, dass der Totalgrad bzgl. (x_i, y_i) den Wert 1 hat, wenn $i \notin C$ gilt, und im Fall $i \in C$ den Wert 2 besitzt, treten auch die gleichen Produkte der x_i als Koeffizienten auf.

Wir beginnen mit der ersten Summe in (3.16). Ist $|A \cup B| = n + m + s + t$, dann kann das Monom nicht auftreten, da nicht alle Indizes im Monom (3.17) auftreten können. Im Fall $|A \cup B| > n + m + s + t$ kann das Monom über die Teilmengen $L \subsetneq C$ mit

$$\{c_1, \ldots, c_n\} \subset L \subset \{c_1, \ldots, c_{n+m}\}$$

gezählt werden: Das Produkt $y_{c_1}^2 \cdots y_{c_n}^2$ kann ausschließlich aus $\mathrm{N}(y_L) = \prod (y^2 + xy)_L$, die Indizes a_i aus $A \setminus C$ und die b_i aus $B \setminus C$ stammen; es kann aber variieren, ob die Indizes $c_{n+1}, \ldots, c_{n+m}$ von $\mathrm{N}(y_L)$ oder $\mathrm{Tr}(y_{(A \cup B) \setminus L})$ stammen. Jede solche Menge $L \subsetneq C$ sorgt somit für genau ein Auftreten des betrachteten Monoms. Wenn $\{c_1, \ldots, c_{n+m}\} \subsetneq C$ gilt, existieren 2^m Möglichkeiten, im Fall $\{c_1, \ldots, c_{n+m}\} = C$ gibt es $2^m - 1$ Wahlen von $L \subsetneq C$.

In der zweiten Summe kann das Monom (3.17) nur auftreten, wenn $C = \{c_1, \ldots, c_{n+m}\}$ gilt, da durch den Vorfaktor $\mathrm{N}(y_C)$ jeder Index aus C auftreten muss. Ist dies der Fall und ist weiterhin $A \setminus C = \{a_1, \ldots, a_s\}$ erfüllt, kann das Monom ebenfalls nicht auftreten, da mindestens ein Index aus $A \setminus C$ nicht auftritt. Im Fall $C = \{c_1, \ldots, c_{n+m}\}$ und $\{a_1, \ldots, a_s\} \subsetneq A \setminus C$ werden die Mengen M mit

$$\{a_1, \ldots, a_s\} \subset M \subsetneq A \setminus C$$

betrachtet. Es gibt $2^{|A \setminus C| - s} - 1$ viele solcher Mengen. Gilt $\{b_1, \ldots, b_t\} \subsetneq B \setminus C$, dann tritt das Monom (3.17) für jede dieser Mengen M genau einmal auf. Ist $B \setminus C = \{b_1, \ldots, b_t\}$, so muss $M = \{a_1, \ldots, a_s\}$ ausgeschlossen werden, da in diesem Fall $\mathrm{Tr}(y_{M \cup (B \setminus C)})$ bzgl. y-Graduierung zu kleinen Grad besitzt.

Das Monom (3.17) tritt in der linken Seite von (3.16) als Produkt der Form

$$\left(y_{\{c_1, \ldots, c_n\}} \cdot y_{\{a_1, \ldots, a_s\}} \cdot y_M\right) \cdot \left(y_{\{c_1, \ldots, c_n\}} \cdot y_{\{b_1, \ldots, b_t\}} \cdot y_{\{c_{n+1}, \ldots, c_{n+m}\} \setminus M}\right)$$

für $M \subset \{c_{n+1}, \ldots, c_{n+m}\}$ auf, wobei die Fälle ausgeschlossen werden müssen, in denen einer der beiden Faktoren mit y_A bzw. y_B übereinstimmt. (Es gilt $\deg_y(\mathrm{Tr}(y_A)) < |A|$.) Dies kann nur passieren, wenn bereits alle Indizes aus A oder B im Produkt (3.17) auftreten.

Die folgende Tabelle fasst die gerade betrachteten Fälle zusammen.

Auftreten des Monoms (3.17)	in linker Seite:	in rechter Seite:
$\lvert C\rvert > n+m,\ \lvert A\setminus C\rvert > s, \lvert B\setminus C\rvert > t$	2^m	$2^m + 0$
$\lvert C\rvert > n+m,\ \lvert A\setminus C\rvert > s, \lvert B\setminus C\rvert = t$	2^m	$2^m + 0$
$\lvert C\rvert > n+m,\ \lvert A\setminus C\rvert = s, \lvert B\setminus C\rvert > t$	2^m	$2^m + 0$
$\lvert C\rvert > n+m,\ \lvert A\setminus C\rvert = s, \lvert B\setminus C\rvert = t$	2^m	$2^m + 0$
$\lvert C\rvert = n+m,\ \lvert A\setminus C\rvert > s, \lvert B\setminus C\rvert > t$	2^m	$2^m - 1 + 2^{\lvert A\setminus C\rvert - s} - 1$
$\lvert C\rvert = n+m,\ \lvert A\setminus C\rvert > s, \lvert B\setminus C\rvert = t$	$2^m - 1$	$2^m - 1 + 2^{\lvert A\setminus C\rvert - s} - 2$
$\lvert C\rvert = n+m,\ \lvert A\setminus C\rvert = s, \lvert B\setminus C\rvert > t$	$2^m - 1$	$2^m - 1 + 0$
$\lvert C\rvert = n+m,\ \lvert A\setminus C\rvert = s, \lvert B\setminus C\rvert = t$	$\max\{2^m - 2, 0\}$	$0 + 0$

Damit treten auf beiden Seiten von (3.16) alle Summanden modulo 2 gleich oft auf. □

Die nachgewiesenen Relationen erzeugen nach [10], Theorem 3.6, tatsächlich alle Relationen zwischen den Erzeugern des Invariantenrings. Wir verwenden im Folgenden Notation 3.24 auch für die Unbestimmten X_i, V_j, N_i, es gilt also z. B. $X_M = \prod_{i\in M} X_i$. Für die Unbestimmten T_M gilt diese Notation nicht!

Proposition 3.26. *Es gelten die Voraussetzungen aus Lemma 3.25. Weiter sei*

$$S_0 = K\left[T_M, N_i, X_i \mid M \subset \{1,\dots,n\},\, i = 1,\dots,g\right]$$

Polynomring in $2^g + 2g$ Unbestimmten. Es sei $\phi\colon S_0 \to S_K^\iota$ der Homomorphismus von K-Algebren, welcher durch die Festlegung $\phi(T_M) = \mathrm{Tr}(y_M)$, $\phi(N_i) = \mathrm{N}(y_i)$, $\phi(X_i) = x_i$ gegeben ist. Der Kern von ϕ wird erzeugt von den Elementen

$$T_\emptyset, \quad X_i - T_{\{i\}}, \tag{3.18}$$

$$\sum_{L\subsetneq D} X_{D\setminus L}\, T_L, \tag{3.19}$$

$$T_A T_B + \sum_{L\subsetneq A\cap B} X_{(A\cap B)\setminus L}\ N_L\ T_{(A\cup B)\setminus L} + N_{A\cap B} \sum_{M\subsetneq A\setminus B} X_{(A\setminus B)\setminus M}\ T_{M\cup(B\setminus A)} \tag{3.20}$$

für $1 \le i \le g$, $A, B, D \subset \{1,\dots,g\}$ sodass $\lvert A\rvert, \lvert B\rvert \ge 2$, $\lvert D\rvert \ge 3$. Wählt man zu A, B nur eine der Relationen von Typ (3.20)*, so bilden diese Elemente zusammen mit den Elementen von Typ* (3.19) *und* (3.18) *ein minimales Erzeugendensystem von* $\ker(\phi)$.

Der Homomorphismus ϕ ist nach Theorem 3.17 surjektiv. Die Unbestimmten X_i sind de facto überflüssig, sie ermöglichen aber eine leichtere Notation, da Produkte von Elementen der Form $\mathrm{Tr}(y_i)$ in der obigen Notation sonst nicht durch Mengen als Index abgekürzt werden können. Ebenso wird $T_\emptyset$ nur für die Darstellung der Elemente (3.19) und (3.20) benötigt.

Die Relationen aus Lemma 3.25 können für den Invariantenring R^ι leicht angepasst

werden: Man erhält für $A, B, D \subset \{1, \dots, g\}$ die entsprechenden Relationen

$$(i) \quad \sum_{L \subsetneq D} x_{D' \setminus L'} \, v^2_{D'' \setminus L''} \, \mathrm{Tr}\,(y_{L'} w_{L''}) = 0,$$

$$\begin{aligned}(ii) \quad & \mathrm{Tr}\,(y_{A'} w_{A''}) \, \mathrm{Tr}\,(y_{B'} w_{B''}) \\ & = \sum_{L \subsetneq A \cap B} x_{(A' \cap B') \setminus L'} \; v^2_{(A'' \cap B'') \setminus L''} \; \mathrm{N}\,(y_{L'} w_{L''}) \; \mathrm{Tr}\left(y_{(A' \cup B') \setminus L'} \; w_{(A'' \cup B'') \setminus L''}\right) \\ & \quad + \mathrm{N}\,(y_{A' \cap B'} \; w_{A'' \cap B''}) \sum_{M \subsetneq A \setminus B} x_{(A' \setminus B') \setminus M'} \; v^2_{(A'' \setminus B'') \setminus M''} \; \mathrm{Tr}\left(y_{M' \cup (B' \setminus A')} \; w_{M'' \cup (B'' \setminus A'')}\right),\end{aligned}$$

wobei zu jeder Teilmenge $M \subset \{1, \dots, g\}$ die Mengen M' und M'' durch

$$M' = M \cap \{1, \dots, r\}, \qquad M'' = M \cap \{r+1, \dots, g\}$$

definiert sind. Da die Norm N multiplikativ ist, können die Gleichungen weiter vereinfacht werden durch

$$\begin{aligned}\mathrm{N}\,(y_{L'} w_{L''}) &= \mathrm{N}\,(y)_{L'} \cdot \; \mathrm{N}\,(w)_{L''} = P_{L'} \cdot \; P_{L''} = P_L, \\ \mathrm{N}\,(y_{A' \cap B'} \; w_{A'' \cap B''}) &= P_{A' \cap B'} \cdot \; P_{A'' \cap B''} = P_{A \cap B}.\end{aligned}$$

Die Polynome P_i waren dabei abhängig von den Weierstraß-Gleichungen der elliptischen Kurven definiert durch $P_i = \gamma_i x_i^3 + \delta_i x_i$ für $i \in M'$ und $P_j = v_j$ für $j \in M''$. Diese Normen können also als Polynome in den Unbestimmten x_i und v_j aufgefasst werden.

Wir übertragen nun Proposition 3.26 auf den Ring R^ι.

Proposition 3.27. *Wir benutzen die Benennung aus* (3.5) *sowie Notation 3.24. Weiter betrachten wir den Ring*

$$R_0 = k\left[T_M, X_i, V_j \mid M \subset \{1, \dots, g\}, \; i = 1, \dots, r, \; j = r+1, \dots, g\right].$$

In dieser Situation ist der Homomorphismus von k-Algebren $\psi\colon R_0 \to R^\iota$, der durch $T_M \mapsto \mathrm{Tr}(y_{M'} \, w_{M''})$, $X_i \mapsto x_i$, $V_j \mapsto v_j$ gegeben ist, surjektiv und der Kern $J = \ker(\psi)$ wird erzeugt von den Elementen

$$T_\emptyset\,, \quad X_i - T_{\{i\}}\,, \quad V_j^2 - T_{\{j\}}\,, \tag{3.21}$$

$$\sum_{L \subsetneq D} X_{D' \setminus L'} \, V^2_{D'' \setminus L''} \, T_L, \tag{3.22}$$

$$\begin{aligned}T_A T_B + & \sum_{L \subsetneq A \cap B} X_{(A' \cap B') \setminus L'} \, V^2_{(A'' \cap B'') \setminus L''} \; P_L \; T_{(A \cup B) \setminus L} \\ & + P_{A \cap B} \sum_{M \subsetneq A \setminus B} X_{(A' \setminus B') \setminus M'} \, V^2_{(A'' \setminus B'') \setminus M''} \; T_{M \cup (B \setminus A)}\end{aligned} \tag{3.23}$$

für $1 \le i \le r < j \le g$, $A, B, D \subset \{1, \dots, g\}$ mit $|A|, |B| \ge 2$, $|D| \ge 3$.

