

Zur Berechnung von Mordell-Weil Basen elliptischer Kurven über globalen Funktionenkörpern

Von der Fakultät für Mathematik und Naturwissenschaften der Carl von Ossietzky
Universität Oldenburg zur Erlangung des Grades und Titels eines Doktors der Na-
turwissenschaften (Dr. rer. nat.)

angenommene Dissertation

von Herrn Gerriet Möhlmann
geboren am 10.8.1982 in Berlin.

Gutachter: Prof. Dr. Florian Heß
Zweitgutachter: Prof. Dr. Michael Pohst

Tag der Disputation: 09.01.2014

Zusammenfassung

Deutsch

In dieser Arbeit beschäftigen wir uns mit der Berechnung von Mordell-Weil-Basen für eine elliptische Kurve A über einem globalen Funktionenkörper K . Insbesondere interessiert uns dabei der Fall $\text{char } K = 2$. Im ersten Teil verwenden wir kohomologische Methoden, um explizite Konstruktionen für neue Abstiegs-Abbildungen in verschiedenen Situationen anzugeben und um ihre Bilder über einer Vervollständigung K_v von K zu beschreiben. Weiterhin untersuchen wir, wie sich anhand dieser lokalen Informationen die Selmergruppe und mit dieser wiederum Schranken für den Rang sowie unabhängige Punkte auf $A(K)$ berechnen lassen. Im zweiten Teil konzentrieren wir uns auf den algorithmischen Aspekt des Problems. Wir beschreiben, welche Schritte notwendig sind, um unsere theoretischen Überlegungen in einem Algorithmus umzusetzen und formulieren Aussagen über die Laufzeit. Des Weiteren beschäftigen wir uns mit der Berechnung sowie der Minimierung und Reduktion von Modellen für Kurven vom Geschlecht eins. Im dritten Viertel der Arbeit präsentieren wir Resultate über die Höhen von Punkten auf $A(K)$. Diese liefern uns die fehlenden Bausteine für die Durchführung eines unendlichen Abstiegs. Weiterhin kombinieren wir unsere Überlegungen zu Höhen und zu den Abstiegs-Abbildungen, um auf diese Weise explizite Schranken für die Höhe ganzer Punkte auf $A(K)$ zu ermitteln. Diese Schranken verwenden wir, um verschiedene Methoden zur Berechnung aller ganzen Punkte vorzustellen und zu vergleichen. Im letzten Teil der Arbeit wenden wir unsere Algorithmen auf eine Vielzahl von relevanten Beispielen an, um die Möglichkeiten, aber auch die Grenzen unserer Implementation zu veranschaulichen.

Englisch

This thesis deals with the computation of Mordell-Weil bases for an elliptic curve A over a global function field K with focus on the case $\text{char } K = 2$. In the first part we use cohomological methods to construct explicit formulas for new descent maps in various settings and to describe their images over completions K_v of K . Moreover we examine how this local information can be combined to calculate the Selmer group which in turn yields upper bounds for the rank and helps calculating points on $A(K)$. In the second part we focus on the algorithmic aspect of our goal. We describe the steps that are necessary to turn our theoretical ideas into an algorithm and analyse its running time. Furthermore we deal with the problems of both computing as well as minimizing and reducing models of genus one curves. In the third quarter of the thesis we formulate statements about the height of points on $A(K)$. This yields a way to do an infinite descent. By combining the results about heights and descent maps, we are able to compute explicit bounds for the height of integral points on $A(K)$. Using these bounds we present and compare different methods to compute the integral points. In the last part our algorithms are applied to a large number of relevant examples to illustrate the potential but also the limits of our implementation.

Ich möchte an dieser Stelle Herrn Prof. Dr. Florian Heß ganz herzlich für die angenehme Zusammenarbeit und für zahlreiche hilfreiche Gespräche während der Anfertigung dieser Arbeit danken.
Ferner danke ich Herrn Prof. Dr. Dr. h.c. M. E. Pohst für seine Unterstützung und die Übernahme des Koreferats.

Inhaltsverzeichnis

Inhaltsverzeichnis	i
Einleitung	1
1 Die Abstiegs-Abbildung	5
1.1 Notation	5
1.2 Grundlagen	6
1.3 Die Abstiegs-Abbildung	7
1.4 Lokale Bilder	18
1.5 Globale Selmergruppen	26
1.6 Globale Bilder	29
1.7 Keine volle p^2 -Torsion	36
2 Algorithmische Details	43
2.1 Der Algorithmus	43
2.2 Berechnung der endlichen Untergruppe R_0	44
2.3 Berechnung der Selmergruppe	46
2.4 Globales Bild	52
2.5 Kombinieren von Abstiegs-Abbildungen	62
2.6 Implementation	65
3 Höhen und Anwendungen	67
3.1 Unendlicher Abstieg	67
3.2 Ganze Punkte	69
3.3 Berechnung von Endomorphismen	76
4 Rechnungen	77
4.1 Ein Beispiel von Kramer	77
4.2 Ein Beispiel von Ulmer	78
4.3 Reduktion	79
4.4 Große Koordinaten	81
4.5 Sieben	83
4.6 Berechnung ganzer Punkte	84
4.7 Vergleich mit Magma	85
5 Schluss	87
5.1 Weitere Methoden	87
5.2 Richtungen für zukünftige Arbeiten	88

6 Anhang	89
6.1 Gruppenschema	89
6.2 Kohomologie	92
6.3 Rechnungen und Beweise	94
Literaturverzeichnis	103

Einleitung

Die Berechnung und Beschreibung ihrer rationalen Punkte gehört zu den fundamentalen Problemen für eine elliptische Kurve. Der Schwierigkeitsgrad und die Beschaffenheit einer Lösung hängen stark von dem auftretenden Grundkörper ab. Elliptische Kurven über \mathbb{C} besitzen überabzählbar viele \mathbb{C} -rationale Punkte und diese können mit einem eindimensionalen komplexen Torus assoziiert werden. Auf der anderen Seite besitzen elliptische Kurven über einem endlichen Körper nur endlich viele rationale Punkte. Der Satz von Hasse liefert eine gute Abschätzung für ihre Anzahl. Die Untersuchung ihrer Gruppenstruktur ist für verschiedene kryptographische Fragestellungen relevant. Der Satz von Mordell-Weil besagt, dass für einen globalen Körper die Gruppe der rationalen Punkte endlich erzeugt ist. Der in [Sil86] gegebene Beweis gilt zwar nur in Charakteristik 0, lässt sich aber ziemlich direkt auf globale Funktionenkörper übertragen. Für Beweise unter teilweise noch schwächeren Voraussetzungen siehe zum Beispiel [Ulm09], [LN59], [Lan83]. Es wird verwendet, dass auch in dieser Situation die Klassengruppe und Einheitengruppe des Grundkörpers endlich bzw. endlich erzeugt sind. Der Beweis liefert aber keine Anleitung, wie die Erzeuger oder auch nur ihre Anzahl bestimmt werden kann. Erste Ideen für einen Algorithmus zur Beantwortung genau dieser Fragen gehen auf Birch und Swinnerton-Dyer [BSD63, BSD65] zurück. Sie geben für elliptische Kurven über \mathbb{Q} einen auf Invariantentheorie basierenden Algorithmus an, der diese Probleme zwar nicht immer löst, zumindest aber obere Schranken und unabhängige Punkte berechnet. Seitdem hat sich vieles auf diesem Gebiet getan. Wichtige Resultate sind:

- Den Ansatz von Birch und Swinnerton-Dyer aufgreifend, entwickelt Cremona einen Algorithmus für einen invariantentheoretischen 2-Abstieg. Seine effiziente Implementation [Cre, Cre97] wird benutzt, um systematisch große Mengen an Beispielen zu untersuchen, siehe [Cre06].
- In [MSS96] und [Wom03] beschreiben Merriman, Siksek, Smart und später Womack die Idee für einen 4-Abstieg. Diese wird in [Sta05] zu einem 8-Abstieg erweitert.
- Simon beschreibt in [Sim02] einen Algorithmus für einen 2-Abstieg über Zahlkörpern im Unterschied zu den vorherigen Methoden, die meist auf Kurven über \mathbb{Q} beschränkt waren.
- In [Ban04], [CP09], [Fis00] werden Ideen für einen 3-, 5- und 7-Abstieg entwickelt.
- In einer Reihe von Arbeiten untersuchen erst Schaefer und Stoll in [SS04] und dann Cremona, Fisher, O’Neil, Simon und Stoll in [CFO⁺08], [CFO⁺09] und [CFO⁺] allgemeine p - bzw. n -Abstiege. Creutz erweitert diese Idee in [Cre10] zu p^2 -Abstiegen.

Die oben beschriebenen Methoden können grob in zwei Gruppen unterteilt werden. Die eine wird als „direkt“ oder „algebraisch“, die andere als „indirekt“ oder „invariantentheoretisch“ bezeichnet. Historisch gesehen waren die ersten Methoden alle indirekt, denn zu der damaligen Zeit waren die für die direkte Methode benötigten zahlentheoretischen Aufgaben noch nicht lösbar. Doch mit den Weiterentwicklungen auf dem Gebiet der Klassengruppen- und Einheitengruppenberechnung haben sich die direkten Methoden mehr und mehr durchgesetzt und auch bei der in dieser Arbeit vorgestellten handelt es sich um eine direkte Methode. Für einen ausführlichen Vergleich der beiden Ansätze sei auf [DS98] verwiesen. Die oben aufgezählten Resultate beziehen sich größtenteils auf elliptische Kurven über Zahlkörpern. Doch auch in Charakteristik p wurden einige Ergebnisse erzielt.

- Kramer stellt in [Kra77] einen 2-Abstieg für gewöhnliche elliptische Kurven in Charakteristik 2 vor. Große Teile dieser Arbeit basieren auf diesem Artikel.
- Voloch präsentiert in [Vol90] einen p -Abstieg in Charakteristik p für $p \geq 3$. In [Bro97] werden diese Resultate von Broumas weiterentwickelt.
- In [Ulm91] untersucht Ulmer die Kohomologie, die hinter einem p -Abstieg in Charakteristik p steht.
- Roberts beschreibt und implementiert in [Rob07] einen 2-Abstieg für elliptische Kurven mit voller 2-Torsion über rationalen Funktionenkörpern der Charakteristik $p \geq 5$.

Abgesehen von [Rob07] sind diese Arbeiten eher theoretisch und zielen weniger auf die konkrete Berechnung von Mordell-Weil-Basen ab.

Die Gründe, sich für die Berechnung von Mordell-Weil-Basen elliptischer Kurven über globalen Funktionenkörpern zu interessieren, sind zahlreich und gleichen denen für elliptische Kurven über Zahlkörpern. Die berühmte Birch-Swinnerton-Dyer-Vermutung setzt arithmetische Daten wie den Rang der Kurve mit analytischen Daten, nämlich der Nullstellenordnung der L -Funktion im Punkt 1 in Verbindung. Ihr Beweis steht auch über Funktionenkörpern noch aus. Siehe [Ulm09] für einen Überblick über bekannte Resultate. Die Berechnung von Mordell-Weil-Basen hilft uns, die arithmetische Seite besser zu verstehen, indem sie uns nicht nur Auskünfte über den Rang gibt, sondern auch bei der Beschreibung von Elementen der Shafarevich-Tate-Gruppe von Nutzen ist. Des Weiteren kann sich die Kenntnis einer Mordell-Weil-Basis für die Lösung anderer Fragestellungen als hilfreich erweisen. Ein prominentes Beispiel, auf das wir im Verlauf dieser Arbeit genauer eingehen werden, ist die Berechnung ganzer Punkte auf elliptischen Kurven, siehe auch [GPZ94]. Im Allgemeinen ist es für einen n -Abstieg notwendig, Rechnungen in dem Körper, über dem die Kurve volle n -Torsion besitzt, durchzuführen. Daher werden in der Praxis meist sehr kleine n verwendet. Aus diesem Grunde ist ein 2-Abstieg auch in Charakteristik 2 interessant. Die Vorteile, die das Rechnen über potentiell einfacheren Körpern bringt, liefern eine ausreichende Begründung, sich genauer mit der tendenziell komplizierteren Theorie dahinter zu beschäftigen.