Beweis. Der Homomorphismus ψ ist surjektiv, da ein Erzeugendensystem von R^ι im Bild liegt. Es sei J das von den Elementen der Form (3.21)-(3.23) erzeugte Ideal. Die Relationen aus J liegen im Kern von ψ. Es sei $\bar{R} = R_0/J$. Wir zeigen, dass ψ einen Isomorphismus $\bar{\psi}\colon \bar{R} \cong R^\iota$ induziert, womit die Aussage bewiesen ist.

Es sei $\bar{Q} \in \ker(\bar{\psi})$, d. h., $\bar{Q}$ ist die Restklasse eines Polynoms in $\bar{R}$, das in R^ι durch Einsetzen der Erzeuger zu null wird. Mit den Relationen vom Typ (3.23) können wir einen Repräsentanten Q_0 von $\bar{Q}$ im Polynomring R_0 finden, sodass die Bedingung $\deg_{T_M}(Q_0) \leq 1$ für alle Unbestimmten der Form T_M mit $|M| \geq 2$ gilt. (Im Fall $|M| = 1$ wird T_M mit einem Element X_i oder V_j identifiziert, $T_\emptyset$ ist trivial.) Somit gibt Q_0 in R^ι eine Relation der Form

$$\sum_{|M|\geq 2} \mu_M \operatorname{Tr}(y_{M'} w_{M''}) \;=\; 0$$

für geeignete Polynome $\mu_M \in k[x_1, \ldots, x_r, v_{r+1}, \ldots v_g]$. Diese Relation gilt offensichtlich auch in R. Nach Korollar 3.13 gilt sie aber auch in $S = S_k$ aus Lemma 3.25. Da in der Relation nur invariante Polynome auftreten, gilt sie auch in S^ι. Damit ist Q_0 eine Relation zwischen den Erzeugern des Invariantenrings S^ι und liegt daher im Ideal $\ker(\phi)$ aus Proposition 3.26. Die Restklasse $\bar{Q}$ ist folglich trivial in

$$S_0/(\ker(\phi) + (N_i + P_i,\, 1 \leq i \leq g)) \cong R_0/J = \bar{R},$$

also ist $\bar{\psi}$ ein Isomorphismus. □

Die vervollständigten lokalen Ringe der Singularitäten können direkt aus der Proposition abgelesen werden:

Korollar 3.28. *Es seien X eine wilde n-dimensionale Kummer-Varietät, die von einem Produkt elliptischer Kurven stammt, und $x \in X$ ein singulärer Punkt. Dann gilt*

$$\hat{\mathcal{O}}_{X,x} \cong k[\![T_M, X_i, V_j \mid M \subset \{1, \ldots, g\},\ i = 1, \ldots, r,\ j = r+1, \ldots, g]\!]/J,$$

wobei r die Anzahl der gewöhnlichen Faktoren im Produkt bezeichnet und das Ideal J die gleichen Erzeuger wie in Proposition 3.27 besitzt.

Es schließen Bemerkungen zur Cohen–Macaulay- und zur Vollständiger-Durchschnitt-Eigenschaft von $\hat{R}^\iota$ an.

Bemerkung 3.29. Von Invariantenringen bzgl. wilder Gruppenwirkung ist bekannt, dass sie fast nie Cohen–Macaulay-Ringe sind: In [18], Propositionen 2 und 4, wird gezeigt, dass der Invariantenring A^G die Tiefe $\operatorname{depth}(A^G) = 2$ besitzt, wenn A, A^G noethersche, integre lokale k-Algebren bezeichnet, $\dim(A) \geq 2$ gilt, A ein endlich erzeugter A^G-Modul ist und die G-Wirkung frei außer am maximalen Ideal ist. Dies ist hier gegeben. Insbesondere ist $\hat{R}^\iota$ genau dann ein Cohen–Macaulay-Ring, wenn $g \leq 2$ gilt.

Für lineare Gruppenwirkung auf Polynomringen stimmt die Tiefe ebenfalls selten mit der Dimension überein: Es seien V ein endlich-dimensionaler k-Vektorraum mit einer linearen Wirkung von $G = \mathbb{Z}/p^n\mathbb{Z}$ und $\mathbb{V}$ das assoziierte affine Schema. Für jedes $x \in \mathbb{V}/G$, das Bildpunkt eines Elements von V^G ist, hat der lokale Ring nach [17], Théorèm 3.1, die Tiefe $\operatorname{depth}(\mathscr{O}_{\mathbb{V}/G,x}) = \min\{2 + \dim_k(V^G), \dim_k(V)\}$.

Als vollständiger lokaler noetherscher Ring ist $\hat{R}^\iota$ ein *Kettenring* ([8], Cor. 2.1.13), d. h., alle nicht verfeinerbaren Primidealketten mit vorgegebenem Anfang und Ende haben die gleiche Länge.

Bemerkung 3.30. Es sei R^ι wie oben der Invariantenring, den man von einem Produkt von g gewöhnlichen elliptischen Kurven erhält. Die Elemente $X_1, \ldots, X_g$ bilden keine reguläre Folge, wenn $g \geq 3$ gilt. Sie erfüllen aber die Bedingung (1.8), die für Cohen–Macaulay-Ringe reguläre Folgen charakterisiert. Im Faktorring $R^\iota/(X_1, \ldots, X_i)$ sind die Elemente T_M mit $\{1, \ldots, i\} \cap M \neq \emptyset$ nilpotent. So ist etwa $T^2_{\{1,j\}} = 0$. Weiter ist $T^2_{\{1,j_1,\ldots,j_l\}}$ eine Summe von Elementen der Form $T_{\{1,m_1,\ldots,m_{l-1}\}}$. Sukzessives Quadrieren wird daher zur Auslöschung führen. Man kann diese nilpotenten Elemente herausteilen, ohne dass sich die Krull-Dimension ändert, und erhält dadurch den Invariantenring eines Produkts von $g - i$ elliptischen Kurven, der integer ist. Also ist auch das Spektrum von $R^\iota/(X_1, \ldots, X_i)$ irreduzibel.

Bemerkung 3.31. Im Fall $g \leq 2$ ist $\hat{R}^\iota$ ein vollständiger Durchschnitt, da er entweder regulär ist ($g \leq 1$) oder der Quotient eines Potenzreihenrings nach einem echten Hauptideal ($g = 2$). Nach der Berechnung der Invariantenringe in [2] gilt dies auch für die Singularitäten beliebiger Kummer-Flächen. Ist $g \geq 3$, so ist $\hat{R}^\iota$ nie ein vollständiger Durchschnitt, da bereits die Cohen–Macaulay-Eigenschaft verletzt ist. Auch dies gilt nicht nur für den Fall von Produkten elliptischer Kurven, sondern für die Singularitäten beliebiger Kummer-Varietäten der Dimension $g \geq 3$. Die Frage, ob der Invariantenring ein vollständiger Durchschnitt ist, hat folglich in den beiden Fällen $\operatorname{char}(k) = 2$ und $\operatorname{char}(k) \neq 2$ die gleiche Antwort.

Wir betrachten noch einmal den Polynomring $S = k[x_1, y_1, \ldots, x_g, y_g]$ mit Involutionswirkung von ι. Für ein Ideal $\mathfrak{a} \subset S^\iota$ bezeichne $\mathfrak{a}^e \subset S$ das von $\mathfrak{a}$ in S erzeugte Ideal. Für ein Ideal $\mathfrak{b} \subset S$ sei $\mathfrak{b}^c = \mathfrak{b} \cap S^\iota$. Für treu-flache Ringerweiterungen ist bekannt, dass stets $(\mathfrak{a}^e)^c = \mathfrak{a}$ gilt (z. B. [39], Thm. 7.5). Die Ringerweiterung $S^\iota \subset S$ aus Lemma 3.25 ist jedoch im Allgemeinen nicht flach: Wenn S eine flache S^ι-Algebra wäre, würde man durch Lokalisieren einen flachen Ringhomomorphismus von lokalen Ringen $S^\iota_{\mathfrak{m}} \to S_{\mathfrak{n}}$ erhalten. Hier bezeichne $\mathfrak{n}$ das von den Unbestimmten erzeugte maximale Ideal in S und $\mathfrak{m} = \mathfrak{n} \cap S^\iota$. Der lokale Ring $S_{\mathfrak{n}}$ wäre regulär, insbesondere ein Cohen–Macaulay-Ring, sowie eine flache $S^\iota_{\mathfrak{m}}$-Algebra. Aus Proposition 1.51 ist jedoch bekannt, dass dann auch $S^\iota_{\mathfrak{m}}$ regulär sein und die Cohen–Macaulay-Eigenschaft besitzen müsste (alle Bedingungen R_n und S_n von Serre übertragen sich auf den Invariantenring). Dies ist fast nie der Fall.

Die Gleichheit $(\mathfrak{a}^e)^c = \mathfrak{a}$ ist zumindest für das Ideal $\mathfrak{a}_g = \sum_{i=1}^{g}(y_i^2 + x_i y_i + P_i(x_i))S^\iota$ gültig. Dies lässt sich für eine Primidealkette verallgemeinern:

Proposition 3.32. *Es seien S bzw. S^ι wie oben und $\hat{S}$ bzw. $\hat{S}^\iota$ die Vervollständigungen am Ursprung. Wir betrachten die Primideale $\mathfrak{p}_\nu = \sum_{i=1}^{\nu}(y_i^2 + x_i y_i + P_i(x_i))\hat{S}$ in $\hat{S}$ für $\nu = 1, \ldots, g$. Weiter bezeichne $\mathfrak{a}_\nu = \sum_{i=1}^{\nu}(y_i^2 + x_i y_i + P_i(x_i))\hat{S}^\iota$ das in $\hat{S}^\iota$ vom gleichen Erzeugendensystem erzeugte Ideal. Dann gilt $\mathfrak{p}_\nu \cap \hat{S}^\iota = \mathfrak{a}_\nu$, man erhält also die Ketten*

$$\begin{array}{ccccccccc} 0 = \mathfrak{p}_0 & \subset & \mathfrak{p}_1 & \subset & \ldots & \subset & \mathfrak{p}_g & \subset \hat{S} \\ & & \downarrow & & & & \downarrow & \\ 0 = \mathfrak{a}_0 & \subset & \mathfrak{a}_1 & \subset & \ldots & \subset & \mathfrak{a}_g & \subset \hat{S}^\iota \end{array}$$

von übereinander liegenden Primidealen.

Der Grund dafür, dass die Aussage für die vervollständigten Ringe getroffen wird, ist die Anwendung des Durchschnittsatzes von Krull (Cor. 5.4 in [16]), für die ein lokaler oder ein integrer Ring vorausgesetzt wird. Im Beweis tritt ein Faktorring auf, von dem a priori nicht bekannt ist, ob er integer ist.

Beweis. Die Aussage wird mit einem Induktionsbeweis gezeigt. Der Fall $\nu = g$ folgt aus dem Beweis von Proposition 3.27: Mit der dort bewiesenen Isomorphie ergibt sich

$$\hat{S}^\iota/\mathfrak{a}_g \cong \hat{S}_0/(\ker(\phi) + \mathfrak{a}_g) \cong \hat{R}^\iota,$$

also ist $\mathfrak{a}_g$ ein Primideal, weiterhin ist $\mathfrak{a}_g$ im Primideal $\mathfrak{p}_g \cap \hat{S}^\iota$ enthalten. Wäre die Inklusion strikt, dann müsste nach *going down* ein echt kleineres Primideal $\mathfrak{p} \subset \mathfrak{p}_g$ existieren, das über $\mathfrak{a}_g$ liegt, aber die Erzeuger von $\mathfrak{p}_g$ enthält. Somit sind die Ideale gleich.

Wir nehmen nun an, dass $\mathfrak{p}_\nu \cap \hat{S}^\iota = \mathfrak{a}_\nu$ für alle $\nu > n$, $n < g$, erfüllt ist und zeigen $\mathfrak{p}_n \cap \hat{S}^\iota = \mathfrak{a}_n$. Die Inklusion „$\supset$“ ist trivial. Für die andere Inklusion sei $f \in \mathfrak{p}_n \cap \hat{S}^\iota$. Insbesondere liegt f in $\mathfrak{p}_{n+1} \cap \hat{S}^\iota = \mathfrak{a}_{n+1}$, also können wir

$$f = f_n^{(0)} + f_{n+1}^{(0)}\left(y_{n+1}^2 + x_{n+1}y_{n+1} + P_{n+1}(x_{n+1})\right)$$

mit $f_n^{(0)} \in \mathfrak{a}_n$ und $f_{n+1}^{(0)} \in \hat{S}^\iota$ schreiben. Folglich ist auch die Differenz $f - f_n^{(0)}$ in $\mathfrak{p}_n$ enthalten, was – da $\mathfrak{p}_n \subset \hat{S}$ ein Primideal ist – nur sein kann, wenn $f_{n+1}^{(0)}$ in $\mathfrak{p}_n$ enthalten ist. Wir können nun mit $f_{n+1}^{(0)}$ statt f von vorne beginnen und wiederum eine Zerlegung in Summanden $f_n^{(1)} \in \mathfrak{a}_n$ und $f_{n+1}^{(1)} \in \mathfrak{p}_n \cap \hat{S}^\iota$ erhalten. Mit $Q = y_{n+1}^2 + x_{n+1}y_{n+1} + P_{n+1}(x_{n+1})$ ergibt sich für f die Darstellung

$$\begin{aligned} f &= f_n^{(0)} + Q \cdot \left(f_n^{(1)} + Q \cdot \left(f_n^{(2)} + Q \cdot (\ldots)\right)\right) \\ &= f_n^{(0)} + Q f_n^{(1)} + Q^2 f_n^{(2)} + \ldots + Q^m f_n^{(m)} + Q^{m+1} f_{n+1}^{(m)} \end{aligned}$$

und folglich gilt die Inklusionskette

$$\mathfrak{a}_n \subset \mathfrak{p}_n \cap \hat{S}^\iota \subset \bigcap_{m\in\mathbb{N}} (\mathfrak{a}_n + Q^m).$$

Im Faktorring $\hat{S}^\iota/\mathfrak{a}_n$ gilt $\bigcap_{m\in\mathbb{N}}(\mathfrak{a}_n + Q^m) = 0$ nach dem Durchschnittsatz von Krull, was die Gleichheit der Ideale zeigt. □

Nachdem ein Erzeugendensystem des Invariantenrings R^ι bekannt ist, stellt sich nun auch die Frage nach einem *minimalen* Erzeugendensystem und nach der Einbettungsdimension von $\hat{R}^\iota$, der Vervollständigung des Invariantenrings am Ursprung.

Proposition 3.33. *Ein minimales Erzeugendensystem der k-Algebra R^ι ist durch die Elemente*

$$x_1, \ldots, x_r,\, v_{r+1}, \ldots, v_g,\;\; f_M = \mathrm{Tr}(y_{M'}\, w_{M''}) \;\; \text{mit } |M| \geq 2$$

gegeben, wobei $M \subset \{1, \ldots, g\}$ bezeichnet. Die Einbettungsdimension von $\hat{R}^\iota$ beträgt daher $2^g - 1$.

Beweis. Es bezeichne $\mathfrak{m} \subset \hat{R}^\iota$ das maximale Ideal, welches von den Bildern der Erzeuger von R^ι in der Vervollständigung erzeugt wird. Wenn die Aussage über die Einbettungsdimension bewiesen ist, folgt auch die Minimalität des Erzeugendensystems von R^ι: Wir nehmen an, es gäbe ein weiteres Erzeugendensystem $a_1, \ldots, a_d$ der k-Algebra R^ι mit $d < 2^g - 1$. Diese Elemente sind Polynome in den Unbestimmten x_i, y_i, v_j, w_j und wir können ohne Einschränkung annehmen, dass sie keinen konstanten Term besitzen. Damit ist $(a_1, \ldots, a_d)$ das maximale Ideal zum singulären Punkt von $\mathrm{Spec}(R^\iota)$ und wir haben ein Erzeugendensystem von $\mathfrak{m}$ mit weniger als $2^g - 1$ Elementen gefunden, was im Widerspruch zur Einbettungsdimension steht. Um die Einbettungsdimension zu berechnen, zeigen wir, dass die Elemente der Form x_i, v_j, f_M linear unabhängig im Kotangentialraum $\mathfrak{m}/\mathfrak{m}^2$ sind. Dieser besitzt als k-Vektorraum höchstens die Dimension $2^g - 1$, da die Restklassen eines minimalen Erzeugendensystems von $\mathfrak{m}$ eine Vektorraumbasis bilden. Durch den Nachweis der linearen Unabhängigkeit der genannten Elemente folgt die Aussage.

Wir ersetzen $\hat{R}^\iota$ durch die Vervollständigung des Rings $R_0/\ker(\psi)$ aus Proposition 3.27. Anstatt im k-Vektorraum $\mathfrak{m}/\mathfrak{m}^2$ eine Linearkombination des Nullvektors hinzuschreiben, können wir auch äquivalent dazu fordern, dass im Ring $\hat{R}^\iota$ die Beziehung

$$\sum_{i=1}^{r} \lambda_i\, X_i \;+\; \sum_{i=r+1}^{g} \lambda_i\, V_i \;+\; \sum_{|M|\geq 2} \mu_M\, T_M \in \mathfrak{m}^2 \tag{3.24}$$

für geeignete Koeffizienten $\lambda_i, \mu_M \in k$ erfüllt ist. Es sei etwa $f \in \mathfrak{m}^2$ dieses Element. Das Ideal $\mathfrak{m}^2 \subset \hat{R}^\iota$ wird von Produkten von je zwei Elementen des bekannten Erzeugendensystems erzeugt. Die Relationen der Form (3.23) zeigen, dass jedes dieser Produkte im Ideal

$\mathfrak{a} = (X_1, \ldots, X_r, V_{r+1}, \ldots V_g) \subset \hat{R}^\iota$ enthalten ist; folglich ist auch $f \in \mathfrak{a}$. Der Faktorring $\hat{R}^\iota/\mathfrak{a}$ kann auch als

$$\hat{R}^\iota/\mathfrak{a} = k[\![\, T_M \,|\, M \subset \{1, \ldots, g\}, |M| \geq 2]\!]/(T_A \cdot T_B,\ |A|, |B| \geq 2)$$

geschrieben werden, indem in den Relationen aus Proposition 3.27 die Unbestimmten X_i, V_j eliminiert werden. Durch Reduktion der Linearkombination (3.24) modulo $\mathfrak{a}$ erhalten wir daher

$$\sum_{|M|\geq 2} \mu_M T_M = 0 \in \hat{R}^\iota/\mathfrak{a},$$
$$\text{bzw.} \quad \sum_{|M|\geq 2} \mu_M T_M \in (T_A \cdot T_B,\, |A|, |B| \geq 2) \subset k[\![\, T_M \mid |M| \geq 2]\!],$$

was nur erfüllt sein kann, wenn alle Koeffizienten μ_M verschwinden. Mit den Koeffizienten λ_i kann ähnlich verfahren werden: Dazu sei $\mathfrak{b} = (T_M,\, |M| \geq 2) \subset \hat{R}^\iota$. Reduziert man (3.24) modulo $\mathfrak{b} + \mathfrak{m}^2$, so ergibt sich

$$\sum_{i=1}^{r} \lambda_i X_i \ + \ \sum_{i=r+1}^{n} \lambda_i V_i \ = 0 \in \hat{R}^\iota/(\mathfrak{b} + \mathfrak{m}^2),$$

wobei der Faktorring auf der rechten Seite als

$$k[\![X_1, \ldots, X_r, V_{r+1}, \ldots, V_g]\!]/\left(X_i X_{i'}, X_i V_j, V_j V_{j'},\, 1 \leq i, i' \leq r < j, j' \leq g\right)$$

geschrieben werden kann. Dies ist wieder nur möglich, wenn alle Koeffizienten λ_i verschwinden. Damit ist die Trivialität der Linearkombination bewiesen. □

Bei wilden Kummer-Flächen besitzen die Singularitäten in jedem Fall die Einbettungsdimension $\operatorname{edim}(\hat{\mathscr{O}}_{A/\iota,e}) = 3$. Ein analoges Resultat in höherer Dimension ist nicht bekannt.

Frage 3.34. Wenn X eine wilde Kummer-Varietät der Dimension g bezeichnet und $x \in X$ ein singulärer Punkt ist, gilt dann $\operatorname{edim}(\hat{\mathscr{O}}_{X,x}) = 2^g - 1$?

Wir werden in Abschnitt 3.4 sehen, dass dies auch auf Kummer-Varietäten von beliebigen gewöhnlichen abelschen Varietäten zutrifft.

3.3 Beispiele

Es werden nun einige Beispiele für kleine Dimension g der Kummer-Varietät gegeben. Jeder der folgenden Ringe ist der affine Koordinatenring eines offenen affinen Unterschemas einer g-dimensionalen Kummer-Varietät, das genau einen singulären Punkt (nämlich am Ursprung) enthält. Solche offenen Umgebungen scheinen bislang kaum betrachtet worden zu sein.

Wenn nicht explizit anders angegeben, setzen wir in diesem Abschnitt k als algebraisch abgeschlossenen Grundkörper der Charakteristik $p = 2$ voraus.

3.3.1 Flächen und Dreifaltigkeiten

Wir beginnen mit Kummer-Flächen ($g = 2$), die von Produkten elliptischer Kurven herrühren.

Beispiel 3.35. Man erhält die folgenden Koordinatenringe einer offenen Umgebung eines singulären Punktes, abhängig von der Anzahl r der gewöhnlichen Faktoren im Produkt $A = E_1 \times E_2$:

$$\begin{aligned}
R_2 &= k[X_1, X_2, T]/\left(T^2 + X_1X_2T + X_1^2P_2(X_2) + X_2^2P_1(X_1)\right), && \text{wenn } r = 2,\\
R_1 &= k[X_1, V_2, T]/\left(T^2 + X_1V_2^2T + X_1^2V_2 + V_2^4P_1(X_1)\right), && \text{wenn } r = 1,\\
R_0 &= k[V_1, V_2, T]/\left(T^2 + V_1^2V_2^2T + V_1^4V_2 + V_2^4V_1\right), && \text{wenn } r = 0.
\end{aligned}$$

Die definierenden Gleichungen der Flächensingularitäten können in den ersten beiden Fällen nach Koordinatenwechsel mit den Normalformen in Tabelle 1 abgeglichen werden: Dazu sei daran erinnert, dass die Polynome P_i von der Form $P_i(X_i) = X_i \cdot U_i(X_i)$ mit $U_i(X_i) = \gamma_i X_i^2 + \delta_i$ sind. Das Bild von U_i in der Vervollständigung von R_2 bzw. R_1 ist eine Einheit, da der konstante Term eine Einheit in k ist.

Im Ring $\hat{R}_2$ können wir neue Unbestimmte $T' = TU_1^{-1}U_2^{-1}$, $X_1' = X_1U_1^{-1}$, $X_2' = X_2U_2^{-1}$ wählen, sodass R_2 durch

$$\hat{R}_2 = k[\![X_1', X_2', T']\!]/\left(T'^2U_1^2U_2^2 + X_1'X_2'T'U_1^2U_2^2 + X_1'^2X_2'U_1^2U_2^2 + X_1'X_2'^2U_1^2U_2^2\right)$$

gegeben ist. Durch Elimination der Einheit $U_1^2U_2^2$ erhält man schließlich die Gleichung $T'^2 + X_1'X_2'T' + X_1'X_2'^2 + X_1'^2X_2'$, die nach Tabelle 1 eine Singularität vom Typ D_4^1 beschreibt. Völlig analog kann durch den Koordinatenwechsel $T' = TU_1^{-1}$, $X_1' = X_1U_1^{-1}$ der vervollständigte Ring $\hat{R}_1$ als

$$\hat{R}_1 = k[\![X_1', V_2, T']\!]/\left(T'^2 + X_1'V_2^2T' + X_1'^2V_2 + V_2^4X_1'\right)$$

geschrieben werden, was der tabellierten Normalform einer Singularität vom Typ D_8^2 ent-

spricht, in Übereinstimmung mit dem Resultat in [48], Propositionen 5.1 und 5.2. Beim Ring R_0, Invariantenring eines Produkts supersingulärer elliptischer Kurven, entspricht die gefundene Relation bereits der Normalform aus Bemerkung 3.5.