Ziel dieser Arbeit ist es, explizite Methoden zur Berechnung von Mordell-Weil-Basen über globalen Funktionenkörpern anzugeben und diese auch algorithmisch umzusetzen. Dabei untersuchen wir, in wie weit sich die Methoden, die über Zahlkörpern verwendet werden, auch auf globale Funktionenkörper übertragen lassen. Auf diese Weise befreien wir den Ansatz von Roberts [Rob07] von den bei ihm verwendeten

Einschränkungen und verallgemeinern seine Arbeit. Des Weiteren untersuchen wir Methoden, die kein Analogon in Charakteristik 0 besitzen. Dazu greifen wir die Ideen der oben zitierten Arbeiten zu p -Abstiegen in Charakteristik p auf und untersuchen, wie sie sich algorithmisch umsetzen lassen. Zu dem bei Kramer in [Kra77] beschriebenen 2-Abstiegen für gewöhnliche elliptische Kurven in Charakteristik 2 konstruieren wir einen 4-Abstieg und einen 2-Abstieg für supersinguläre elliptische Kurven. Während das Augenmerk zuvor eher auf der Berechnung des Ranges lag, kombinieren wir unsere Resultate mit Ergebnissen von Cremona, Fisher und Stoll und stellen die bislang eher abstrakten Elemente der Selmergruppen als explizite homogene Räume dar. Diese verwenden wir, um unabhängige Punkte auf elliptischen Kurven zu berechnen. Anschließend übertragen wir Sikseks unendlichen Abstieg – siehe [Sik95] – auf unsere Situation und zeigen, wie sich auf diese Weise unabhängige Punkte zu einer vollen Mordell-Weil-Basis erweitern lassen. Die von uns beschriebenen Algorithmen haben wir für elliptische Kurven über rationalen Funktionenkörpern in Magma [BCP97] implementiert. Die Implementationen sollten sich aber ohne große Schwierigkeiten auch auf beliebige globale Funktionenkörper erweitern lassen.

Die Arbeit gliedert sich wie folgt:

Im ersten Kapitel geben wir eine kurze Zusammenfassung der benötigten Grundlagen. Anschließend beschreiben wir, wie Abstiegs-Abbildungen in verschiedenen Situationen konstruiert werden können. Wir beweisen eine Orthogonalitätsaussage für die Bilder der Abstiegs-Abbildungen über lokalen Körpern und verwenden diese, um Aussagen über eben jene Bilder zu treffen. Danach zeigen wir, wie sich die lokalen Informationen zu globalen kombinieren lassen und beschreiben, wie diese zur Konstruktion unabhängiger Punkte auf der elliptischen Kurve verwendet werden können.

Das zweite Kapitel widmet sich den algorithmischen Aspekten des Problems. Wir beschreiben, welche Schritte für einen Abstieg durchgeführt werden und wie sich diese algorithmisch realisieren lassen. Des Weiteren geben wir Auskunft über die Komplexität einiger Unterprobleme und analysieren, wie sich verschiedene Teilschritte beschleunigen lassen.

Im dritten Kapitel beschäftigen wir uns mit Höhen. Wir beschreiben, wie die kanonische Höhe verwendet werden kann, um aus unabhängigen Punkten eine Mordell-Weil-Basis zu berechnen. Des Weiteren stellen wir Methoden zur Berechnung ganzer Punkte auf elliptischen Kurven in Charakteristik 2 vor.

Im vierten Kapitel geben wir zahlreiche Beispielrechnungen an, die wir mit unserer Magma Implementation durchgeführt haben. Anhand dieser veranschaulichen wir die Laufzeiten der verschiedenen Schritte. Des Weiteren vergleichen wir verschiedene Methoden zur Berechnung ganzer Punkte.

Im fünften Kapitel geben wir einen kurzen Überblick über die nicht in dieser Arbeit behandelten Methoden zur Berechnung des Ranges einer elliptischen Kurven über einem globalen Funktionenkörper. Weiterhin zeigen wir einige Richtungen für zukünftige Arbeiten auf.

Der Anhang gibt eine kurze Zusammenfassung über endliche flache Gruppenschemata und ihre Kohomologietheorie, welche wir zuvor verwendetet haben.

Kapitel 1

Die Abstiegs-Abbildung

In diesem Kapitel beschäftigen wir uns mit Abstiegs-Abbildungen. Der erste Abschnitt beschreibt die theoretischen Grundlagen ihrer Konstruktion und gipfelt in den damit ermittelten expliziten Formeln in den Lemmata 1.3.4, 1.3.7, 1.3.9 und 1.3.12. Anschließend beweisen wir in Theorem 1.4.2 eine allgemeine Orthogonalitätsaussage und verwenden diese in den Aussagen 1.4.9, 1.4.12, 1.4.16 zur Beschreibung der lokalen Bilder der zuvor konstruierten Abbildungen. Wir kombinieren die lokalen Aussagen zu den globalen Resultaten 1.5.1, 1.5.5 und 1.5.6. Des Weiteren beschreiben wir in Abschnitt 1.6 die Konstruktion von expliziten Modellen für homogene Räume in den verschiedenen Situationen und zeigen, wie diese zur Berechnung unabhängiger Punkte auf den jeweiligen elliptischen Kurven verwendet werden können.

1.1 Notation

Im Verlauf der Arbeit werden wir von verschiedenen Notationen regelmäßig Gebrauch machen. Mit K bezeichnen wir einen globalen Körper, von dem wir annehmen, dass er in einem festen algebraischen Abschluß \bar{K} liegt und mit $K^{\text{sep}} \subseteq \bar{K}$ bezeichnen wir den separablen Abschluß von K . Die Galoisgruppe $\text{Gal}(K^{\text{sep}}/K)$ nennen wir die absolute Galoisgruppe von K und schreiben abkürzend auch G_K . Für eine Bewertung v von K werden wir die Vervollständigung von K an v mit K_v und den Bewertungsring von K_v mit R_v bezeichnen. Für den Restklassenkörper von K_v verwenden wir das Symbol k . Ist K ein globaler Funktionenkörper, so verlangen wir, dass der Konstantenkörper gleich der volle Konstantenkörper ist.

Ist C eine algebraische Kurve über K und $K' \supseteq K$ ein Erweiterungskörper, dann nennen wir die Menge der Punkte von C mit Koordinaten in K' die K' -rationalen Punkte von C und schreiben $C(K')$. Da wir K mit einem Teilkörper von K_v identifizieren können, ergibt es auch Sinn, von den K_v -rationalen Punkten einer Kurve C über K zu reden. Die von uns betrachteten Kurven sind im Allgemeinen glatt und projektiv. Je nach Situation betrachten wir Punkte auf Kurven manchmal als in einen affinen und manchmal als in einen projektiven Raum eingebettet.

Ist $\phi : A \rightarrow B$ eine Isogenie zweier elliptischer Kurven A und B über K , so bezeichnen wir mit $A[\phi]$ ihren Kern und reden von der ϕ -Torsion oder den ϕ -Torsionspunkten. Die Vereinigung der Kerne aller Isogenien nennen wir die Torsionsuntergruppe A_{tor} . Für den Schnitt von $A(K')$ und $A[\phi]$ oder A_{tor} schreiben wir $A(K')[\phi]$ bzw. $A(K')_{\text{tor}}$. Bei allen diesen Teilmengen handelt es sich um Untergruppen von A beziehungsweise

von $A(K')$. Ist die Isogenie die Multiplikation mit einer ganzen Zahl n , so bezeichnen wir sie auch $[n]$, sprechen aber von den n -Torsionspunkten und schreiben $A[n]$ für sie. Wir benutzen die Bezeichnung ϕ^\vee für die duale Isogenie zu ϕ .

1.2 Grundlagen

Die in diesem Abschnitt vorgestellten Definitionen und Aussagen lassen sich in verschiedenen Büchern nachlesen. Neben vielen anderen kommen dafür zum Beispiel die Bücher [Sil86], [Sil94], [Lan78] und [KM85] in Frage.

Sei A eine elliptische Kurve über einem globalen Funktionenkörper K der Charakteristik p gegeben durch die Weierstraß-Gleichung

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

Dann bezeichnen wir mit $A^{(p^n)}$ die durch die Weierstraß-Gleichung

$$y^2 + a_1^{p^n}xy + a_3^{p^n}y = x^3 + a_2^{p^n}x^2 + a_4^{p^n}x + a_6^{p^n}$$

gegebene elliptische Kurve. Die Abbildung $F^n : A \rightarrow A^{(p^n)}$, $(x, y) \mapsto (x^{p^n}, y^{p^n})$ ist eine Isogenie. Wir nennen sie p^n -Frobenius, aber wenn klar ist, was p und n sind, schreiben wir gelegentlich auch nur *Frobenius*. Mit $V^n : A^{(p^n)} \rightarrow A$ bezeichnen wir die duale Isogenie des p^n -Frobenius und nennen sie die p^n -Verschiebung. Sowohl bei F^n als auch bei V^n handelt es sich um eine zyklische Isogenie vom Grad p^n .

Wir nennen A *gewöhnlich*, wenn A nichttriviale Punkte der Ordnung p besitzt und *supersingulär*, falls das nicht der Fall ist. Es zeigt sich, dass A genau dann gewöhnlich ist, wenn V^n für ein und somit alle n separabel ist.

In Charakteristik 2 ist eine elliptische Kurve genau dann gewöhnlich, wenn der Koeffizient a_1 der Weierstraß-Gleichung ungleich null ist. In diesem Fall können wir eine Variablentransformation durchführen und erhalten eine kurze Weierstraß-Gleichung der Form $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ mit Diskriminante $\Delta = a_1^6 a_6 \neq 0$. Dann ist $(0, \sqrt{a_6})$ der nichttriviale 2-Torsionspunkt. Die Weierstraß-Gleichungen supersingulärer elliptischer Kurven hingegen lassen sich über Körpern der Charakteristik 2 immer in die Form $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ mit Diskriminante $\Delta = a_3^4 \neq 0$ bringen.

Wir nennen eine elliptische Kurve A über einem Funktionenkörper K *konstant*, wenn sie eine Weierstraß-Gleichung besitzt, bei der alle Koeffizienten a_i im Konstantenkörper von K liegen. Wir nennen A *isotrivial*, wenn K eine endliche Erweiterung L besitzt, so dass A über L konstant ist. Es zeigt sich, dass A genau dann isotrivial ist, wenn die j -Invariante $j(A)$ im Konstantenkörper von K liegt.

Für eine elliptische Kurve A über einem lokalen Körper K_v , definieren wir Untergruppen

$$A_0(K_v) := \{P \in A(K_v) \mid \text{Reduktion von } P \text{ liefert nichtsingulären Punkt auf reduzierter Kurve}\}$$

$$A_1(K_v) := \{P \in A(K_v) \mid \text{Reduktion von } P \text{ liefert neutrales Element der Gruppe der nichtsingulären Punkte der reduzierten Kurve}\}$$

Der Satz von Mordell-Weil besagt, dass für eine elliptische Kurve über einem globalen Körper K die Untergruppe der K -rationalen Punkte endlich erzeugt ist, d.h.

$$A(K) \simeq \mathbb{Z}^r \bigoplus A(K)_{\text{tor}}$$

mit $A(K)_{\text{tor}}$ endlich. Ein Beweis findet sich zum Beispiel bei [Lan83]. In diesem Kontext bezeichnen wir r als den *Rang* von $A(K)$ und Erzeuger des freien Anteils als eine *Mordell-Weil-Basis*. Im Folgenden werden wir uns der Frage widmen, wie sich unter bestimmten Voraussetzungen Aussagen über den Rang und über unabhängige Punkte auf $A(K)$ machen lassen. Die Technik, von der wir dabei Gebrauch machen wollen, nennt sich *Abstieg* und basiert darauf, die Kardinalität oder sogar Erzeuger der Menge $A(K)/nA(K)$ für ein $n \in \mathbb{N}^{\geq 2}$ zu finden. Da die Berechnung der Torsionspunkte vergleichsweise einfach ist, gehen wir davon aus, dass uns diese bekannt sind. Somit liefern uns die Kardinalität oder Erzeuger von $A(K)/nA(K)$ den Rang von $A(K)$ bzw. eine maximale unabhängige Menge von Punkten auf $A(K)$. Die Berechnung der Faktorgruppe $A(K)/nA(K)$ selbst lässt sich mitunter auf die Berechnung anderer Faktorgruppen reduzieren. Sei dazu B eine weitere elliptische Kurve über K und $\psi : A \rightarrow B$ eine K -rationale Isogenie vom Grad n mit dualer Isogenie ψ^\vee . Dann ist die Sequenz

$$\begin{aligned} 0 \rightarrow A(K)[\psi] \rightarrow A(K)[n] \rightarrow B(K)[\psi^\vee] \rightarrow B(K)/\psi(A(K)) \\ \rightarrow A(K)/nA(K) \rightarrow A(K)/\psi^\vee(B(K)) \rightarrow 0 \end{aligned} \quad (1.2.1)$$

exakt. Kennen wir den Rang oder Erzeuger für $B(K)/\psi(A(K))$ und $A(K)/\psi^\vee(B(K))$, so auch für $A(K)/nA(K)$.

1.3 Die Abstiegs-Abbildung

In diesem Abschnitt nehmen wir an, dass K ein Körper der Charakteristik p ist. Insbesondere interessieren uns dabei globale Funktionenkörper sowie ihre Vervollständigungen bezüglich einer Bewertung. Für elliptische Kurven A und B über K und eine über K rationale Isogenie $\psi : A \rightarrow B$ bezeichnen wir einen Gruppenmonomorphismus von $B(K)/\psi(A(K))$ in eine geeignete Gruppe R_ψ als eine ψ -Abstiegs-Abbildung. Im Folgenden untersuchen wir die Konstruktion solch einer Abbildung in unterschiedlichen Fällen. Als erstes betrachten wir für ψ die Multiplikation mit einer zur Charakteristik p teilerfremden Primzahlpotenz größer gleich zwei. Anschließend untersuchen wir die Situation für ψ die p^m -Verschiebung oder den p^m -Frobenius. Wie im vorherigen Abschnitt beschrieben, sind wir an Informationen über die Faktorgruppe $A(K)/nA(K)$ interessiert. Diese lassen sich mit Blick auf die exakte Sequenz 1.2.1 durch die Berechnung der Bilder der Abstiegs-Abbildungen finden. Daher sollten die Gruppen R_ψ eine Form besitzen, in der Rechnungen möglichst einfach durchzuführen sind. Des Weiteren verlangen wir, dass die Abstiegs-Abbildungen als Verbindungshomomorphismen zwischen gewissen Kohomologiegruppen entstehen. So können wir sicher gehen, dass die später verwendeten Techniken zur Berechnung des Bildes funktionieren.

Wir stellen die Konstruktion der V^m - und F^m -Abstiegs-Abbildung zunächst in voller Allgemeinheit vor. Wenn wir aber explizite Formeln angeben, dann beschränken wir uns auf die Fälle $m = 1$ und $m = 2$. Der Grund dafür ist, dass größere Werte von m zum gegenwärtigen Zeitpunkt für praktische Zwecke kaum verwendet werden können. Der Rechenaufwand, der für einen Abstieg für größere Werte von m sowohl bei der in den folgenden Abschnitten beschriebenen Berechnung der Selmergruppen, als auch bei der Berechnung von Modellen für die homogenen Räume, anfällt, ist im Allgemeinen zu groß.

1.3.1 n teilerfremd zur Charakteristik

Ist K ein Zahlkörper oder die Vervollständigung eines Zahlkörpers, so wurde die Konstruktion von n -Abstiegs-Abbildungen schon für verschiedene n detailliert untersucht. In der Einleitung dieser Arbeit findet sich eine Übersicht über einige der wichtigsten Resultate. Die verwendeten Techniken lassen sich relativ direkt auf Körper K der Charakteristik $p \geq 5$ koprim zu n übertragen und führen zu entsprechenden Abbildungen. Grund dafür ist, dass wir unter diesen Voraussetzungen ebenfalls mit einer kurzen Weierstraß-Gleichung und – da die Multiplikation mit n separabel ist – mit Methoden der Galoiskohomologie arbeiten können. Roberts konstruiert zum Beispiel auf diese Weise in [Rob07] eine 2-Abstiegs-Abbildung für einen rationalen Funktionenkörper K und eine elliptische Kurve A mit voller 2-Torsion über K . Diese beiden Einschränkungen können wir mit den bei [Sim02] oder [Wom03] beschriebenen Techniken leicht beseitigen. Der Übergang von rationalen zu beliebigen globalen Funktionenkörpern verläuft analog zu dem Übergang von \mathbb{Q} zu Zahlkörpern. Ist nicht die volle 2-Torsion rational, so müssen gewisse Rechnungen in dem Körper, in dem sie liegt, durchgeführt werden. Damit beantworten wir die entsprechenden Fragen, die Roberts in seiner Arbeit unter „Possible directions for further work“ stellt. Da sich weder die verwendeten Werkzeuge noch die konstruierten Abbildungen stark von denen über Zahlkörpern unterscheiden, verweisen wir an dieser Stelle nur auf die zitierten Arbeiten.

1.3.2 V^m -Abstieg

1.3.2.1 Allgemein

In diesem Abschnitt wollen wir eine V^m -Abstiegs-Abbildung α_m konstruieren. Wir nehmen an, dass A eine gewöhnliche elliptische Kurve ist. Die Überlegungen zu supersingulären A folgen später. Bei der Konstruktion von α_m arbeiten wir mit Wittvektoren. Wir geben hier nur kurz grundlegende Definitionen und Aussagen an. Details, Beweise und weitere Aussagen können zum Beispiel in [Lor90] und [Haz09] nachgelesen werden.

Sei K ein Körper der Charakteristik p , dann bezeichnen wir mit $W(K)$ die Menge der Folgen $x = (x_0, x_1, \dots)$ in K . Wir versehen $W(K)$ mit zwei inneren Verknüpfungen $+$ und \cdot . Dabei berechnet sich für $x = (x_0, x_1, \dots)$ und $y = (y_0, y_1, \dots)$ aus $W(K)$ die $(n+1)$ -te Komponente von $x \circ y$ mit $\circ \in \{+, \cdot\}$ über $(x \circ y)_n = S_n^\circ(x_0, y_0, \dots, x_n, y_n)$. Hierbei ist S_n° ein Polynom mit ganzzahligen Koeffizienten. So gilt zum Beispiel

$$(x + y)_0 = x_0 + y_0, (x + y)_1 = x_1 + y_1 + x_0^p + y_0^p - (x_0 + y_0)^p/p,$$

$$(x \cdot y)_0 = (x_0 y_0), (x \cdot y)_1 = x_0^p y_1 + y_0^p x_1.$$

Mit diesen Verknüpfungen wird $W(K)$ zu einem kommutativen Ring, in dem $(0, 0, \dots)$ das additive und $(1, 0, 0, \dots)$ das multiplikative neutrale Element sind. Auf den Wittvektoren haben wir den Frobenius-Operator

$$F : W(K) \rightarrow W(K), (x_0, x_1, \dots) \mapsto (x_0^p, x_1^p, \dots)$$

und die Verschiebung

$$V : W(K) \rightarrow W(K), (x_0, x_1, \dots) \mapsto (0, x_0, x_1, \dots).$$

Sie genügen der Relation

$$p(x_0, x_1, \dots) = VF(x_0, x_1, \dots) = FV(x_0, x_1, \dots) = (0, x_0^p, x_1^p, \dots).$$

Für $m \in \mathbb{N}$ liefert $V^m W(K)$ ein Ideal von $W(K)$. Den Faktorring $W(K)/V^m(W(K))$ bezeichnen wir mit $W_m(K)$ und identifizieren ihn mit Wittvektoren der Länge m . Da V und F kommutieren, liefert uns F auch einen Endomorphismus von $W_m(K)$. Die Abbildung

$$\wp : W_m(K) \rightarrow W_m(K), x \mapsto Fx - x$$

ist additiv und liefert daher einen Endomorphismus der additiven Gruppe von $W_m(K)$. Für ein Element $a \in K$ gilt $a^p = a$ genau dann, wenn a im Primkörper liegt. Daher gilt $\ker \wp = W_m(\mathbb{F}_p) \subseteq W_m(K)$. Somit ist $\ker \wp$ zyklisch und $(1, 0, 0, \dots, 0)$ ein Erzeuger. Dieser liefert einen Isomorphismus $\ker \wp \simeq \mathbb{Z}/p^m\mathbb{Z}$. Die Komponenten der Urbilder unter \wp sind die Nullstellen separabler Polynome, daher ist $\wp : W_m(K^{\text{sep}}) \rightarrow W_m(K^{\text{sep}})$ surjektiv. Die Artin-Schreier-Witt-Theorie beschäftigt sich mit dem Zusammenhang zwischen Untergruppen von $W_m(K)$ und abelschen Erweiterungen von K . Die wichtigsten Aussagen dazu fasst der folgende Satz zusammen.

Theorem 1.3.1. *Sei K ein Körper der Charakteristik p .*

1. *Sei $a = (a_0, \dots, a_{m-1}) \in W_m(K)$ und $\alpha = (\alpha_0, \dots, \alpha_{m-1}) \in W_m(K^{\text{sep}})$ ein Urbild von a unter \wp . Sei $L = K(\alpha_0, \dots, \alpha_{m-1})$ der Erweiterungskörper, der durch Adjunktion der Komponenten von α an K entsteht. Dann ist L/K eine zyklische Erweiterung vom Exponenten p^m .*
2. *Jede zyklische Erweiterung von K vom Exponenten p^m entsteht auf diese Weise.*
3. *Die Abbildung $U \mapsto K(\wp^{-1}(U))$ liefert eine Bijektion zwischen den Untergruppen U von $W_m(K)$, die $\wp(W_m(K))$ enthalten und den abelschen Erweiterungen von K vom Exponenten p^m . Hierbei entsteht $K(\wp^{-1}(U))$ durch Adjunktion der Koordinaten sämtlicher Urbilder der Elemente aus U .*

Beweis. Ein Beweis findet sich bei [Lor90] auf Seite 26. □

Ist L/K eine Galoiserweiterung mit Galoisgruppe G , so operiert G durch

$$\sigma(x_0, x_1, \dots, x_{m-1}) := (\sigma x_0, \sigma x_1, \dots, \sigma x_{m-1}), \sigma \in G$$

auf $W_m(L)$. Diese Operation versieht $W_m(L)$ mit einer G -Modulstruktur. Dabei ist $W_m(K) \subseteq W_m(L)$ genau die Menge der G -invarianten Elemente. Der Homomorphismus \wp ist G -äquivariant. Für die absolute Galoisgruppe G_K von K ist daher die folgende Sequenz eine kurze exakte Sequenz von G_K -Modulen:

$$0 \rightarrow W_m(\mathbb{F}_p) \rightarrow W_m(K^{\text{sep}}) \xrightarrow{\wp} W_m(K^{\text{sep}}) \rightarrow 0$$

Wir nennen sie Artin-Schreier-Sequenz. Sie induziert eine lange exakte Sequenz in Kohomologie:

$$0 \rightarrow W_m(\mathbb{F}_p) \rightarrow W_m(K) \xrightarrow{\wp} W_m(K) \rightarrow H^1(G_K, W_m(\mathbb{F}_p)) \rightarrow H^1(G_K, W_m(K^{\text{sep}})). \quad (1.3.1)$$

Nach dem Satz Hilbert 90 wissen wir, dass $H^1(G_K, W_m(K^{\text{sep}})) = 0$ gilt (siehe [Lan02] oder [Haz09]). Somit gilt $W_m(K)/\wp W_m(K) \simeq H^1(G_K, W_m(\mathbb{F}_p))$. Dieser Isomorphismus lässt sich explizit angeben: Für $v \in W_m(K)$ gibt es ein $w \in W_m(K^{\text{sep}})$

mit $\wp(w) = v$. Nun bilden wir v auf die Abbildung $\xi : G_K \rightarrow W_m(\mathbb{F}_p), \sigma \mapsto \sigma(w) - w$ ab und erhalten den gewünschten Isomorphismus. Diese Konstruktion des Verbindungshomomorphismus ist wohlbekannt und der Beweis der Wohldefiniertheit lässt sich in jedem Buch über Galoiskohomologie nachlesen (siehe zum Beispiel [Ser97]). Die Surjektivität folgt aus $H^1(G_K, W_m(K^{\text{sep}})) = 0$.