Wir fahren fort mit einer gewöhnlichen und der super-speziellen Kummer-Dreifaltigkeit.

Beispiel 3.36. Sind alle Faktoren im Fall $g = 3$ gewöhnliche elliptische Kurven, so erhält man mit dem Spektrum von

$$R = k[X_1, X_2, X_3, T_{\{1,2\}}, T_{\{1,3\}}, T_{\{2,3\}}, T_{\{1,2,3\}}]/J$$

eine offene Umgebung eines singulären Punktes der Kummer-Varietät. Das Ideal J wird erzeugt von den elf Elementen

$$\begin{aligned}
&X_1T_{\{2,3\}} + X_2T_{\{1,3\}} + X_3T_{\{1,2\}} + X_1X_2X_3,\\
&T^2_{\{1,2\}} + X_1X_2T_{\{1,2\}} + X_1^2P_2 + X_2^2P_1,\\
&T^2_{\{1,3\}} + X_1X_3T_{\{1,3\}} + X_1^2P_3 + X_3^2P_1,\\
&T^2_{\{2,3\}} + X_2X_3T_{\{2,3\}} + X_2^2P_3 + X_3^2P_2,\\
&T_{\{1,2\}}T_{\{1,3\}} + X_1T_{\{1,2,3\}} + P_1X_2X_3,\\
&T_{\{1,2\}}T_{\{2,3\}} + X_2T_{\{1,2,3\}} + P_2X_1X_3,\\
&T_{\{1,3\}}T_{\{2,3\}} + X_3T_{\{1,2,3\}} + P_3X_1X_2,\\
&T_{\{1,2\}}T_{\{1,2,3\}} + X_1X_2T_{\{1,2,3\}} + X_1P_2T_{\{1,3\}} + X_2P_1T_{\{2,3\}},\\
&T_{\{1,3\}}T_{\{1,2,3\}} + X_1X_3T_{\{1,2,3\}} + X_1P_3T_{\{1,2\}} + X_3P_1T_{\{2,3\}},\\
&T_{\{2,3\}}T_{\{1,2,3\}} + X_2X_3T_{\{1,2,3\}} + X_2P_3T_{\{1,2\}} + X_3P_2T_{\{1,3\}},\\
&T^2_{\{1,2,3\}} + X_1X_2X_3T_{\{1,2,3\}} + X_2X_3P_1T_{\{2,3\}} + X_1X_3P_2T_{\{1,3\}} + X_1X_2P_3T_{\{1,2\}}\\
&\qquad\qquad + X_1^2P_2P_3 + X_2^2P_1P_3 + X_3^2P_1P_2.
\end{aligned}$$

Analog zum Fall einer gewöhnlichen abelschen Fläche ist davon auszugehen, dass die Singularität von R verglichen mit denen anderer Kummer-Dreifaltigkeiten „am wenigsten gravierend“ ist. Im nächsten Abschnitt wird bewiesen, dass sich die Singularität der Kummer-Varietät nicht ändert, wenn wir alle Faktoren E_i durch die elliptische Kurve E mit $j(E) = 1$ ersetzen. Dadurch kann $P_i(x_i) = x_i^3 + x_i$ für $i = 1, 2, 3$ angenommen werden.

Der Ansatz, mit Blow-up im singulären Punkt eine partielle Auflösung zu berechnen, gestaltet sich wegen der relativ großen Zahl an Erzeugern des Ideals J als schwierig. Es ist beispielsweise a priori unklar, ob die strikte Transformation des Ideals J von den strikten Transformationen seiner Erzeuger erzeugt wird.

Beispiel 3.37. Treten im Fall $g = 3$ nur supersinguläre elliptische Kurven als Faktoren auf, wird ein offenes affines Unterschema der zugehörigen Kummer-Varietät durch

$$R = k[V_1, V_2, V_3, T_{\{1,2\}}, T_{\{1,3\}}, T_{\{2,3\}}, T_{\{1,2,3\}}]/J$$

beschrieben. Das Ideal J wird dabei erzeugt von den elf Elementen

$$
\begin{aligned}
&V_1^2T_{\{2,3\}} + V_2^2T_{\{1,3\}} + V_3^2T_{\{1,2\}} + V_1^2V_2^2V_3^2,\\
&T_{\{1,2\}}^2 + V_1^2V_2^2T_{\{1,2\}} + V_1^4V_2 + V_1V_2^4,\\
&T_{\{1,3\}}^2 + V_1^2V_3^2T_{\{1,3\}} + V_1^4V_3 + V_1V_3^4,\\
&T_{\{2,3\}}^2 + V_2^2V_3^2T_{\{2,3\}} + V_2^4V_3 + V_2V_3^4,\\
&T_{\{1,3\}}T_{\{1,2\}} + V_1^2T_{\{1,2,3\}} + V_1V_3^2V_2^2,\\
&T_{\{1,2\}}T_{\{2,3\}} + V_2^2T_{\{1,2,3\}} + V_2V_1^2V_3^2,\\
&T_{\{1,3\}}T_{\{2,3\}} + V_3^2T_{\{1,2,3\}} + V_3V_1^2V_2^2,\\
&T_{\{1,2\}}T_{\{1,2,3\}} + V_1^2V_2^2T_{\{1,2,3\}} + V_1^2V_2T_{\{1,3\}} + V_2^2V_1T_{\{2,3\}},\\
&T_{\{1,3\}}T_{\{1,2,3\}} + V_1^2V_3^2T_{\{1,2,3\}} + V_1^2V_3T_{\{1,2\}} + V_3^2V_1T_{\{2,3\}},\\
&T_{\{2,3\}}T_{\{1,2,3\}} + V_2^2V_3^2T_{\{1,2,3\}} + V_2^2V_3T_{\{1,2\}} + V_3^2V_2T_{\{1,3\}},\\
&T_{\{1,2,3\}}^2 + V_1^2V_2^2V_3^2T_{\{1,2,3\}} + V_2^2V_3^2V_1T_{\{2,3\}} + V_1^2V_3^2V_2T_{\{1,3\}} + V_1^2V_2^2V_3T_{\{1,2\}}\\
&\qquad\qquad + V_1^4V_2V_3 + V_2^4V_1V_3 + V_3^4V_1V_2.
\end{aligned}
$$

Im folgenden Unterabschnitt werden wir den Funktionenkörper dieser Kummer-Varietät genauer betrachten.

3.3.2 Rationalität und Kummer-Varietäten

Dadurch, dass nun ein offenes affines Unterschema der Kummer-Varietäten bekannt ist, kann auch der Funktionenkörper explizit beschrieben werden. In kleiner Dimension $g \leq 1$ kennen wir die Kummer-Varietäten beliebiger abelscher Varietäten. Diese sind isomorph zu $\mathbb{P}_k^0$ und $\mathbb{P}_k^1$ und können somit als rationale Varietäten identifiziert werden. Im Fall einer wilden Kummer-Fläche ist bekannt, dass sie genau dann rational ist, wenn sie von einer supersingulären abelschen Fläche stammt. Diese Beobachtung geht zurück auf Shioda in [51], Proposition 1, der dies am Produkt zweier supersingulärer elliptischer Kurven feststellte.

Der rationale Funktionenkörper der Kummer-Varietät, die von einem Produkt aus zwei supersingulären elliptischen Kurven stammt, ist nach Beispiel 3.35 durch $K = k(V_1, V_2, T)$ gegeben, wobei zwischen den Unbestimmten die Relation $T^2 + V_1^2V_2^2T + V_1^4V_2 + V_2^4V_1 = 0$ besteht. Durch mehrere Substitutionen zeigt Shioda, dass $K = k(r, s)$ gilt. Es werden die wesentlichen Schritte kurz angegeben:

(*i*) Führe eine neue Unbestimmte t über die Gleichung $T = t\,V_1^2V_2^2$ ein und dividiere die Relation durch $V_1^4V_2^4$. Dadurch wird $K = k(V_1, V_2, t)$ erhalten mit der Relation $t^2 + t + V_1^{-3} + V_2^{-3} = 0$.

(*ii*) Führe eine neue Unbestimmte s über die Gleichung $V_2^{-1} = V_1^{-1} + s$ ein und ersetze V_2^{-1} in der Relation aus (*i*). Wir erhalten dadurch $K = k(V_1, s, t)$ mit der Relation $t^2 + t + s \cdot (V_1^{-2} + V_1^{-1}s + s^2) = 0$.

(*iii*) Führe eine neue Unbestimmte r über die Gleichung $t = r \cdot (V_1^{-1} + \omega\, s)$ ein, wobei ω eine primitive dritte Einheitswurzel bezeichnet, und setze den Ausdruck für t in der Relation ein. Nach Division durch $(V_1^{-1} + \omega\, s)$ wird die Gleichung zu

$$r^2(V_1^{-1} + \omega\, s) + r + s \cdot (V_1^{-1} + \omega^2\, s) = 0.$$

Diese Gleichung lässt sich nach V_1 auflösen, womit $K = k(r, s)$ gezeigt ist.

Man kann nun auch V_1, V_2 und T explizit als rationale Funktionen in r, s ausdrücken. Für die V_i ergibt sich

$$V_1 = \frac{r^2 + s}{\omega r^2 s + r + \omega^2 s^2}, \qquad V_2 = \frac{r^2 + s}{\omega^2 r^2 s + r + \omega s^2}\ .$$

Es ist offen, ob es eine Verallgemeinerung des Resultats in höhere Dimension gibt.

Frage 3.38. Ist die superspezielle Kummer-Varietät der Dimension g für (ein) $g > 2$ rational?

Wir betrachten den Funktionenkörper der superspeziellen Kummer-Varietät aus Beispiel 3.37. Dieser kann zunächst als $K = k(V_1, V_2, V_3, T_{\{1,2\}}, T_{\{1,3\}}, T_{\{2,3\}}, T_{\{1,2,3\}})$ mit einer großen Zahl an Relationen beschrieben werden. Wegen der Relationen

$$T_{\{2,3\}} = \frac{V_2^2 T_{\{1,3\}} + V_3^2 T_{\{1,2\}} + V_1^2 V_2^2 V_3^2}{V_1^2}, \qquad T_{\{1,2,3\}} = \frac{T_{\{1,2\}} T_{\{1,3\}} + V_1 V_2^2 V_3^2}{V_1^2}$$

können diese Unbestimmten ausgelassen werden. Für $i = 2, 3$ sind die beiden Teilkörper $K_i = k(V_1, V_i, T_{\{1,i\}}) = k(r_i, s_i)$ von K rationale Funktionenkörper. Jede der verbliebenen Unbestimmten V_1, V_2, V_3, $T_{\{1,2\}}$, $T_{\{1,3\}}$ kann als eine rationale Funktion in r_2, s_2 oder r_3, s_3 dargestellt werden, das Element V_1 sogar sowohl in K_2 als auch in K_3, wodurch sich die Bedingung

$$\frac{r_2^2 + s_2}{\omega r_2^2 s_2 + r_2 + \omega^2 s_2^2} = \frac{r_3^2 + s_3}{\omega r_3^2 s_3 + r_3 + \omega^2 s_3^2} \quad (= V_1)$$

in $K = k(r_2, s_2, r_3, s_3)$ ergibt. Es bleibt leider unklar, ob sogar $K = k(a, b, c)$ ein rationaler Funktionenkörper ist.

3.3.3 Analoga in Charakteristik p

Wesentliche Resultate für die Berechnung des Invariantenrings in Abschnitt 3.2 waren Proposition 3.12 sowie Theorem 3.17, in dem Erzeuger des Invariantenrings angegeben wurden. Da beide Aussagen nicht nur auf den Fall $p = 2$ beschränkt sind, kann mit den genannten Hilfsmitteln ebenso der Quotient eines Produkts von Artin–Schreier-Kurven nach einer $\mathbb{Z}/p\mathbb{Z}$-Wirkung untersucht werden.