Für eine gewöhnliche elliptische Kurve A ist die Verschiebung V^m für alle natürlichen Zahlen m eine separable Isogenie mit zyklischem Kern der Ordnung p^m . Daher besteht für jeden Punkt $P \in A(K^{\text{sep}})$ das Urbild unter V^m aus p^m verschiedenen Punkten in $A^{(p^m)}(K^{\text{sep}})$. Die folgende Sequenz abelscher Gruppen ist somit exakt

$$0 \rightarrow A^{(p^m)}(K^{\text{sep}})[V^m] \rightarrow A^{(p^m)}(K^{\text{sep}}) \xrightarrow{V^m} A(K^{\text{sep}}) \rightarrow 0.$$

Sei nun G_K die absolute Galoisgruppe von K . Durch Anwenden der Automorphismen auf die Koordinaten der Punkte operiert G_K auf den Gruppen obiger Sequenz. Da auch die auftretenden Homomorphismen mit der Gruppenoperation verträglich sind, haben wir eine kurze exakte Sequenz von G_K -Modulen. Solche induzieren lange exakte Sequenzen in Kohomologie:

$$0 \rightarrow A^{(p^m)}(K)[V^m] \rightarrow A^{(p^m)}(K) \rightarrow A(K) \xrightarrow{\alpha'_m} H^1(G_K, A^{(p^m)}(K^{\text{sep}})[V^m])$$

Die Punkte auf A und $A^{(p^m)}$, die invariant unter der Gruppenoperation bleiben, sind genau die K -rationale Punkte, also besitzt der Verbindungshomomorphismus den gewünschten Kern. Wie schon bei der Artin-Schreier-Sequenz beschrieben, ist dieser durch $P \mapsto (\sigma \mapsto \sigma(Q) - Q)$ für ein $Q \in A^{(p^m)}(K^{\text{sep}})$ mit $V^m(Q) = P$ gegeben. Die Kohomologiegruppe $H^1(G_K, A^{(p^m)}(K^{\text{sep}})[V^m])$ lässt sich sehr explizit beschreiben, wenn die V^m -Torsion rational ist, d.h. wenn $A^{(p^m)}(K^{\text{sep}})[V^m] = A^{(p^m)}(K)[V^m]$ gilt. In diesem Fall ist $A^{(p^m)}(K)[V^m]$ eine zyklische Gruppe der Ordnung p^m , auf der G_K trivial operiert. Fixieren wir Erzeuger, so bekommen wir Isomorphismen zwischen $A^{(p^m)}(K)[V^m]$, $\mathbb{Z}/p^m\mathbb{Z}$ und $W_m(\mathbb{F}_p)$. Dann sind aber auch $H^1(G_K, A^{(p^m)}(K^{\text{sep}})[V^m])$ und $H^1(G_K, W_m(\mathbb{F}_p))$ isomorph. Zusammen ergibt das einen Homomorphismus

$$\alpha_m : A(K) \rightarrow W_m(K)/\wp W_m(K)$$

mit $\ker \alpha_m = V^m(A^{(p^m)}(K))$. Dieser ist die gesuchte V^m -Abstiegs-Abbildung. Er bildet einen Punkt $P \in A(K)$ wie folgt ab: Sei $Q \in A^{(p^m)}(K^{\text{sep}})$ mit $V^m(Q) = P$ beliebig. Da ein $\sigma \in G_K$ auf Q durch Addition eines p^m -Torsionspunkts operiert und da diese nach Voraussetzungen K -rational sind, ist $K(Q)$, der Körper, der durch Adjunktion der Koordinaten von Q entsteht, eine zyklische Erweiterung von K vom Exponenten p^m . Solch eine Erweiterung korrespondiert zu einem Wittvektor $w \in W_m(K^{\text{sep}})$. Dabei ist die von w erzeugte Untergruppe U von $W_m(K^{\text{sep}})/\wp W_m(K^{\text{sep}})$ eindeutig. Sei nun $\phi : A^{(p^m)}(K)[V^m] \rightarrow W_m(\mathbb{F}_p)$ ein fester Isomorphismus und σ ein Erzeuger der Galoisgruppe von $K(Q)/K$. Wir bilden P auf $\wp(w_0) \in W_m(K)$ ab, wobei w_0 der Erzeuger von U ist, der $\sigma(w_0) - w_0 = \phi(\sigma(Q) - Q)$ erfüllt. Für konkrete n und p lässt sich diese Abbildung durch einen expliziten polynomiellen Ausdruck in den Koordinaten des Punktes P beschreiben.

Bemerkung 1.3.2. *In diesem Abschnitt wird in den Aussagen und Rechnungen Galoiskohomologie verwendet. Alles funktioniert aber analog, wenn wir stattdessen die im Anhang beschriebene spezialisierte Version flacher Kohomologie verwenden. Da Rechnungen in Galoiskohomologie im Allgemeinen einfacher sind, haben wir uns hier für Erstherr entscheiden.*

1.3.2.2 Der Fall $m = 1$

In [Vol90] und [Kra77] geben Voloch und Kramer Konstruktionen für Homomorphismen $\alpha_1 : A(K) \rightarrow K/\wp(K)$ mit $\ker \alpha_1 = V(A^{(p)}(K))$ an. Dabei gilt $\wp(z) = z^p - z$ und wir identifizieren $W_1(K)$ mit K . Wir interessieren uns besonders für den Fall $p = 2$. Daher nehmen wir für den Rest des Abschnittes an, dass die Charakteristik von K gleich zwei ist. Dieser Fall wird von Kramer detailliert betrachtet. Er arbeitet mit der oben beschriebenen Weierstraß-Gleichung $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ und gibt für α_1 die durch

$$(x, y) \mapsto \frac{x + a_2}{a_1^2} \equiv \frac{a_6}{a_1^2 x^2}$$

beschriebene Abbildung an. Kramer zeigt durch konkrete Rechnungen, dass diese ein Homomorphismus mit dem gewünschten Kern ist. Für elliptische Kurven mit der oben beschriebenen Weierstraß-Gleichung, ist die Verschiebung durch

$$V : A^{(2)} \rightarrow A, (x, y) \mapsto \left(\frac{x^2 + a_1^2 a_6}{a_1^2 x}, \frac{y + a_2 x + a_6}{a_1^3} + \frac{a_6(y + a_2 x + a_6)}{a_1 x^2} + \frac{a_1 a_6}{x} \right)$$

gegeben. Sei nun $P = (x, y) \in A(K)$ und $K(Q)$ die zyklische Erweiterung, die durch die Adjunktion der Koordinaten eines Urbilds von P unter V entsteht. Einfache Rechnungen zeigen, dass $K(Q)$ isomorph zu $K(x(Q))$ ist, d.h. dass wir die ganze Erweiterung schon durch Adjunktion der x -Koordinate bekommen. Daraus folgt unmittelbar, dass die Erweiterung $K(Q)$ isomorph zu der durch das Polynom $t^2 + t + (x + a_2)/a_1^2$ erzeugten Artin-Schreier-Erweiterung ist, und die im vorherigen Abschnitt beschriebene Gleichheit gilt.

1.3.2.3 Der Fall $m = 2$

Die Konstruktion, die Voloch in [Vol90] verwendet, um für $p \geq 3$ einen Homomorphismus $\alpha_1 : A(K) \rightarrow K/\wp(K)$ mit $\ker \alpha_1 = V(A^{(p)}(K))$ zu bestimmen, können wir iterieren. Damit bekommen wir ein Verfahren, das für beliebige $m \in \mathbb{N}$ und gewöhnliche elliptische Kurven A mit $p \geq 3$ und K -rationaler p^m -Torsion auf $A^{(p^m)}$, eine explizite Beschreibung der Abbildung $\alpha_m : A(K) \rightarrow W_m(K)/\wp(W_m(K))$ mit $\ker \alpha_m = V(A^{(p^m)}(K))$ berechnet. Für tatsächliche Anwendungen scheint das aber weniger geeignet. Zum einen wird die Abbildung α_m mit wachsendem m und p schnell sehr kompliziert, zum anderen ist es eine starke Einschränkung zu verlangen, dass die p^m -Torsion K -rational ist. Aber der Fall $p = 2$ und $m = 2$ lässt sich noch in der Praxis gewinnbringend verwenden. Wir untersuchen ihn im Folgenden genauer. Sei also die Charakteristik von K gleich zwei und A durch $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ gegeben.

Lemma 1.3.3. *Die Kurve $A^{(4)}$ gegeben durch $y^2 + a_1^4 xy + x^3 + a_2^4 x^2 + a_6^4 = 0$ besitzt genau dann K -rationale 4-Torsion, wenn $a_2 = a_1^2(s^2 + s)$ für ein $s \in K$ gilt. Dann sind $(a_1^2 a_6, a_1^5 s^4 a_6 + a_6^2)$ und $(a_1^2 a_6, a_1^6 s^4 a_6 + a_6^2 + a_1^6 a_6)$ die Punkte der Ordnung 4.*

Beweis. Wir wissen, dass $T = (0, a_6^2)$ der nichttriviale 2-Torsionspunkt auf $A^{(4)}$ ist. Daher gilt es nun zu untersuchen, wann es einen Punkt $S \in A^{(4)}(K)$ gibt, der $[2]S = T$ erfüllt. Wir bekommen für die x -Koordinate von S die Gleichung $x^4 + a_1^8 a_6^4 = 0$. Diese besitzt immer die eindeutige Lösung $x = a_1^2 a_6$. Nun ist zu untersuchen, wann das die

x -Koordinate eines Punktes auf $A^{(4)}(K)$ ist. Die Gleichung

$$y^2 + a_1^6 a_6 y + a_1^6 a_6^3 + a_2^4 a_1^4 a_6^2 + a_6^4 = 0$$

besitzt eine Lösung $y \in K$ genau dann, wenn

$$\begin{aligned} y_1^2 + y_1 &= \frac{a_1^6 a_6^3 + a_2^4 a_1^4 a_6^2 + a_6^4}{a_1^{12} a_6^2} \\ &= \frac{a_6}{a_1} + \frac{a_6^2}{a_1^{12}} + \frac{a_2^4}{a_1^8} \end{aligned}$$

eine Lösung $y_1 \in K$ besitzt und die Relation ist gegeben durch $y_1 = \frac{y}{a_1^6 a_6}$. Letztere Gleichung ist wiederum genau dann über K lösbar, wenn

$$y_2^2 + y_2 = \frac{a_2^4}{a_1^8}$$

es ist und zwischen den Lösungen besteht die Relation $y_2 = y_1 + \frac{a_6}{a_1}$. Die Transformation $y_3 = y_2 + \frac{a_2^2}{a_1^4} + \frac{a_2}{a_1}$ liefert dann die Gleichung

$$y_3^2 + y_3 = \frac{a_2}{a_1^2}$$

und diese ist genau dann über K lösbar, wenn $a_2 = a_1^2(s^2 + s)$ gilt. Das liefert uns die gesuchten Punkte der Ordnung 4. \square

Lemma 1.3.4. *Sei A durch die Gleichung $y^2 + a_1 xy + x^3 + a_1^2(s^2 + s)x^2 + a_6 = 0$ über K definiert. Die Abbildung*

$$\begin{aligned} \alpha_2 : A(K) &\rightarrow W_2(K)/\wp(W_2(K)), \\ (x, y) &\mapsto \left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{sa_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right) \end{aligned}$$

ist der zuvor beschriebene Homomorphismus mit Kern $\ker \alpha_2 = V^2(A^{(4)}(K))$.