Es bezeichne k einen algebraisch abgeschlossenen Körper der Charakteristik $p > 0$. Wir betrachten eine Artin–Schreier-Kurve $C = V_+(F)$, wobei F das homogene Polynom

$$F(X, Y, Z) = Y^p - X^{p-1}Y - \left(XZ^{p-1} + \alpha_2 X^2 Z^{p-2} + \ldots + \alpha_p X^p\right)$$

mit Koeffizienten $\alpha_i \in k$ bezeichnet. Die Kurve C besitzt keine Singularitäten: Ein singulärer Punkt $P = (a : b : c)$ müsste $a = 0$ erfüllen, damit $\partial F/\partial Y$ an P verschwindet. Weiter muss $b = 0$ gelten, damit P eine Nullstelle von F ist, und schließlich $c = 0$ wegen der Bedingung $\partial F/\partial X(P) = 0$.

Es sei $G = \mathbb{Z}/p\mathbb{Z} = \langle\sigma\rangle$ zyklisch. Auf C ist durch $\sigma((X : Y : Z)) = (X : Y + X : Z)$ eine G-Wirkung gegeben. Der einzige Fixpunkt dieser Wirkung ist der Punkt $(0 : 0 : 1)$, der im offenen affinen Unterschema $D_+(Z) \subset C$ liegt. Dieses ist offensichtlich invariant unter der G-Wirkung, da die Z-Koordinate von σ nicht manipuliert wird. Mittels neuer Koordination $x = X/Z$, $y = Y/Z$ erhalten wir den affinen Koordinatenring

$$k[x, y]/(y^p - x^{p-1}y - (x + \alpha_2 x^2 + \ldots + \alpha_p x^p))$$

von $D_+(Z)$ mit der induzierten G-Wirkung durch $\sigma(x) = x$, $\sigma(y) = y + x$. Es bezeichne $f(x) = x + \alpha_2 x^2 + \ldots + \alpha_p x^p$. Die definierende Gleichung der Kurve kann damit auch kurz als $\mathrm{N}(y) - f(x) = 0$ geschrieben werden.

Ist nun $V = C_1 \times \ldots \times C_n$ das Produkt von n Artin–Schreier-Kurven der obigen Form, dann besitzt die Diagonalwirkung auf V wieder einen eindeutigen Fixpunkt, für den eine G-invariante offene affine Umgebung durch das Spektrum des Rings

$$R = k[x_1, y_1, \ldots, x_n, y_n]/(\mathrm{N}(y_i) - f_i(x_i),\ 1 \le i \le n)$$

gegeben ist; der Fixpunkt entspricht darin dem Ursprung, d. h. dem maximalen Ideal $\mathfrak{m} = (x_1, y_1, \ldots, x_n, y_n)$. Der Invariantenring R^G ist nun der affine Koordinatenring eines offenen affinen Unterschemas vom Quotienten V/G. Das maximale Ideal $R^G \cap \mathfrak{m} \subset R^G$ gibt einen singulären Punkt, wenn $n \ge 2$ gilt.

Nach Theorem 3.17 und Proposition 3.12 bilden die Restklassen der folgenden Elemente in R ein Erzeugendensystem der k-Algebra R^G:

$$\begin{aligned} &x_i \ \text{ für } 1 \le i \le n, \\ &x_i y_j - x_j y_i \ \text{ für } 1 \le i < j \le n, \\ &\mathrm{Tr}\,(y_1^{a_1} \cdots y_n^{a_n}) \ \text{ für } 0 \le a_1, \ldots, a_n \le p-1 \text{ und } \sum a_i > 2(p-1). \end{aligned} \tag{3.25}$$

Die Elemente $\mathrm{N}(y_i) = y_i^p - x_i^{p-1} y_i$, welche in Theorem 3.17 aufgelistet sind, können weggelassen werden, da in R ja die Gleichheit $\mathrm{N}(y_i) = f_i(x_i)$ gilt.

Wir bestimmen die Anzahl der Elemente des Erzeugendensystems (3.25): Es gibt n Elemente $x_1, \ldots, x_n$ und $n(n-1)/2$ Elemente der Form $x_i y_j - x_j y_i$ für $i < j$. Die Elemente der Form $\mathrm{Tr}(y_1^{a_1} \cdots y_n^{a_n})$ entsprechen bijektiv den Tupeln $a = (a_1, \ldots, a_n)$ mit Einträgen $a_i \in \{0, \ldots, p-1\}$, deren Summe $|a|$ den Wert $2(p-1)$ übersteigt. Es ist allerdings leichter die Tupel zu zählen, bei denen $|a| \leq 2(p-1)$ erfüllt ist. Es wird gezeigt, dass

$$\left| \left\{ a \in \{0, \ldots, p-1\}^n \mid |a| \leq 2(p-1) \right\} \right| = \binom{n+2p-2}{2p-2} - n\binom{n+p-2}{p-2}$$

gilt. Dazu zählen wir zunächst alle Tupel $a \in \mathbb{N}^n$, für die $|a| = M$ für ein $M \in \mathbb{N}$ gilt. Von diesen gibt es $\binom{n+M-1}{M}$ viele; man kann jedes dieser Tupel als ein Monom vom Grad M in n Unbestimmten auffassen und das gleiche kombinatorische Modell wie im Beweis von Proposition 2.7 benutzen. Mit Lemma 2.8 erhält man die Zahl der $a \in \mathbb{N}^n$ mit $|a| \leq M$: Es gilt

$$\left| \left\{ a \in \mathbb{N}^n \mid |a| \leq M \right\} \right| = \sum_{i=0}^{M} \binom{n+i-1}{i} = \binom{n+M}{M},$$

speziell gibt es also $\binom{n+2p-2}{2p-2}$ Tupel, deren Einträge sich zu höchstens $2p-2$ summieren. Hiervon muss nun noch die Zahl der Tupel abgezogen werden, bei denen ein Eintrag a_i größer als $p-1$ ist. Da sich die anderen Einträge höchstens zu $p-2$ summieren, ist dieser Eintrag der einzige, der den Wert $p-1$ übersteigt. Es reicht daher, n-mal die Anzahl der Tupel zu subtrahieren, bei denen $a_1 \geq p$ gilt. Es muss nun lediglich die Zahl der Tupel $(a_1 - p, a_2, \ldots, a_n)$ ermittelt werden, deren Einträge sich zu höchstens $p-2$ summieren. Diese ist nach obiger Betrachtung gerade $\binom{n+p-2}{p-2}$, was die gewünschte Anzahl ergibt.

Insgesamt erhält man nun, dass das Erzeugendensystem (3.25) aus

$$p^n - \binom{n+2p-2}{2p-2} + n\binom{n+p-2}{p-2} + \binom{n}{2} + n$$

Elementen besteht.

Bemerkung 3.39. In der Einleitung von [10] wird eine Formel für die Anzahl der Elemente des Erzeugendensystems aus Theorem 3.17 gegeben. Obige Formel gibt diese Anzahl verringert um n wieder, der Anzahl der redundanten Elemente $\mathrm{N}(y_i)$. Da in [10] kein Beweis gegeben ist, wurde dieser hier ergänzt. Eine Beschreibung aller Relationen zwischen den Erzeugern des Invariantenrings ist bisher nur für den Fall $p = 2$ bekannt, aus diesem Grund kann der Invariantenring ohne Weiteres nicht explizit als Quotient eines Polynomrings nach einem Ideal geschrieben werden.

3.4 Formale Gruppen

Eine Kummer-Varietät, die von einer gewöhnlichen abelschen Varietät stammt, bezeichnen wir im Folgenden auch als *gewöhnliche Kummer-Varietät*. In [32], Lemma 4, wird die Untersuchung der Singularitäten von gewöhnlichen Kummer-Flächen auf den Spezialfall des Produkts gewöhnlicher elliptischer Kurven zurückgeführt. Das Argument hierzu soll in diesem Abschnitt erläutert und für höhere Dimension verallgemeinert werden. Dazu werden einige Aussagen über formale Gruppen benötigt. Die Hauptquellen für den Exkurs sind die Artikel [37], [38] von Manin. Nach einer kurzen Zusammenfassung relevanter Resultate folgt der Beweis, dass die formalen Gruppen gewöhnlicher abelscher Varietäten mit denen von Produkten gewöhnlicher elliptischer Kurven übereinstimmen. Hieraus kann dann schließlich deduziert werden, dass auch die Singularitäten der Kummer-Varietäten formal isomorph sind.

In diesem Abschnitt bezeichne k stets einen algebraisch abgeschlossenen Grundkörper der Charakteristik $p > 0$.

Definition 3.40. Es seien X ein noethersches Schema und $Y \subset X$ ein abgeschlossenes Unterschema, welches durch die Idealgarbe $\mathscr{I} \subset \mathscr{O}_X$ gegeben ist. Wir definieren die *formale Vervollständigung von X entlang Y* als den geringten Raum, der aus dem topologischen Raum von Y besteht und dessen Strukturgarbe durch $\varprojlim \mathscr{O}_X/\mathscr{I}^n$ gegeben ist. Wenn Y bzw. $\mathscr{I}$ aus dem Kontext klar sind, wird die formale Vervollständigung kurz mit $\hat{X}$ notiert.

Wichtigstes Beispiel in diesem Abschnitt ist die formale Vervollständigung eines Schemas an einem abgeschlossenen Punkt.

Beispiel 3.41. Es seien X ein noethersches Schema und $Y = \{P\}$ ein abgeschlossener Punkt. Nach [24], Example II.9.3.4, ist $\hat{X} = \{P\}$ und die Strukturgarbe ist durch den vervollständigten lokalen Ring an P gegeben, d. h. $\mathscr{O}_{\hat{X}} = \hat{\mathscr{O}}_{X,P}$.

Definition 3.42. Es seien A ein noetherscher Ring und $\hat{A}$ die Vervollständigung bzgl. eines Ideals $I \subset A$.

(*i*) Das *formale Spektrum* $\mathrm{Spf}(\hat{A})$ ist die formale Vervollständigung von $\mathrm{Spec}(A)$ entlang $V(I)$. Ein Morphismus zwischen formalen Spektren ist ein Morphismus von lokal geringten Räumen. Wenn A eine k-Algebra ist, erhält man einen Morphismus $\mathrm{Spf}(\hat{A}) \to \mathrm{Spec}(k)$ und kann analog zu Schemata über k von formalen Spektren über k sprechen.

(*ii*) Eine *formale Gruppe* über einem Körper k ist ein Gruppenobjekt G in der Kategorie der formalen Spektren über k, das von der Form $G = \mathrm{Spf}(\hat{A})$ für eine noethersche, lokale k-Algebra $(A, \mathfrak{m}, k)$ ist. Ein *Homomorphismus* zwischen formalen Gruppen ist ein Morphismus zwischen formalen Spektren über k, der kompatibel mit dem Gruppengesetz $\mu\colon G \times G \to G$ ist.

Die formalen Spektren umfassen insbesondere jedes affine Schema als Vervollständigung entlang seiner selbst. Implizit wurde in der Definition auch schon genutzt, dass die Kategorie der formalen Spektren ein Produkt besitzt: Sind A_j vollständige Algebren bzgl. Idealen I_j für $j = 1, 2$ über einem vollständigen Grundring (z. B. einem Körper k), dann ist $\mathrm{Spf}(A_1) \times \mathrm{Spf}(A_2) = \mathrm{Spf}(B)$, wobei B die Vervollständigung von $A_1 \otimes A_2$ bzgl. des Ideals $I_1 \otimes A_2 + A_1 \otimes I_2$ bezeichnet. Wir schreiben dafür auch kurz $B = A_1 \hat{\otimes} A_2$.

Beispiel 3.43. Wir betrachten den Spezialfall, dass X eine algebraische Gruppe über einem Körper k und $Y = \{e\}$ das neutrale Element ist. In diesem Fall ist

$$\mathscr{O}_{\hat{X}} = k[\![T_1, \ldots, T_g]\!] = \hat{O}_{X,e}$$

ein Ring von formalen Potenzreihen mit $g = \dim(X)$. Die Multiplikation $\mu\colon X \times X \to X$ und die Inversion $\iota\colon X \to X$ induzieren Ringhomomorphismen zwischen den vollständigen Ringen $\hat{\mathscr{O}}_{X,e} \to \hat{\mathscr{O}}_{X\times X,(e,e)} \cong \hat{\mathscr{O}}_{X,e} \hat{\otimes} \hat{\mathscr{O}}_{X,e}$ und $\hat{\mathscr{O}}_{X,e} \to \hat{\mathscr{O}}_{X,e}$. Durch diese sind Morphismen $\hat{X} \times \hat{X} \to \hat{X}$ und $\hat{X} \to \hat{X}$ gegeben, die die Bedingungen für ein Gruppenobjekt (1.1)–(1.3) erfüllen. Dadurch besitzt $\hat{X} = \mathrm{Spf}(\hat{\mathscr{O}}_{X,e})$ die Struktur einer formalen Gruppe.

Als Nächstes definieren wir den Begriff der Isogenie für kommutative formale Gruppen. Für die Definition aus [38], S. 23, wird das Konzept der *Quotientenkategorie* gebraucht. Es seien $\mathcal{C}$ die Kategorie der kommutativen formalen Gruppen über k und $\mathcal{D}$ die volle Unterkategorie der formalen Gruppen über k der Form $\mathrm{Spf}(A)$ mit A artinsch und lokal. Die Kategorien $\mathcal{C}$ und $\mathcal{D}$ sind abelsch und die Unterkategorie $\mathcal{D}$ erfüllt die Bedingung, dass für jede kurze exakte Sequenz

$$0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0$$

in $\mathcal{C}$ die formale Gruppe G_2 genau dann in $\mathcal{D}$ liegt, wenn G_1 und G_3 in $\mathcal{D}$ liegen. Die Quotientenkategorie $\mathcal{C}/\mathcal{D}$ besteht aus den Objekten von $\mathcal{C}$ und für formale Gruppen G, H in $\mathcal{C}$ ist

$$\mathrm{Hom}_{\mathcal{C}/\mathcal{D}}(G, H) = \varinjlim \mathrm{Hom}_{\mathcal{C}}(G', H/H'),$$

wobei G' und H' alle Unterobjekte von G und H mit $G/G', H' \in \mathcal{D}$ durchlaufen (siehe [19], Kap. I, Abs. 2). Für $G' = G$ und $H' = 0$ erhält man die Morphismenmenge in $\mathcal{C}$ und auf diese Weise eine kanonische Abbildung $\mathrm{Hom}_{\mathcal{C}}(G, H) \to \mathrm{Hom}_{\mathcal{C}/\mathcal{D}}(G, H)$.

Definition 3.44. Ein Homomorphismus von kommutativen formalen Gruppen $\alpha\colon G \to H$ heißt *Isogenie*, wenn das Bild von α in $\mathrm{Hom}_{\mathcal{C}/\mathcal{D}}(G, H)$ ein Isomorphismus ist. Die formalen Gruppen G und H heißen in diesem Fall *isogen*.

Die Relation „ist isogen zu“ ist eine Äquivalenzrelation. Eine Isogenie zwischen algebraischen Gruppen, d. h. ein surjektiver Homomorphismus mit endlichem Kern, induziert eine Isogenie zwischen den zugehörigen formalen Gruppen ([38], S. 23).

Es seien $G = \mathrm{Spf}(k[\![x_1, \ldots, x_n]\!])$, $H = \mathrm{Spf}(k[\![y_1, \ldots, y_m]\!])$ formale Gruppen mit Gruppengesetz μ_G bzw. μ_H. Jeder Homomorphismus $\alpha\colon G \to H$ induziert einen lokalen Ringhomomorphismus zwischen den Potenzreihenringen. Nach Proposition 1 in [37] existiert zu α eine eindeutige Folge $m = s_0 \geq s_1 \geq \ldots \geq s_t \geq 0$ von natürlichen Zahlen, sodass der induzierte Ringhomomorphismus (nach Einführen geeigneter Koordinaten) durch

$$\begin{aligned} y_i &\longmapsto x_i^{p^\nu} && \text{für } m - s_\nu < i \leq m - s_{\nu+1}, \\ y_i &\longmapsto 0 && \text{für } m - s_t < i < m \end{aligned}$$

gegeben ist. Wenn α eine Isogenie ist, dann gelten $n = m$ und $s_t = 0$. Wir definieren in dieser Situation $\deg(\alpha) = p^{s_1 + \ldots + s_{t-1}}$ als den Grad der Isogenie.

Die Dimension einer formalen Gruppe $G = \mathrm{Spf}(B)$ ist per Definition die Dimension des Rings B. Endlich-dimensionale kommutative formale Gruppen wurden in [38], Kap. II, §4, bis auf Isogenie klassifiziert:

Theorem 3.45. *Jede endlich-dimensionale kommutative formale Gruppe G über k ist isogen zu einer Summe der Form $G \sim T \oplus U \oplus V$ mit*

$$T = \bigoplus_{i=1}^{r} G_{1,0} \ , \quad U = \bigoplus_{n \geq 1} G_{n,\infty}^{\oplus r_n} \ , \quad V = \bigoplus_{\substack{n,m \geq 1 \\ (n,m)=1}} G_{n,m}^{\oplus s_{n,m}}$$

und natürlichen Zahlen r, r_n, $s_{n,m}$. Dabei sind nur endlich viele r_n und $s_{n,m}$ positiv. Diese Darstellung ist bis auf Isogenie eindeutig. Die Summanden $G_{n,m}$, wobei $1 \leq n < \infty$, $0 \leq m \leq \infty$, $\mathrm{ggT}(n,m) = 1$ für $m \neq \infty$, sind kommutative formale Gruppen, die bis auf Isogenie eindeutig durch die folgenden Bedingungen bestimmt sind:

(i) $G_{n,m}$ ist n-dimensional.

(ii) $G_{n,m}$ ist unzerlegbar.

(iii) Die Multiplikation mit p ist für $G_{n,m}$ mit $m \neq \infty$ eine Isogenie vom Grad p^{n+m} und für $G_{n,\infty}$ keine Isogenie.

Insbesondere liegen $G_{n,m}$ und $G_{n',m'}$ mit $(n,m) \neq (n',m')$ in verschiedenen Isogenieklassen.

Durch Lemma 1 in [37] werden die verschiedenen Isogenie-Begriffe in Beziehung gesetzt:

Proposition 3.46. *Es seien A und B algebraische Gruppen über k. Weiter sei $\alpha\colon A \to B$ eine Isogenie und $\hat{\alpha}\colon \hat{A} \to \hat{B}$ die induzierte Isogenie zwischen den formalen Gruppen. Dann gilt*

$$\deg(\hat{\alpha}) = \mathrm{insdeg}(\alpha),$$

wobei $\mathrm{insdeg}(\alpha)$ *den Inseparabilitätsgrad von α bezeichnet.*

Wir wenden Proposition 3.46 auf den Fall $\alpha = p_A \colon A \to A$ an, wobei A eine abelsche Varietät der Dimension g bezeichnet. Da die Kardinalität des Kerns $\ker(p_A)(k)$ mit dem Separabilitätsgrad von p_A übereinstimmt, erhält man die Gleichung

$$\operatorname{insdeg}(p_A) = \frac{p^{2g}}{|\ker(p_A)(k)|} \tag{3.26}$$

und hiermit insbesondere die Möglichkeit, Rückschlüsse auf die Struktur der formalen Gruppe $\hat{A}$ zu ziehen. Dies wird in den beiden folgenden Korollaren ausgeführt.

Korollar 3.47. *Ist E eine elliptische Kurve über k, dann liegt $\hat{E}$ in einer der beiden Isogenie-Klassen $G_{1,0}$ oder $G_{1,1}$. Ist E gewöhnlich, so gilt $\hat{E} \sim G_{1,0}$. Ist E supersingulär, dann gilt $\hat{E} \sim G_{1,1}$.*

Beweis. Da p_E auf E eine Isogenie vom Grad p^2 ist, liegt $\hat{E}$ entweder in der Isogenieklasse von $G_{1,0}$ oder von $G_{1,1}$. Die Unterscheidung erfolgt anhand des Grades der induzierten Isogenie $\widehat{p_E} \colon \hat{E} \to \hat{E}$. Ist E supersingulär, so ist $\ker(p_E)(k) = \{e\}$ ein Punkt und folglich ist $\operatorname{insdeg}(p_E) = \deg(\widehat{p_E}) = p^2$. Also gilt $\hat{E} \sim G_{1,1}$. Wenn E gewöhnlich ist, dann gilt $\ker(p_E)(k) \cong \mathbb{Z}/p\mathbb{Z}$ und entsprechend gelten $\operatorname{insdeg}(p_E) = p$ und $\hat{E} \sim G_{1,0}$. □

Bemerkung 3.48. In Korollar 3.47 wurde die formale Gruppe einer elliptischen Kurve nur bis auf Isogenie ermittelt. Im Fall von eindimensionalen formalen Gruppen der Form $\operatorname{Spf}(k[\![T]\!])$ kann Isogenie durch Isomorphie ersetzt werden: Nach [26], Theorem 18.5.1, sind solche formalen Gruppen G_1, G_2 genau dann isomorph, wenn die Isogenien $\hat{p}_i \colon G_i \to G_i$ den gleichen Grad besitzen.

Beispiel 3.49. Die multiplikative Gruppe $\mathbb{G}_m$ ist eindimensional und die „Multiplikation“ mit p induziert die Erweiterung der Funktionenkörper $k(T^p) \subset k(T)$, die rein inseparabel ist. Damit ist $\hat{\mathbb{G}}_m$ nach obiger Klassifikation isogen zu $G_{1,0}$. Wir können daher $\hat{\mathbb{G}}_m = G_{1,0}$ als ausgezeichneten Repräsentanten der Isogenieklasse ansehen. Es sei $R = k[X,U]/(XU-1)$. Als Schema ist $\mathbb{G}_m = \operatorname{Spec}(R)$ und die Gruppenstruktur kann als Hopf-Algebra-Struktur auf R erklärt werden mit neutralem Element 1 und Komultiplikation $\Delta \colon R \to R \otimes R$, $X \mapsto X_1X_2$, $U \mapsto U_1U_2$. Indem wir X und U durch $X-1$, $U-1$ ersetzen, verschieben wir das neutrale Element in den Ursprung und erhalten $R \cong k[X,U]/(XU+X+U)$. Die Vervollständigung am Ursprung ist $k[\![X]\!]$, da die formale partielle Ableitung nach U eine Einheit ist. Die Komultiplikation definiert nun das Gruppengesetz der formalen Gruppe und ist durch $\Delta \colon k[\![X]\!] \to k[\![X_1, X_2]\!]$, $X \mapsto X_1X_2 + X_1 + X_2$ gegeben.

Da die formale Gruppe $G_{1,0}$ von der multiplikativen Gruppe $\mathbb{G}_m$ stammt, wird der Summand T in Theorem 3.45 auch als *toroidaler Anteil* bezeichnet. Unter leichten Voraussetzungen kann Isogenie zu einer toroidalen formalen Gruppe durch Isomorphie ersetzt

werden, wobei eingeht, dass der Grundkörper k algebraisch abgeschlossen ist. Dies ist die Aussage von [38], Theorem 1.2 (S. 20):

Proposition 3.50. *Wenn G eine reduzierte formale Gruppe über k und $G \sim T$ erfüllt ist, dann gilt sogar Isomorphie $G \cong T$.*

Dabei heißt $G = \mathrm{Spf}(B)$ reduziert, wenn B eine reduzierte k-Algebra ist.

Das folgende Resultat ist im Wesentlichen Theorem 4.1 aus [38], welches jedoch ausschließlich für endliche Körper formuliert wurde. Oort zeigt in [44], S. III.19-3, dass sich die Aussage auch auf den unendlichen Körper $k = \bar{k}$ übertragen lässt.

Theorem 3.51. *Sind A eine abelsche Varietät über k und $\hat{A}$ die formale Gruppe zu A, dann gilt*

$$\hat{A} \sim G_{1,0}^{\oplus r} \oplus G_{1,1}^{\oplus s} \oplus \bigoplus_{\substack{m>n\geq 1 \\ (n,m)=1}} (G_{n,m} \oplus G_{m,n})^{\oplus t_{n,m}} \tag{3.27}$$

für geeignete $r, s, t_{n,m} \geq 0$, d. h., die Summanden $G_{n,m}$ und $G_{m,n}$ treten stets mit gleicher Multiplizität und $G_{n,\infty}$ gar nicht auf.

Bemerkung 3.52. Es ist nicht klar, ob umgekehrt jede formale Gruppe der Form (3.27) von einer abelschen Varietät herrührt. Manin zeigt in [38], Kap. IV, §5, durch Beispiele, dass dies bis einschließlich Dimension 4 der Fall ist.