Beweis. Wir zeigen, dass für alle $P = (x_0, y_0) \in A(K)$ mit einem Urbild $Q = (x_1, y_1)$ unter V^2 und σ ein Erzeuger der Galoisgruppe von $K(Q)/K$ die Gleichheit

$$\Psi(Q - \sigma(Q)) = w - \sigma w$$

gilt. Hierbei ist w ein Urbild von $\alpha_2(P)$ unter \wp und Ψ ein fester Automorphismus von $\ker V^2$ nach $W_2(\mathbb{F}_2)$ gegeben durch die Wahl eines Erzeugers von $\ker V^2$, der auf einen Erzeuger von $W_2(\mathbb{F}_2)$ abgebildet wird. Diese Gleichheit lässt sich durch explizite Rechnungen – siehe Abschnitt 6.3.1 im Anhang – verifizieren. Der Verbindungshomomorphismus $A(K) \rightarrow H^1(G_K, \ker V^2)$ ist dadurch bestimmt, dass ein Punkt P auf den Kozykel $\sigma \mapsto Q - \sigma(Q)$ abgebildet wird. Der Isomorphismus aus der Artin-Schreier-Sequenz $W_2(K)/\wp(W_2(K)) \rightarrow H^1(G_K, W_2(\mathbb{F}_2))$ ist analog durch $v \mapsto (\sigma \mapsto w - \sigma(w))$ mit w ein Urbild von v unter \wp gegeben. Die Rechnung beweist, dass die Hintereinanderausführung des Verbindungshomomorphismus und des Isomorphismus die behauptete Form besitzt. \square

1.3.3 F^m -Abstieg

1.3.3.1 Allgemein

In diesem Abschnitt wollen wir eine Abbildung β_m mit den zuvor beschriebenen Eigenschaften konstruieren. Wie auch beim V^m -Abstieg, liefert uns die Kohomologietheorie wichtige Werkzeuge. Für den F^m -Abstieg genügt Galoiskohomologie nicht mehr. Wir müssen eine allgemeinere Theorie verwenden. Eine kurze Zusammenfassung der benötigten Aussagen sowie Verweise zu einer ausführlichen Behandlung der Themen finden sich im Anhang.

Sei K ein Körper der Charakteristik p , dann ist die folgende Sequenz von Garben abelscher Gruppen über K exakt. Für eine genauere Erklärung zu diesen Garben sei auf den Anhang über Gruppenschema verwiesen.

$$0 \rightarrow \mathbb{H}_{p^m} \rightarrow \mathbb{G}_m \xrightarrow{p^m} \mathbb{G}_m \rightarrow 0.$$

Wir bezeichnen sie als die Kummer-Sequenz. Sie induziert eine lange exakte Sequenz in Kohomologie.

$$0 \rightarrow \mathbb{H}_{p^m}(K) \rightarrow \mathbb{G}_m(K) \xrightarrow{p^m} \mathbb{G}_m(K) \xrightarrow{\delta_{K,m}} H^1(K, \mathbb{H}_{p^m}) \rightarrow H^1(K, \mathbb{G}_m)$$

Nach Satz Hilbert 90 – siehe zum Beispiel [Wat79] – wissen wir, dass $H^1(K, \mathbb{G}_m) = 0$ gilt. Somit gilt $\mathbb{G}_m(K)/\mathbb{G}_m(K)^{p^m} = K^\times/(K^\times)^{p^m} \simeq H^1(K, \mathbb{H}_{p^m})$ unter $\delta_{K,m}$.

Sei nun A eine gewöhnliche elliptische Kurve über K . Dann ist

$$0 \rightarrow A[F^m] \rightarrow A \xrightarrow{F^m} A^{(p^m)} \rightarrow 0$$

eine kurze exakte Sequenz von Garben abelscher Gruppen über K . Als solche induziert sie eine lange exakte Sequenz in Kohomologie:

$$0 \rightarrow H^0(K, A[F^m]) \rightarrow H^0(K, A) \xrightarrow{F^m} H^0(K, A^{(p^m)}) \xrightarrow{\delta_{F^m}} H^1(K, A[F^m])$$

Besitzt $A^{(p^m)}$ volle p^m -Torsion über K , dann sind $\ker V^m$ und $\mathbb{Z}/p^m\mathbb{Z}$ isomorph. Dieser Isomorphismus ist dadurch gegeben, dass ein fest gewählter Erzeuger P' von $\ker V^m(K)$ auf 1 abgebildet wird und wurde von uns bereits im vorherigen Abschnitt bei der Konstruktion einer V^m -Abstiegsabbildung verwendet. Wie im Anhang 6 über Gruppenschema beschrieben, sind $\ker F^m$ und $\ker V^m$ sowie \mathbb{H}_{p^m} und $\mathbb{Z}/p^m\mathbb{Z}$ jeweils dual unter der Cartier-Dualität. Für eine endliche K -Algebra R sind die Dualitäts-paarungen gegeben durch

$$\ker F^m(R) \times \ker V^m(R) \rightarrow R^\times, (P, P') \mapsto e(P, P')$$

mit e die Weil-Paarung – siehe Bemerkung 6.1.6 im Anhang – und

$$\mathbb{H}_{p^m}(R) \times \mathbb{Z}/p^m\mathbb{Z}(R) \rightarrow R^\times, (\zeta, i) \mapsto \zeta^i.$$

Es sind also auch $A[F^m]$ und \mathbb{H}_{p^m} als K -Gruppenschemata isomorph. Mit der Bezeichnung Ξ für den oben beschriebenen Isomorphismus

$$\ker V^m(R) \rightarrow \mathbb{Z}/p^m\mathbb{Z}, P' \mapsto 1$$

bekommen wir

$$\ker F^m(R) \rightarrow (\ker V^m)^D(R) \rightarrow (\mathbb{Z}/p^m\mathbb{Z})^D(R) \rightarrow \mathbb{H}_{p^m}(R)$$

$$P \mapsto e(P, \cdot) \mapsto e(P, \Xi(\cdot)) \mapsto e(P, \Xi(P'))$$

einen Isomorphismus $e_{P'} : \ker F^m \rightarrow \mathbb{H}_{p^m}$, für den das Diagramm

$$\begin{array}{ccc} \ker F^m \times \ker V^m & \longrightarrow & \mathbb{G}_m \\ e_{P'} \downarrow & & \downarrow \text{id} \\ \mathbb{H}_{p^m} \times \mathbb{Z}/p^m\mathbb{Z} & \longrightarrow & \mathbb{G}_m \end{array}$$

kommutiert. Die Zeilen sind dabei durch die Paarungen der Cartier-Dualität gegeben. Die Komposition der von $e_{P'}$ auf den 1-Kozykeln induzierten Abbildung und δ_{F^m} liefert somit den Homomorphismus mit den gewünschten Eigenschaften

$$\beta_m : A^{(p^m)}(K) \rightarrow K^\times / (K^\times)^{p^m}.$$

Sein Kern ist $\ker \beta_m = F^m(A(K))$. Wir konstruieren β_m explizit. Die Idee dafür findet sich schon bei [Vol90] und auch bei [Sil86, X.1]. Sei P' ein Punkt der Ordnung p^m in $A^{(p^m)}$, also ein Erzeuger von $\ker V^m$. Nach den Voraussetzungen ist P' über K definiert. Dann gibt es nach dem Satz von Riemann-Roch eine rationale Funktion f mit Divisor $p^m P' - p^m O'$ wobei O' der unendliche Punkt von $A^{(p^m)}$ ist. Wir können f berechnen und so skalieren, dass $f \circ F^m = g^{p^m}$ für ein $g \in K(A)$ gilt. Nun definieren wir eine Abbildung

$$\hat{\beta}_m : A^{(p^m)}(K) \rightarrow K^\times / (K^\times)^{p^m}, P \mapsto \begin{cases} 1, & \text{für } P = O' \\ f(-P')^{-1}, & \text{für } P = P' \\ f(P), & \text{sonst} \end{cases}$$

Es bezeichne δ_{F^m} den Verbindungshomomorphismus $A^{(p^m)}(K) \rightarrow H^1(K, A[F^m])$. Verwenden wir Čech-Kohomologie, so ist δ_{F^m} durch

$$P \mapsto (1 \otimes x_Q, 1 \otimes y_Q) - (x_Q \otimes 1, y_Q \otimes 1)$$

gegeben, wobei $Q = (x_Q, y_Q) \in A(\bar{K})$ ein Punkt mit $F^m(Q) = P$ ist und sich das Minus auf das Gruppengesetz bezieht. Analog bezeichne $\delta_{K,m}$ den Verbindungshomomorphismus der Kummer-Sequenz, gegeben durch

$$\delta_K : K^\times \rightarrow H^1(K, \mathbb{H}_{p^m}), a \mapsto (1 \otimes b) / (b \otimes 1),$$

wobei $b^{p^m} = a$ gelte.

Lemma 1.3.5. *Sei $P' \in \ker V^m(K)$ ein K -rationaler Punkt der Ordnung p^m und sei $\hat{\beta}_m$ die oben beschriebene Abbildung mit $(f) = (p^m P' - p^m O')$. Bezeichne e die Weil-Paarung, so wie sie z.B. in [KM85] definiert ist. Dann gilt für alle $P \in A^{(p^m)}(K)$ die Beziehung $\delta_{K,m}(\hat{\beta}_m(P)) = e(\delta_{F^m}(P), P')$.*

Beweis. In [Sil86, X.1.1] gibt Silverman einen Beweis dieser Aussage für den zur Charakteristik teilerfremden Fall unter Benutzung von Galoiskohomologie an. Dieser lässt sich auf unseren Fall und Čech-Kohomologie übertragen. Sei $Q = (x_Q, y_Q)$ ein Punkt in $A(\bar{K})$ mit $F^m(Q) = P$ und sei $\hat{\beta}_m(P) = g^{p^m}(Q) = \gamma^{p^m}$, das heißt $\gamma \in \bar{K}$

mit $\gamma^{p^m} \in K$. Nun haben wir

$$\begin{aligned} e(\delta_F(P), P') &= e((1 \otimes x_Q, 1 \otimes y_Q) - (x_Q \otimes 1, y_Q \otimes 1), P') \\ &= \frac{g((1 \otimes x_Q, 1 \otimes y_Q))}{g((x_Q \otimes 1, y_Q \otimes 1))} \\ &= \frac{1 \otimes g((x_Q, y_Q))}{g((x_Q, y_Q)) \otimes 1}. \end{aligned}$$

Da $g^{p^m} = f \circ F^m$ gilt, haben wir

$$g((x_Q, y_Q))^{p^m} = f(x_P, y_P) = \gamma^{p^m}$$

also

$$g((x_Q, y_Q)) = \gamma.$$

Auf der anderen Seite gilt

$$\delta_K(\hat{\beta}_m(P)) = \delta_K(\gamma^{p^m}) = \frac{1 \otimes \gamma}{\gamma \otimes 1}.$$

□

Als Ergebnis sehen wir, dass sich die abstrakte Abbildung der Kohomologiegruppen β_m durch die explizite Formel von $\hat{\beta}_m$ auswerten lässt.

Bemerkung 1.3.6. *Voloch gibt in [Vol90] einen anderen Beweis dafür, dass $\hat{\beta}_1$ die gewünschte Abbildung ist. Auch dieser Beweis lässt sich ohne große Schwierigkeiten für unsere Situation und $m \geq 2$ anpassen. Da die Technik weniger allgemein ist, verzichten wir an dieser Stelle darauf.*

1.3.3.2 Der Fall $m = 1$

Gegeben sei eine gewöhnliche elliptische Kurve A und ein Punkt P der Ordnung p auf $A^{(p)}(K)$, dann lässt sich eine Funktion f mit Divisor $(f) = (pP' - p\mathcal{O}')$ zum Beispiel mit Magma berechnen. Voloch gibt für $p \geq 3$ eine auf Gunji zurückgehende allgemeine Konstruktion an und Kramer zeigt, dass für $A : y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ die Abbildung

$$\beta_1 : A^{(2)}(K) \rightarrow K^\times / (K^\times)^2, (x, y) \mapsto \begin{cases} x, & \text{für } x \neq 0 \\ a_6, & \text{für } x = 0 \\ 1, & \text{für } (x, y) = \mathcal{O}' \end{cases}$$

die gewünschte ist.

1.3.3.3 Der Fall $m = 2$

Wir haben gezeigt, dass für einen Körper K der Charakteristik 2 und eine durch $A : y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ definierte elliptische Kurve die Kurve $A^{(4)}$ genau dann K -rationale 4-Torsion besitzt, wenn $a_2 = a_1^2(s^2 + s)$ für $s \in K$ gilt. Als Resultat unserer vorherigen Überlegungen bekommen wir das folgende Lemma.

Lemma 1.3.7. *Die Abbildung*

$$\beta_2 : A^{(4)}(K) \rightarrow K^\times / (K^\times)^4, (x, y) \mapsto \begin{cases} a_1^2 a_6^3, & \text{für } (x, y) = T \\ 1, & \text{für } (x, y) = \mathcal{O}' \\ (y + 1/a_1^4 x^2 + a_1^4 s^4 x), & \text{sonst} \end{cases}$$

ist die gesuchte F^2 -Abstiegs-Abbildung. Hierbei ist $T = (a_1^2 a_6, a_1^6 s^4 a_6 + a_6^2)$ ein Punkt der Ordnung 4.

1.3.4 Supersinguläre Kurven

1.3.4.1 Allgemein

In den vorherigen Abschnitten haben wir angenommen, dass A eine gewöhnliche elliptische Kurve ist. Für supersinguläre elliptische Kurven A können wir ähnliche Resultate erzielen.

Lemma 1.3.8. *Für eine supersinguläre elliptische Kurve A sind $\ker F^m$ und $\ker V^m$ als endliche flache Gruppenschemata über K isomorph.*

Beweis. In diesem Fall ist die Verschiebung auch rein inseparabel, faktorisiert also durch den Frobenius. Da $\deg F^m = \deg V^m$ gilt, folgt die Behauptung. \square

1.3.4.2 Der Fall $m = 1$

Da $\ker F$ und $\ker V$ einerseits isomorph andererseits aber auch dual sind, sind sie aufgrund von Klassifikationsresultaten von Oort und Tate [OT70] – siehe auch Proposition 2.1 in [Ulm91] – isomorph zu \mathfrak{a}_p , dem Kern des Frobenius auf \mathbb{G}_a . Analog zu den gewöhnlichen elliptischen Kurven haben wir exakte Sequenzen

$$0 \rightarrow A[F] \rightarrow A \xrightarrow{F} A^{(p)} \rightarrow 0$$

und

$$0 \rightarrow \mathfrak{a}_p \rightarrow \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \rightarrow 0$$

von Garben abelscher Gruppen (siehe 6.1 und 6.2). Nun betrachten wir die induzierten langen exakten Sequenzen in Kohomologie. Nach Hilbert 90 gilt $H^1(K, \mathfrak{a}_p) \simeq K/K^p$. Fixieren wir einen Isomorphismus $\ker F \rightarrow \mathfrak{a}_p$, dann bekommen wir einen Homomorphismus

$$\beta_1 : A^{(p)}(K) \rightarrow K/K^p$$

mit $\ker \beta_1 = F(A(K))$. Für V verläuft alles analog.

Ist die Charakteristik von K gleich 2, so können wir einen Isomorphismus zwischen $\ker F$ und \mathfrak{a}_2 explizit angeben. Dieser wird von einem Isomorphismus der korrespondierenden Hopfalgebren induziert. Siehe Anhang 6.1 für eine Definition und relevante Eigenschaften. Die Hopfalgebra von \mathfrak{a}_2 ist $K[x]/(x^2)$, die von $\ker F$ bekommen wir, indem wir die projektiven Koordinaten auf der Kurve zu $y = 1$ skalieren. Details finden sich im Anhang unter 6.3.2. Mit dem resultierenden Isomorphismus der Gruppenschemata können wir wie zuvor beschrieben eine Abstiegs-Abbildung konstruieren. Ausführlichere Informationen finden sich im Abschnitt 6.3.2 im Anhang. Als Resultat bekommen wir die folgende Aussage.

Lemma 1.3.9. *Die Abbildung*

$$\beta_1 : A^{(2)}(K) \rightarrow K/K^2, (x, y) \mapsto 1/a_3^2 x.$$

ist die gesuchte F -Abstiegs-Abbildung.

Zum Beweis des Lemmas können die erforderlichen Eigenschaften auch direkt nachgeprüft werden.

Für die Verschiebung gehen wir analog vor. Wieder starten wir mit einem Isomorphismus $\ker V \rightarrow \mathfrak{a}_2$ der Gruppenschemata und dem davon induzierten Isomorphismus $H^1(K, \ker V) \rightarrow H^1(K, \mathfrak{a}_2)$ der Kohomologiegruppen. Da wir wollen, dass die Abstiegs-Abbildungen mit der Weil-Paarung verträglich sind, müssen wir an dieser Stelle den richtigen Isomorphismus verwenden. Ziel ist also, dass das Diagramm

$$\begin{array}{ccc} \ker F \times \ker V & \longrightarrow & \mathbb{G}_m \\ \downarrow & & \downarrow \text{id} \\ \mathfrak{a}_2 \times \mathfrak{a}_2 & \longrightarrow & \mathbb{G}_m \end{array} \quad (1.3.2)$$

kommutiert. Dabei ist die obere Zeile durch die Weil-Paarung und die untere durch die Selbstdualität gegeben. Die Abbildung $\ker F \rightarrow \mathfrak{a}_2$ ist der in Lemma 6.3.1 fixierte Isomorphismus. Dieses Diagramm korrespondiert zu dem Diagramm der Hopfalgebren:

$$\begin{array}{ccc} K[\ker F] \otimes K[\ker V] & \longleftarrow & K[x, x^{-1}] \\ \uparrow & & \uparrow \text{id} \\ K[x]/(x^2) \otimes K[x]/(x^2) & \longleftarrow & K[x, x^{-1}] \end{array} \quad (1.3.3)$$

Die Abbildung $K[x, x^{-1}] \rightarrow K[x]/(x^2) \otimes K[x]/(x^2)$ ist durch $x \mapsto 1 \otimes 1 + x \otimes x$, vergleiche zum Beispiel [Sha63, Beweis Thm 2], und $K[x]/(x^2) \rightarrow K[\ker F]$ ist nach Lemma 6.3.1 durch $x \mapsto x$ gegeben. Wir wollen nun die obere Zeile genauer untersuchen.

Lemma 1.3.10. *Die Weil-Paarung $e : \ker F \times \ker V \rightarrow \mathbb{G}_m$ induziert die Abbildung $K[x, x^{-1}] \rightarrow K[\ker F] \otimes K[\ker V]$, $x \mapsto 1 \otimes 1 + a_3 x \otimes x$ der Hopfalgebren.*

Beweis. Für den Beweis dieser Aussage berechnen wir den Wert, den die Weil-Paarung für zwei beliebige Punkte $P \in \ker F$ und $P' \in \ker V$ annimmt, als Ausdruck in geeigneten Koordinaten der Punkte. Dieser Ausdruck liefert uns direkt den gesuchten Morphismus der Hopfalgebren. Da die Gruppe der K' -rationalen Punkte der Kerne des Frobenius und der Verschiebung für alle Körpererweiterungen K'/K trivial ist, genügt es nicht, diese zu betrachten. Wir müssen mit S -rationalen Punkten arbeiten, wobei S ein endliches, affines K -Schema ist. Der resultierende Beweis verläuft ähnlich dem in [Sil86, III.8] nur unter deutlich allgemeineren Voraussetzungen. Er findet sich im Anhang unter 6.3.3. \square

Korollar 1.3.11. *Für die Hopfalgebrenmorphisme $K[x]/(x^2) \rightarrow K[\ker V]$, $x \mapsto a_3 x$ und $K[x]/(x^2) \rightarrow K[\ker F]$, $x \mapsto x$ kommutiert Diagramm 1.3.3.*

Dieser Isomorphismus der Hopfalgebren liefert uns wiederum einen Isomorphismus $H^1(K, \ker V) \rightarrow H^1(K, \mathfrak{a}_2)$. Benutzen wir diesen in

$$A(K) \rightarrow H^1(K, \ker V) \rightarrow H^1(K, \mathfrak{a}_2) \rightarrow K/K^2,$$

so erhalten wir nach einer Rechnung, die analog zu der für $\ker F$ verläuft, das folgende Ergebnis.

Lemma 1.3.12. *Die Abbildung*

$$\alpha_1 : A(K) \rightarrow K/K^2, (x, y) \mapsto x$$

ist die gesuchte V -Abstiegs-Abbildung. Sie ist mit der zuvor beschriebenen Abbildung β_1 verträglich, in dem Sinne, dass Diagramm 1.3.2 kommutiert.

1.3.4.3 Der Fall $m = 2$

Da im supersingulären Fall die Verschiebung $V : A^{(p)} \rightarrow A$ rein inseparabel ist, lässt sie sich als Hintereinanderausführung von $F : A^{(p)} \rightarrow A^{(p^2)}$ und einem Isomorphismus $\Psi : A^{(p^2)} \rightarrow A$ schreiben. Der Kern von F^2 ist somit isomorph zum Kern von $F \circ V$, also zum Kern der Multiplikation mit p auf A . Nach [Oor66] sind die Gruppenschemata $\ker F^2$, $\ker V^2$ und $A[p]$ isomorph zu einem mit M_2 bezeichneten endlichen, flachen Gruppenschema. Diese Isomorphie kann möglicherweise bei der Konstruktion expliziter Abstiegs-Abbildungen verwendet werden. Vergleiche dazu auch die Beschreibung von $A[p]$ in [Ulm91].

1.4 Lokale Bilder

1.4.1 Allgemein

Sei $\psi : A \rightarrow B$ eine Isogenie der über dem globalen Körper K definierten elliptischen Kurven A und B . Wie schon in den vorherigen Abschnitten verwendet, liefert das eine exakte Sequenz von Garben abelscher Gruppen über K . Siehe dazu auch unser Erklärungen im Anhang.

$$0 \rightarrow \ker \psi \rightarrow A \rightarrow B \rightarrow 0$$

Diese induziert eine lange exakte Kohomologiesequenz und die ψ -Abstiegs-Abbildung entspricht dem Verbindungshomomorphismus $B(K)/\psi(A(K)) \rightarrow H^1(K, \ker \psi)$ verknüpft mit einem Monomorphismus, der eine explizite Darstellung der ersten Kohomologiegruppe von $\ker \psi$ liefert. Im Folgenden sei v eine Stelle von K und K_v die dazugehörige Vervollständigung.

Definition 1.4.1. *Wir definieren die lokale Selmergruppe $\text{Sel}(K_v, \psi)$ von ψ als das Bild des Verbindungshomomorphismus*

$$B(K_v)/\psi(A(K_v)) \rightarrow H^1(K_v, \ker \psi).$$

Die globale Selmergruppe definieren wir als die Menge der Elemente in $H^1(K, \ker \psi)$, deren Restriktion auf $H^1(K_v, \ker \psi)$ für alle Stellen v in $\text{Sel}(K_v, \psi)$ liegt. Gelgentlich betten wir $H^1(K, \ker \psi)$ oder $H^1(K_v, \ker \psi)$ mit Hilfe eines Monomorphismus in eine andere Gruppe ein. Das Bild der Selmergruppe bezeichnen wir dann ebenfalls als Selmergruppe. Die Shafarevich-Tate-Gruppe $\text{III}(K, A)$ ist der Kern der Abbildung $H^1(K, A) \rightarrow \prod_v H^1(K_v, A)$ und mit $\text{III}(K, A)[\psi]$ bezeichnen wir wiederum den Kern der von ψ induzierten Abbildung $\text{III}(K, A) \rightarrow \text{III}(K, B)$.