Korollar 3.53. *Es sei A eine gewöhnliche g-dimensionale abelsche Varietät über k. In diesem Fall ist die formale Gruppe $\hat{A}$ isomorph zu $G_{1,0}^{\oplus g}$.*

Beweis. Es sei $\hat{A}$ wie in (3.27) gegeben. Es gilt $|\ker(p_A)(k)| = p^g$, da A gewöhnlich ist. Mit Gleichung (3.26) ergibt sich $\deg(\widehat{p_A}) = \mathrm{insdeg}(p_A) = p^g$. Durch Vergleich des Grades von $\widehat{p_A}$ und der Dimension bei den formalen Gruppen in (3.27) ergeben sich die Bedingungen

$$\begin{aligned} g &= r + s + \sum (m+n) t_{n,m}, \\ g &= r + 2s + \sum 2(m+n) t_{n,m}, \end{aligned}$$

die nur gleichzeitig erfüllt sein können, wenn $s = 0$ und $t_{m,n} = 0$ erfüllt ist. Somit ist $\hat{A}$ isogen zu $G_{1,0}^{\oplus g}$. Da $\hat{A}$ reduziert ist, gilt nach Proposition 3.50 auch die Isomorphie. □

Bei gewöhnlichen abelschen Varietäten existiert somit nur eine Isomorphieklasse von formalen Gruppen. Die Beobachtung, dass sich für jeden Faktor $\mathbb{Z}/p\mathbb{Z}$ von $\ker(p_A)$ eine multiplikative Gruppe $G_{1,0}$ abspaltet, gilt aber auch für beliebige abelsche Varietäten. Dies ist Theorem 2 in [37], das hier nun als Korollar folgt.

$\dim(G)$	mögliche G bis auf Isogenie
1	$G_{1,0}, \quad G_{1,1}$
2	$G_{1,0}^{\oplus 2}, \quad G_{1,1}^{\oplus 2}, \quad G_{1,0} \oplus G_{1,1}$
3	$G_{1,0}^{\oplus r} \oplus G_{1,1}^{\oplus 3-r}$, $0 \leq r \leq 3$, $\quad G_{1,2} \oplus G_{2,1}$
4	$G_{1,0}^{\oplus r} \oplus G_{1,1}^{\oplus 4-r}$, $0 \leq r \leq 4$, $\quad G_{1,0} \oplus G_{1,2} \oplus G_{2,1}, \quad G_{1,1} \oplus G_{1,2} \oplus G_{2,1}, \quad G_{1,3} \oplus G_{3,1}$

Tabelle 2: Formale Gruppen abelscher Varietäten

Korollar 3.54. *Ist A eine abelsche Varietät der Dimension g über dem Körper k und gilt weiter $\ker(p_A)(k) = (\mathbb{Z}/p\mathbb{Z})^{\oplus f}$, dann ist*

$$\hat{A} \sim G_{1,0}^{\oplus f} \oplus \bigoplus_i G_{n_i,m_i}$$

erfüllt. Dabei muss $\sum m_i = \sum n_i = g - f$ gelten.

Beweis. Wir nehmen an, dass $\hat{A}$ wie in (3.27) gegeben ist, und vergleichen wieder Dimension und Inseparabilitätsgrad. Dadurch erhalten wir

$$\begin{aligned} g &= r + s + \sum (m+n) t_{n,m}, \\ 2g - f &= r + 2s + \sum 2(m+n) t_{n,m}. \end{aligned}$$

Subtrahiert man zweimal die erste Gleichung von der zweiten, so ergibt sich $-f = -r$, womit die Behauptung bewiesen ist. Der Zusatz folgt aus der Symmetriebedingung aus Theorem 3.51. □

Die möglichen formalen Gruppen kleiner Dimension, die von abelschen Varietäten herrühren, sind in Tabelle 2 aufgeführt. Die Gruppen $G_{1,2} \oplus G_{2,1}$ und $G_{1,3} \oplus G_{3,1}$ sind die ersten Beispiele, deren Isogenieklasse nicht durch Produkte von elliptischen Kurven beschrieben werden kann. Eine solche abelsche Varietät kann nach Korollar 3.54 keinen Punkt der Ordnung p besitzen, da sonst mindestens ein Summand $G_{1,0}$ auftreten würde.

Als Nächstes wird nun untersucht, welche formalen Gruppen bei einer g-dimensionalen abelschen Varietät mit $|\ker(p_A)(k)| = p^{g-1}$ auftreten können, also bei „fast gewöhnlichen“ abelschen Varietäten. Nach dem letzten Korollar ist bereits klar, dass in diesem Fall

$$\hat{A} \sim G_{1,0}^{\oplus g-1} \oplus G_{1,1}$$

gelten muss. Es wird sich herausstellen, dass sogar Isomorphie gilt. Dazu ist ein Resultat nötig, dass die formale Gruppe $\hat{A}$ mit der p-divisiblen Gruppe $A(p)$ in Beziehung setzt.

Definition 3.55. Für eine abelsche Varietät A über k sei $A(p) = \varinjlim \ker(p_A^n)$. Dabei bilden die Gruppenschemata $\ker(p_A^n)$ ein induktives System vermöge der Inklusionen.

Die Verbindung zu formalen Gruppen besteht darin, dass die Zusammenhangskomponente des neutralen Elements $A(p)^0$ mit der formalen Vervollständigung von A am neutralen Element, also mit der formalen Gruppe $\hat{A}$ übereinstimmt ([53], Examples S. 166). Um den Limes $\varinjlim \ker(p_A^n)$ zu verstehen, stellt sich die Frage nach der Schemastruktur von $\ker(p_A^n)$. In [42], S. 146f., wird folgende Zerlegung des Gruppenschemas erhalten:

Theorem 3.56. *Es sei A eine abelsche Varietät über dem Grundkörper k. Dann gilt*

$$\ker(p_A^n) \cong (\mathbb{Z}/p^n\mathbb{Z})^r \times (\mu_{p^n})^r \times N_{p^n},$$

wobei r durch $p^r = |\ker(p_A)(k)|$ definiert ist und N_{p^n} ein Gruppenschema vom Typ lokal-lokal bezeichnet.

Beispiel 3.57. Die Definition der p-divisiblen Gruppe lässt sich auf allgemeinere algebraische Gruppen übertragen. Für die Schemata μ_{p^n} mit $n \geq 1$ erhält man den direkten Limes

$$\begin{aligned}\varinjlim\ \mu_{p^n} &= \varinjlim\ \operatorname{Spec}\left(k[X]/(X^{p^n}-1)\right) = \varinjlim\ \operatorname{Spec}\left(k[Y]/(Y^{p^n})\right)\\ &= \operatorname{Spf}\left(\varprojlim\ k[Y]/(Y^{p^n})\right) = \operatorname{Spf}\left(k[\![Y]\!]\right),\end{aligned}$$

wobei $Y = X - 1$ ersetzt wurde und das System der Ideale (Y^{p^n}) nach Lemma 7.14 aus [16] ausreicht, um als Vervollständigung den Ring der formalen Potenzreihen zu erhalten. Damit ist der Limes als formales Schema bestimmt. Da die Gruppenstruktur auf μ_{p^n} mit der von $\mathbb{G}_m$ übereinstimmt, ist folglich $\varinjlim\ \mu_{p^n} \cong G_{1,0}$.

Proposition 3.58. *Es sei A eine abelsche Varietät über k. Es gelte $\hat{A} \sim G_{1,1} \oplus G_{1,0}^{\oplus g-1}$. In diesem Fall kann Isogenie durch Isomorphie ersetzt werden.*

Beweis. Nach Voraussetzung gilt $|\ker(p_A)(k)| = p^{g-1}$ und das endliche Gruppenschema $\ker(p_A^n)$ ist damit von der Form $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus g-1} \oplus \mu_{p^n}^{\oplus g-1} \oplus N_{p^n}$, wobei N_{p^n} vom Typ lokal-lokal ist. Die formale Gruppe zu A kann nach Theorem 3.56 durch

$$\begin{aligned}\hat{A} &\cong \varinjlim \left(\mu_{p^n}^{\oplus g-1} \oplus N_{p^n}\right) \cong (\varinjlim \mu_{p^n})^{\oplus g-1} \oplus \varinjlim N_{p^n}\\ &\cong G_{1,0}^{\oplus g-1} \oplus H\end{aligned}$$

ermittelt werden. Dabei wurde benutzt, dass der direkte Limes mit direkten Summen verträglich ist. Aus der eindeutigen Zerlegung von $\hat{A}$ bis auf Isogenie ist klar, dass der Summand H isomorph zu einem Repräsentanten der Isogenieklasse von $G_{1,1}$ ist. Da H eindimensional ist, gilt nach Bemerkung 3.48 die Isomorphie. □

Im Fall $A \sim G_{1,0}^{\oplus g-2} \oplus G_{1,1}^{\oplus 2}$ funktioniert das Argument nicht mehr, da es verschiedene Isomorphieklassen innerhalb der Isogenieklasse von $G_{1,1}^{\oplus 2}$ gibt. Diese Tatsache ist a priori

nicht klar. Im Lichte von Proposition 3.59 folgt sie aus der Existenz von verschiedenen Singularitäten supersingulärer Kummer-Flächen in Theorem 3.4.

Als Anwendung der vorgestellten Resultate können nun die Singularitäten weiterer wilder Kummer-Varietäten bis auf formale Isomorphie bestimmt werden. Es gelte nun für die Charakteristik des Grundkörpers $p = 2$.

Proposition 3.59. *Es seien A und B abelsche Varietäten über k und es gelte* $\mathrm{char}(k) = 2$. *Weiter seien $X = A/\iota_A$ und $Y = B/\iota_B$ die Quotienten nach der Gruppenwirkung durch die jeweilige Vorzeicheninvolution und $x \in X$, $y \in Y$ die Bildpunkte der neutralen Elemente. Wenn die formalen Gruppen $\hat{A}$ und $\hat{B}$ isomorph sind, dann sind die Singularitäten an x und y formal isomorph. Insbesondere ist in diesem Fall $x \in X$ genau dann ein regulärer Punkt, wenn $y \in Y$ regulär ist.*

Beweis. Es bezeichne $\phi\colon \hat{A} \to \hat{B}$ den Isomorphismus. Die Schemata A und B sind von gleicher Dimension, also $\hat{A} \cong \hat{B} \cong \mathrm{Spf}(R)$ als formale Spektren mit $R = k[\![T_1, \ldots, T_g]\!]$. Wir erhalten dadurch einen induzierten Automorphismus $\phi^*\colon R \to R$, ebenso werden durch die Involutionen Automorphismen ι_A^* und ι_B^* der k-Algebra R induziert. Letztere können als die Wirkung auf den vervollständigten Halmen $\hat{\mathcal{O}}_{A,e_A}$ bzw. $\hat{\mathcal{O}}_{B,e_B}$ gedeutet werden. Es reicht nun zu zeigen, dass die Invariantenringe $R^{\iota_A^*}$ und $R^{\iota_B^*}$ isomorph sind, da das Bilden von Invariantenringen mit Vervollständigung kommutiert.

Aus der Kompatibilität von ϕ mit den Gruppengesetzen folgt $\iota_A^* = \phi^* \circ \iota_B^* \circ (\phi^*)^{-1}$. Wir zeigen nun die Gleichheit $R^{\iota_A^*} = \phi^*(R^{\iota_B^*})$, um den Beweis zu vollenden: Ist $f \in R^{\iota_B^*}$, so ist

$$\iota_A^*(\phi^*(f)) = \phi^* \circ \iota_B^* \circ (\phi^*)^{-1} \circ \phi^*(f) = \phi^*(f),$$

also ist $\phi^*(f) \in R^{\iota_A^*}$. Indem man ϕ^* durch ϕ^{*-1} ersetzt, erhält man mit dem gleichen Argument die Inklusion $\phi^{*-1}(R^{\iota_A^*}) \subset R^{\iota_B^*}$. Erneutes Anwenden von ϕ^* liefert die noch fehlende Inklusion. □

Korollar 3.60. *Es sei A eine g-dimensionale abelsche Varietät über k (mit $p = 2$) und es bezeichne $2^r = |\ker(2_A)(k)|$ die Anzahl der 2-Torsionspunkte von A. Wir definieren $B = E_1 \times \ldots \times E_g$ als Produkt von r gewöhnlichen und $g - r$ supersingulären elliptischen Kurven. Wenn $r = g$ oder $r = g - 1$ gilt, dann sind die Singularitäten der Kummer-Varietäten von A und B formal isomorph.*

Beweis. Die Voraussetzung stellt sicher, dass $\hat{A} \sim G_{1,0}^{\oplus r} \oplus G_{1,1}^{\oplus g-r}$ gilt. Die Aussage folgt nun unmittelbar aus den Propositionen 3.50, 3.58 und 3.59. □

Die Beschreibung von Kummer-Varietäten, die von Produkten elliptischer Kurven stammen, schließt also den Fall von beliebigen Kummer-Varietäten mit p^g oder p^{g-1} singulären Punkten mit ein.