Die globale Selmergruppe $\text{Sel}(K, \psi)$ ist endlich und die folgende Sequenz ist exakt:

$$0 \rightarrow B(K)/\psi(A(K)) \rightarrow \text{Sel}(K, \psi) \rightarrow \text{III}(K, A)[\psi] \rightarrow 0.$$

Die Endlichkeit der globalen Selmergruppe gilt für beliebige ψ , doch das zu beweisen ist schwierig. Wir sind aber an ihr nur für bestimmte Isogenien ψ interessiert und für

diese beweisen wir die Aussage jeweils und geben sogar Aussagen über ihre Kardinalität an. Im Allgemeinen ist es einfacher, die globale Selmergruppe zu berechnen, als das Bild der Abstiegs-Abbildung zu bestimmen. Im Folgenden werden wir uns mit der Berechnung der lokalen Selmergruppen beschäftigen. Dabei werden wir von der Cup-Produkt-Paarung

$$\cup : H^1(K_v, \ker \psi) \times H^1(K_v, \ker \psi^\vee) \rightarrow H^2(K_v, \mathbb{G}_m) \quad (1.4.1)$$

Gebrauch machen. Details dazu finden sich bei [Sha86] und [Sha63].

Theorem 1.4.2. *Bezeichnen α und β die ψ^\vee - bzw. ψ -Abstiegs-Abbildung. Die Gruppen $\alpha(A(K_v)) = \text{Sel}(K_v, \psi^\vee)$ und $\beta(B(K_v)) = \text{Sel}(K_v, \psi)$ sind orthogonale Komplemente unter der Cup-Produkt-Paarung.*

Beweis. Das Diagramm

$$\begin{array}{ccc} H^0(K_v, A^\vee) \times H^1(K_v, A) & \longrightarrow & H^2(K_v, \mathbb{G}_m) \\ \alpha \downarrow & & \uparrow \iota \\ H^1(K_v, \ker \psi^\vee) \times H^1(K_v, \ker \psi) & & \end{array}$$

kommutiert. Hierbei ist die untere Paarung durch das Cup-Produkt 1.4.1 und die obere durch [Mil06, Thm. 7.8] gegeben. Die vertikalen Abbildungen sind die passenden Homomorphismen der langen exakten Kohomologiesequenzen von

$$0 \rightarrow \ker \psi \rightarrow A \rightarrow B \rightarrow 0$$

und der dualen Sequenz [Mil08, Thm 9.1]. Die Kommutativität folgt aus der Konstruktion der oberen Paarung, vergleiche [Mil06, C.5] oder [Sha67]. Seien nun mit $b \in \text{Sel}(K_v, \psi) \subseteq H^1(K_v, \ker \psi)$ und $a \in \text{Sel}(K_v, \psi^\vee) \subseteq H^1(K_v, \ker \psi^\vee)$ Elemente der jeweiligen Selmergruppe bezeichnet, d.h. es gibt $P \in H^0(K_v, B) = B(K_v)$ bzw. $Q \in H^0(K_v, A^\vee) \cong H^0(K_v, A) = A(K_v)$ mit $\alpha(Q) = a$ und $\beta(P) = b$. Bezeichnen $(\cdot, \cdot)_1$ und $(\cdot, \cdot)_2$ die obere bzw. untere Paarung des obigen Diagramms und $\iota : H^1(K_v, \ker \psi) \rightarrow H^1(K_v, A)$ die von der Inklusion induzierte Abbildung. Es gilt $(a, b)_2 = (Q, \iota(b))_1 = (Q, 0)_1 = 0$, wegen der Exaktheit der Kohomologiesequenz. Folglich sind die beiden Selmergruppen orthogonal. Sei nun $b' \in H^1(K_v, \ker \psi)$ mit $(a, b')_2 = 0$ für alle $a \in \text{Sel}(K_v, \psi^\vee)$, d.h. $(Q, \iota(b'))_1 = 0$ für alle $Q \in H^0(K_v, A^\vee)$. Da $(\cdot, \cdot)_1$ eine exakte Dualität der beiden Gruppen liefert, gilt $\iota(b') = 0$ und somit $b' \in \text{Sel}(K_v, \psi)$. □

Wie wollen diese Aussage für $\psi = V^m$ und $\psi^\vee = F^m$ anwenden. Wie schon bei der Konstruktion der Abstiegs-Abbildungen unterscheiden wir zwischen gewöhnlichen und supersingulären elliptischen Kurven.

1.4.2 n teilerfremd zur Charakteristik

Sei also A eine elliptische Kurve in kurzer Weierstraß-Form über dem lokalen Körper K_v . Brumer und Kramer beweisen in [BK77], dass wenn die Charakteristik p des Restklassenkörpers von K_v koprim zu 2 ist, die Gleichheit

$$\#A(K_v)/2A(K_v) = \#A(K_v)[2]$$

gilt. Dazu wird eine Untergruppe M von endlichem Index von $A(K_v)$ konstruiert, auf der sich Kern und Bild der Multiplikation mit 2 gut beschreiben lassen. Dann folgt das Resultat aus der Euler-Charakteristik der exakten Kern-Kokern-Sequenz der Multiplikation mit 2 von

$$0 \rightarrow M \rightarrow A(K_v) \rightarrow A(K_v)/M \rightarrow 0.$$

Als M kann dabei zum Beispiel der Kern der Reduktion $A_1(K_v)$ gewählt werden. Dann können wir ausnutzen, dass diese nach [Sil86, VII.2.2] isomorph zu einer formalen Gruppe ist. Wir sehen $\#A_1(K_v)[2] = \#A_1(K_v)/2A_1(K_v) = 1$, da die Multiplikation mit 2 auf $A_1(K_v)$ ein Isomorphismus ist. Die Formel und die Argumentation bleiben richtig, wenn wir 2 durch ein beliebiges aber zur Charakteristik p des Restklassenkörpers von K_v teilerfremdes n ersetzen. Dieses Ergebnis lässt sich leicht auf andere Isogenien verallgemeinern. Da wir bei dem V^m - und F^m -Abstieg etwas anders vorgehen, verzichten wir an dieser Stelle darauf.

Wir können die Kardinalität von $A(K_v)[n]$ durch Faktorisieren des n -Divisionspolynoms ermitteln. Kennen wir die Kardinalität von $A(K_v)/nA(K_v)$ und haben wir eine explizite Formel für die Abstiegs-Abbildung, so lässt sich das lokale Bild mit einem randomisierten Algorithmus wie in [Wom03, 1.7] beschrieben, berechnen.

1.4.3 Gewöhnliche elliptische Kurven

Für den gesamten Abschnitt sei A eine gewöhnliche elliptische Kurve über dem lokalen Körper K_v der Charakteristik p . Wir sind dabei hauptsächlich an dem Fall $p = 2$ interessiert. In diesem Fall gehen wir immer von einer Weierstraß-Gleichung der Form $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ mit ganzen Koeffizienten aus. Weiterhin verlangen wir, dass die volle V^m -Torsion von $A^{(p^m)}$ bereits über K_v definiert ist. Dann bilden die lokalen V^m - und F^m -Abstiegsabbildungen in die Gruppen $W_m(K_v)/\wp W_m(K_v)$ und $K_v^\times/(K_v^\times)^{p^m}$ ab. Viele Aussagen und Argumente haben ihren Ursprung in [Ulm91] und [Kra77].

Das folgende Lemma zeigt, dass wir uns auf Kurven, deren Weierstraß-Gleichungen ganze Koeffizienten haben, beschränken können.

Lemma 1.4.3. *Sei $u \in K_v$ und A' durch $y^2 + ua_1xy + x^3 + u^2a_2x^2 + u^6a_6 = 0$ gegeben.*

1. *Die Abbildung $(x, y) \mapsto (u^2x, u^3y)$ liefert einen über K_v definierten Isomorphismus $A \rightarrow A'$.*
2. *Die Bilder der V - und V^2 -Abstiegs-Abbildungen α_1 und α_2 sind auf $A(K_v)$ und $A'(K_v)$ gleich.*
3. *Die Bilder der F - und F^2 -Abstiegs-Abbildungen β_1 und β_2 sind auf $A^{(2^i)}(K_v)$ und $(A')^{(2^i)}(K_v)$ für $i = 1, 2$ gleich.*

Beweis. 1. Das ist bekannt. Siehe z.B. [Sil86, A.1.1].

2. Wir geben hier die Rechnung für α_2 an. Die Rechnung für α_1 verläuft analog. Sei $(x_0, y_0) \in A(K_v)$ und (u^2x_0, u^3y_0) der korrespondierende Punkt auf $A'(K_v)$.

Wir bezeichnen mit α'_2 die V^2 -Abstiegs-Abbildung auf $A'(K_v)$. Dann gilt

$$\begin{aligned} \alpha_2((x_0, y_0)) &= \left(\frac{a_6}{a_1^2 x_0^2}, \frac{a_6 y_0}{a_1^3 x_0^3} + \frac{a_6}{a_1^4 x_0} + \frac{sa_6 + a_6}{a_1^2 x_0^2} + \frac{a_6^2}{a_1^4 x_0^4} \right) \\ &= \left(\frac{u^6 a_6}{u^2 a_1^2 u^4 x_0^2}, \frac{u^6 a_6 u^3 y_0}{u^3 a_1^3 u^6 x_0^3} + \frac{u^6 a_6}{u^4 a_1^4 u^2 x_0} + \frac{su^6 a_6 + u^6 a_6}{u^2 a_1^2 u^4 x_0^2} + \frac{u^{12} a_6^2}{u^4 a_1^4 u^8 x_0^4} \right) \\ &= \alpha'_2((u^2 x_0, u^3 y_0)). \end{aligned}$$

3. Das folgt aus der Orthogonalität 1.4.2. \square

Die im vorherigen Abschnitt beschriebene Cup-Produkt-Paarung entspricht für gewöhnliche elliptische Kurven einer aus der lokalen Klassenkörpertheorie bekannten Paarung, vergleiche [Sha72], [Ser79].

Theorem 1.4.4. *Sei K_v die Vervollständigung von K an einer Stelle v , dann entspricht die Cup-Produkt-Paarung*

$$\cup : H^1(K_v, \ker V^m) \times H^1(K_v, \ker F^m) \rightarrow H^2(K_v, \mathbb{G}_m)$$

genau der Artin-Schreier-Witt-Paarung

$$[\cdot, \cdot] : W_m(K_v) / \wp W_m(K_v) \times K_v^\times / (K_v^\times)^{p^m} \rightarrow \mathbb{Q}/\mathbb{Z}.$$

unter der zuvor beschriebenen Identifikation von $H^1(K_v, \ker V^m)$ und $H^1(K_v, \ker F^m)$ mit $W_m(K_v) / \wp W_m(K_v)$ und $K_v^\times / (K_v^\times)^{p^m}$. Das Bild der unteren Paarung liegt dabei in $1/p^m \mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ und kann daher mit $\mathbb{Z}/p^m \mathbb{Z}$ identifiziert werden.

Beweis. Die benötigten Aussagen finden sich bei [Sha86, III.4 Bsp. (8)] und [Sha63, Beweis Thm. 4] oder [Mil06, Bemerkung III.7.5] \square

Bemerkung 1.4.5. *Diese Paarung ist eine Verallgemeinerung der bekannten Artin-Schreier-Paarung siehe ([Ser79] und [FV93]). Als Hauptquelle für Aussagen über die Artin-Schreier-Witt-Paarung dient der Artikel [Tho05]. Dort ist neben wichtigen Eigenschaften beschrieben, wie sie sich für gegebene Elemente explizit auswerten lässt.*

Das folgende Lemma gibt Auskunft über die F^2 -Selmergruppe. Die analoge Aussage über die F -Selmergruppe findet sich in [Kra77, Prop. 2.2].