Literaturverzeichnis

[1] M. Artin: *Coverings of the rational double points in characteristic p*. Erschienen in: W. L. Baily Jr., T. Shioda (Hrsg.): *Complex analysis and algebraic geometry*, S. 11-22. Cambridge University Press, Cambridge (1977).

[2] M. Artin: *Wildly ramified $Z/2$ actions in dimension two*. Proceedings of the American Mathematical Society 52, Nr. 1 (1975), S. 60-64.

[3] L. Bădescu: *Algebraic surfaces*. Springer, New York (2001).

[4] C. Birkenhake, H. Lange: *Complex abelian varieties*, 2. Ausgabe. Grundlehren der Mathematischen Wissenschaften 302. Springer, Berlin (2004).

[5] E. Bombieri, W. Gubler: *Heights in Diophantine geometry*. Cambridge University Press, Cambridge (2006).

[6] A. Borel: *Linear algebraic groups*, 2. Ausgabe. Graduate Texts in Mathematics 126. Springer, New York (1991).

[7] N. Bourbaki: *Algebra II: Chapters 4-7*. Elements of Mathematics. Springer, Berlin (1990).

[8] W. Bruns, J. Herzog: *Cohen-Macaulay rings*. Cambridge Studies in Advanced Mathematics 39. Cambridge University Press, Cambridge (1993).

[9] H. E. A. Campbell, I. P. Hughes: *Vector invariants of $U_2(F_p)$: a proof of a conjecture of Richman*. Advances in Mathematics 126, Nr. 1 (1997), S. 1-20.

[10] H. E. A. Campbell, D. L. Wehlau: *The second main theorem vector for the modular regular representation of C_2*. Advances in Mathematics 252 (2014), S. 641-651.

[11] M. Demazure, A. Grothendieck: *Séminaire de géométrie algébrique du Bois Marie: Schémas en groupes (SGA 3)*, Band 1. Lecture Notes in Mathematics 151. Springer, Berlin (1970).

[12] H. Derksen, G. Kemper: *Computational invariant theory*, 2. erweiterte Ausgabe. Encyclopaedia of Mathematical Sciences 130. Springer, Berlin Heidelberg (2015).

[13] I. Dolgachev: *Abstract configurations in algebraic geometry*. Erschienen in: A. Collino et al. (Hrsg.): *The Fano conference*, S. 423-462. Dipartimento di Matematica dell'Università di Torino, Turin (2004).

[14] I. Dolgachev, D. Lehavi: *On isogenous principally polarized abelian surfaces*. Erschienen in: V. Alexeev et al. (Hrsg.): *Curves and abelian varieties*, S. 51-69. Contemporary Mathematics 465. American Mathematical Society, Providence, RI (2008).

[15] I. Dolgachev, D. Ortland: *Point sets in projective spaces and theta functions*. Astérisque 165. Société Mathématique de France, Paris (1988).

[16] D. Eisenbud: *Commutative algebra: with a view toward algebraic geometry*. Graduate Texts in Mathematics 150. Springer, New York (2004).

[17] G. Ellingsrud, T. Skjelbred: *Profondeur d'anneaux d'invariants en caractéristique p*. Compositio Mathematica 41, Nr. 2 (1980), S. 233-244.

[18] J. Fogarty: *On the depth of local rings of invariants of cyclic groups*. Proceedings of the American Mathematical Society 83, Nr. 3 (1981), S. 448-452.

[19] P. Gabriel: *La localisation dans les anneaux non commutatifs*. Séminaire Dubreil. Algèbre et théorie des nombres 13, Nr. 1 (1959-1960), S. 2.01-2.35.

[20] M. R. Gonzalez-Dorrego: *(16,6) configurations and geometry of Kummer surfaces in* $\mathbb{P}^3$. Memoirs of the American Mathematical Society 512. American Mathematical Society, Providence, RI (1994).

[21] U. Görtz, T. Wedhorn: *Algebraic geometry I*. Vieweg & Teubner, Wiesbaden (2010).

[22] A. Grothendieck: *Séminaire de géométrie algébrique du Bois Marie: Revêtements étales et groupe fondamental (SGA 1)*. Lecture Notes in Mathematics 224. Springer, Berlin (1971).

[23] T. H. Gulliksen, G. Levin: *Homology of local rings*. Queen's Papers in Pure and Applied Mathematics 20. Queen's University, Kingston, Ont. (1969).

[24] R. Hartshorne: *Algebraic geometry*. Graduate Texts in Mathematics 52. Springer, New York (2006).

[25] H. Hauser: *Blowups and resolution*. Erschienen in: D. Ellwood et al. (Hrsg.): *The resolution of singular algebraic varieties*, S. 1-80. Clay Mathematics Proceedings 20. American Mathematical Society, Providence, RI (2014).

[26] M. Hazewinkel: *Formal groups and applications*. Pure and Applied Mathematics 78. Academic Press, New York (1978).

[27] H. Hironaka: *Resolution of singularities of an algebraic variety over a field of characteristic zero I, II.* Annals of Mathematics 79, Nr. 1 (1964), S. 109-203 und S. 205-326.

[28] H. Hironaka: *Resolution of singularities in positive characteristics.* Verfügbar unter http://www.math.harvard.edu/∼hironaka (2017).

[29] M. Hochster, J. A. Eagon: *Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci.* American Journal of Mathematics 93, Nr. 4 (1971), S. 1020-1058.

[30] R. W. H. T. Hudson: *Kummer's quartic surface*, bearbeiteter Neudruck der Originalversion von 1905. Cambridge Mathematical Library. Cambridge University Press, Cambridge (1990).

[31] H. Ito, S. Schröer: *Wildly ramified actions and surfaces of general type arising from Artin-Schreier curves.* Erschienen in: C. Faber et al. (Hrsg.): *Geometry and arithmetic*, S. 213-241. EMS Series of Congress Reports 8. European Mathematical Society, Zürich (2012).

[32] T. Katsura: *On Kummer surfaces in characteristic 2.* Erschienen in: M. Nagata (Hrsg.): *Proceedings of the International Symposium on Algebraic Geometry, Kyoto, 1977*, S. 525-542. Books Kinokuniya, Tokyo (1978).

[33] S. L. Kleiman: *The Picard scheme.* Erschienen in: B. Fantechi et al.: *Fundamental algebraic geometry: Grothendieck's FGA explained*, S. 235-321. Mathematical Surveys and Monographs 123. American Mathematical Society, Providence, RI (2005).

[34] H. Knörrer: *Die Fresnelsche Wellenfläche.* Erschienen in: H. Knörrer et al.: *Arithmetik und Geometrie: Vier Vorlesungen*, S. 115-141. Mathematische Miniaturen 3. Birkhäuser, Basel (1986).

[35] E. E. Kummer: *Über die Flächen vierten Grades mit sechzehn singulären Punkten.* Enthalten in: E. E. Kummer, A. Weil (Hrsg.): *Collected papers II: Function theory, geometry and miscellaneous*, S. 418-432. Springer, Berlin (1975).

[36] Q. Liu: *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics 6. Oxford University Press, Oxford (2006).

[37] Y. I. Manin: *On the theory of abelian varieties over a field of finite characteristic.* Erschienen in: N. I. Ahiezer et al.: *American Mathematical Society translations: Fifteen papers on algebra*, Serie 2, Nr. 50, S. 127-140. American Mathematical Society, Providence, RI (1966).

[38] Y. I. Manin: *The theory of commutative formal groups over fields of finite characteristic.* Russian Mathematical Surveys 18, Nr. 6 (1963), S. 1-83.

[39] H. Matsumura: *Commutative ring theory*. Cambridge Studies in Advanced Mathematics 8. Cambridge University Press, Cambridge (1989).

[40] J. S. Milne: *Abelian varieties*. Erschienen in: G. Cornell, J. H. Silverman (Hrsg.): *Arithmetic geometry*, S. 103-150. Springer, New York (1986).

[41] J. S. Milne: *Jacobian varieties*. Erschienen in: G. Cornell, J. H. Silverman (Hrsg.): *Arithmetic geometry*, S. 167-212. Springer, New York (1986).

[42] D. Mumford: *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics 5. Oxford University Press, Oxford (1970).

[43] D. Mumford, J. Fogarty: *Geometric invariant theory*, 2. erweiterte Ausgabe. Ergebnisse der Mathematik und ihrer Grenzgebiete 34. Springer, Berlin (1982).

[44] F. Oort: *Commutative group schemes*. Lecture Notes in Mathematics 15. Springer, Berlin (1966).

[45] B. Peskin: *Quotient-singularities and wild p-cyclic actions*. Journal of Algebra 81, Nr. 1 (1983), S. 72-99.

[46] C. P. Ramanujam: *On a geometric interpretation of multiplicity*. Inventiones Mathematicae 22 (1973), S. 63-67.

[47] D. R. Richman: *On vector invariants over finite fields*. Advances in Mathematics 81, Nr. 1 (1990), S. 30-65.

[48] S. Schröer: *The Hilbert scheme of points for supersingular abelian surfaces*. Arkiv för Matematik 47, Nr. 1 (2009), S. 143-181.

[49] F. Schüller: *On taut singularities in arbitrary characteristics*. arXiv:1303.6128 (2013).

[50] R. J. Shank, D. L. Wehlau: *Computing modular invariants of p-groups*. Journal of Symbolic Computation 34, Nr. 5 (2002), S. 307-327.

[51] T. Shioda: *Kummer surfaces in characteristic 2*. Proceedings of the Japan Academy 50, Nr. 9 (1974), S. 718-722.

[52] J. Silverman: *The arithmetic of elliptic curves*, 2. Ausgabe. Graduate Texts in Mathematics 106. Springer, Dordrecht (2009).

[53] J. T. Tate: *p-divisible groups*. Erschienen in: T. A. Springer (Hrsg.): *Proceedings of a conference on local fields*, S. 158-183. Springer, Berlin (1967).

[54] P. Wagreich: *Elliptic singularities of surfaces*. American Journal of Mathematics 92, Nr. 2 (1970), S. 419-454.

[55] K. Watanabe: *Certain invariant subrings are Gorenstein II*. Osaka Journal of Mathematics 11, Nr. 2 (1974), S. 379-388.

[56] O. Zariski: *Analytical irreducibility of normal varieties*. Annals of Mathematics 49, Nr. 2 (1948), S. 352-361.

[57] O. Zariski: *Sur la normalité analytique des variétés normales*. Annales de l'Institut Fourier 2 (1950), S. 161-164.

Tabellen- und Abbildungsverzeichnis

Abbildungen

Abb. 1 Reelles Bild einer Kummer-Fläche (verschiedene Perspektiven), def. durch $x^4+y^4+z^4-x^2y^2-x^2z^2-y^2z^2-x^2-y^2-z^2+1=0$, erstellt mit der Visualisierungssoftware *Surfer* 1
Abb. 2 Auflösung der A_1-Singularität (reelles Bild), erstellt mit der Visualisierungssoftware *Surfer* 3
Abb. 3 Veranschaulichung der Zählung in (2.3) 44
Abb. 4 Kummer-Konfigurationen: $(1,0)$, $(4,1)$ und $(16,6)$ 53
Abb. 5 $(64,28)$-Konfiguration, Darstellung mit Würfel-Querschnitten 56
Abb. 6 Anordnung der Automorphismen im Würfel (Querschnitte) 60
Abb. 7 Duale Graphen zur Auflösung der Singularitäten 65

Tabellen

Tab. 1 Rationale Doppelpunkte in Charakteristik 2 nach Artin [1] 66
Tab. 2 Formale Gruppen abelscher Varietäten 102