Lemma 1.4.6. *Sei A eine elliptische Kurve über K_v mit einer Weierstraß-Gleichung der Form $y^2 + a_1 xy + x^3 + a_1^2(s^2 + s)x^2 + a_6 = 0$. Sei die Charakteristik von K_v gleich 2, seien $A_1(K_v)$ und $A_1^{(4)}(K_v)$ die Kerne der Reduktion auf $A(K_v)$ bzw. $A^{(4)}(K_v)$ und bezeichne mit U_n die Menge $U_n = \{u \in R_v^\times \mid v(u-1) \geq n\}$. Das Diagramm*

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_1(K_v) & \xrightarrow{F^2} & A_1^{(4)}(K_v) & \xrightarrow{\beta_2} & U_{4v(a_1)}(K_v^\times)^4 / (K_v^\times)^4 & \longrightarrow & 0, \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(K_v) & \xrightarrow{F^2} & A^{(4)}(K_v) & \xrightarrow{\beta_2} & \text{Im } \beta_2 & \longrightarrow & 0 \end{array}$$

dessen Zeilen exakt sind, kommutiert.

Beweis. Der Beweis funktioniert wie in [Kra77]. Es gilt

$$\begin{aligned} \left(y + \frac{x^2}{a_1^4} + a_1^4 s^4 x \right) \frac{a_1^4 x^4}{y^4} &= \frac{x^3 a_1^4 xy + x^3 + a_1^8 s^4 x^2}{y^2} \\ &= \frac{y^2 + a_1^4 xy + a_1^8 (s^8 + s^4) x^2 + a_6^4}{y^2} \frac{y^2 + a_1^8 s^8 x^2 + a_6^4}{y^2} \\ &= 1 + a_1^4 u^{-4} \left(z + a_1^4 s^4 z^2 + a_1^8 s^8 z^3 + a_6^4 \frac{z}{y^2} + a_1^4 a_6^4 s^4 \frac{z^2}{y^2} \right) \end{aligned}$$

mit $z := (x/y)$ und einer Einheit u des Bewertungsrings. Da (x, y) aus $A_1^{(4)}(K_v)$ ist, haben x und y beide eine negative Bewertung und es gilt sogar $2v(y) = 3v(x) = -6r$. Somit hat z die positive Bewertung r . Da die Bewertung aller Koeffizienten nicht negativ ist, liegt das Element in $U_{4v(a_1)}(K_v^\times)^4$. Da die Abbildung $(x, y) \mapsto x/y$ ein Isomorphismus zwischen $A_1^{(4)}(K_v)$ und dem Bewertungsideal ist, siehe ([Sil86, VII.2.2]), folgt die Surjektivität von

$$\beta_2 : A_1^{(4)}(K_v) \rightarrow U_{4v(a_1)}(K_v^\times)^4 / (K_v^\times)^4$$

unter Verwendung von Hensels Lemma, indem wir für ein beliebiges Element aus $U_{4v(a_1)}(K_v^\times)^4 / (K_v^\times)^4$ das geeignete z im Bewertungsideal konstruieren. \square

Korollar 1.4.7. *Es gelten die folgenden Gleichheiten:*

$$[\text{Im } \beta_1 : U_{2v(a_1)}(K_v^\times)^2 / (K_v^\times)^2] = [A^{(2)}(K_v) : A_1^{(2)}(K_v)] / [A(K_v) : A_1(K_v)]$$

$$[K_v^\times / (K_v^\times)^2 : \text{Im } \beta_1] = 2(\#k)^{v(a_1)} [A(K_v) : A_1(K_v)] / [A^{(2)}(K_v) : A_1^{(2)}(K_v)]$$

$$[\text{Im } \beta_2 : U_{4v(a_1)}(K_v^\times)^4 / (K_v^\times)^4] = [A^{(4)}(K_v) : A_1^{(4)}(K_v)] / [A(K_v) : A_1(K_v)]$$

$$[K_v^\times / (K_v^\times)^4 : \text{Im } \beta_2] = 4(\#k)^{v(a_1)} [A(K_v) : A_1(K_v)] / [A^{(4)}(K_v) : A_1^{(4)}(K_v)]$$

Wir erinnern, dass das Bild von β_i gleich der lokalen F^i -Selmergruppe ist. Die V^i -Selmergruppe ist also endlich, die F^i -Selmergruppe besitzt unendlich viele Elemente.

Beweis. Der erste Teil ist genau Proposition 2.2 in [Kra77] und der zweite Teil lässt sich analog durch Anwendung des Schlangenlemmas auf obiges Diagramm beweisen. Hierbei ist k der endliche Restklassenkörper von K_v . \square

Bemerkung 1.4.8. *Mit Hilfe von Tates Algorithmus können wir die Indizes*

$$[A(K_v) : A_1(K_v)] \text{ und } [A^{(2^i)}(K_v) : A_1^{(2^i)}(K_v)]$$

und damit die rechten Seiten der obigen Gleichheiten berechnen. Über die Orthogonalität aus Theorem 1.4.2, liefern die zweite und vierte Gleichung die (endliche) Kardinalität der lokalen V - und V^2 -Selmergruppe. Siehe dazu auch die Bemerkung nach Prop. 2.3 in [Kra77].

Damit bekommen wir häufig schon eine vollständige Beschreibung der lokalen Bilder.

Korollar 1.4.9. *Hat A gute Reduktion, also $v(\Delta(A)) = 0$, dann gilt*

$$\mathrm{Sel}(K_v, F^i) = U_0(K_v^\times)^{2^i} / (K_v^\times)^{2^i}$$

und

$$\mathrm{Sel}(K_v, V^i) = W_i(k) + \wp(W_i(K_v)) / \wp(W_i(K_v))$$

mit k wie zuvor und $i = 1, 2$.

Beweis. Für $i = 1$ ist das Prop. 2.4 in [Kra77]. Zum Beweis der ersten Gleichheit berechnen wir den Index von $U_0(K_v^\times)^{2^i} / (K_v^\times)^{2^i}$ in $\mathrm{Sel}(K_v, F^i)$ unter Verwendung von 1.4.7. Da A und damit auch $A^{(4)}$ gute Reduktion haben, gilt $A(K_v) = A_0(K_v)$. Der Index von $A_1(K_v)$ in $A_0(K_v)$ ist in diesem Fall gleich der Kardinalität der reduzierten Kurve. Da aber die reduzierten Kurven von A und von $A^{(2^i)}$ unter dem Frobenius isomorph sind, sind die Indizes gleich. Für den zweiten Teil der Aussage müssen wir das orthogonale Komplement von $U_0(K_v^\times)^{2^i} / (K_v^\times)^{2^i}$ unter der Artin-Schreier-Witt-Paarung bestimmen. Dabei folgt $W_i(R_v) + \wp(W_i(K_v)) \subseteq (U_0(K_v^\times)^{2^i} / (K_v^\times)^{2^i})^\perp$ aus dem folgenden Lemma 1.4.11. Die andere Inklusion folgt dann entweder aus Kardinalitätsgründen oder, indem wir die expliziten Formeln zur Berechnen der Paarung verwenden, um für $a \notin (W_i(R_v) + \wp(W_i(K_v))) / \wp(W_i(K_v))$ ein $b \in U_0(K_v^\times)^{2^i} / (K_v^\times)^{2^i}$ mit $[a, b] \neq 0$ zu konstruieren. Jedes Element aus $(W_i(R_v) + \wp(W_i(K_v))) / \wp(W_i(K_v))$ besitzt einen Repräsentanten in $W_i(k) + \wp(W_i(K_v))$. Das folgt direkt aus Abschnitt 2.3.1.1. \square

Bemerkung 1.4.10. *Diese folgende Aussage gilt für beliebige $i \in \mathbb{N}^{>0}$ und beliebige $p \in \mathbb{P}$, interessiert uns aber nur für $i = 1, 2$ und $p = 2$.*

Lemma 1.4.11. 1. *Sei $a = (a_0, \dots, a_{i-1})$ in $W_i(K_v)$. Dann besitzt a modulo $\wp(W_i(K_v))$ einen Repräsentanten $a' = (a'_0, \dots, a'_{i-1})$, bei dem für alle Indizes $0 \leq j \leq i$ gilt $a_j \in R_v$ oder $v(a_j)$ ist negativ und nicht durch die Charakteristik p von K_v teilbar. Wir nennen a' reduziert.*

2. *Seien m und u zwei ganze Zahlen, $u \geq 0$ und sei $a = (a_0, \dots, a_{i-1}) \in W_i(K_v)$ ein reduzierter Wittvektor mit $v(a_j) \geq -\left\lfloor \frac{m}{p^{i-j-1}} \right\rfloor$. Sei $b \in U_u K_v^{p^i} / K_v^{p^i}$. Dann gilt für $u > m$*

$$[a, b] = 0.$$

3. *Sei $a = (a_0, \dots, a_{i-1}) \in W_i(K_v)$ ein reduzierter Wittvektor und existiere ein Index $0 \leq j \leq i-1$ mit $v(a_j) < -\left\lfloor \frac{m}{p^{i-j-1}} \right\rfloor$. Dann gibt es ein $u \in U_m K_v^{p^i} / K_v^{p^i}$ mit*

$$[a, u] \neq 0.$$

Beweis. Diese Aussagen stammen direkt aus [Tho05]. Die erste ist Proposition 4.1, die zweite eine geringfügige Modifikationen von Proposition 4.3. Für den dritten Teil verwenden wir erneut Proposition 4.3. Nach den Voraussetzungen existiert ein j mit $-p^{i-j-1}v(a_j) = \max_k \{-p^{i-1-k}v(a_k)\} = m'$. Wähle $u := 1 + u_{m'}\pi^{m'} + O(\pi^{m'+1})$. Dann liegt $u \in U_{m'} \subseteq U_m$. Der Eintrag von $[a, u]$ an der j -ten Stelle ist gegeben durch $\mathrm{Tr}(-v(a_j)u_{m'}a_{j,v(a_j)}^{p^{i-1-j}})$. Dieser Wert ist ungleich 0 für eine geeignete Wahl von $u_{m'}$, da $v(a_j) \neq 0 \pmod p$ gilt. \square

Bemerkung 1.4.12. *Hat A keine gute Reduktion, so ist $U_{2iv(\alpha_1)}(K_v^\times)^{2^i}/(K_v^\times)^{2^i}$ mit Korollar 1.4.7 nur eine Untergruppe endlichen Index von $\text{Sel}(K_v, F^i)$. Über das orthogonale Komplement von $U_{2iv(\alpha_1)}(K_v^\times)^{2^i}/(K_v^\times)^{2^i}$ bekommen wir eine Obermenge der V^i -Selmergruppen. Das Lemma 1.4.11 liefert untere Schranken für die Bewertung der Komponenten eines reduzierten Wittvektors im orthogonalen Komplement von $U_{2iv(\alpha_1)}(K_v^\times)^{2^i}/(K_v^\times)^{2^i}$ und somit für das Bild von α_i . Bemerkung 1.4.8 liefert uns die Kardinalitäten von $\text{Sel}(K_v, V)$ und $\text{Sel}(K_v, V^2)$. Kennen wir ihre Kardinalitäten, so können wir auch Repräsentanten für die endlichen Gruppen $\text{Sel}(K_v, V)$ und $\text{Sel}(K_v, V^2)$ berechnen. Dazu können wir zum Beispiel solange zufällig Punkte auf $A(K_v)$ konstruieren und ihre Bilder unter α_i berechnen, bis wir das gesamte Bild bestimmt haben. Details dazu finden sich im Abschnitt 2.3.1.*

1.4.4 Supersinguläre elliptische Kurven

Für eine supersinguläre elliptische Kurve über einem lokalen Körper der Charakteristik 2 bilden die lokalen Abstiegs-Abbildungen in die additive Gruppe K_v/K_v^2 ab. Ein Repräsentantensystem für K_v/K_v^2 sind die Laurentreihen aus $K_v = k((\pi))$, die von null verschiedene Koeffizienten nur an den ungeraden π -Potenzen besitzen. Die Ableitung $d/d\pi$ nach der lokalen Uniformisierenden ist also injektiv auf K_v/K_v^2 und liefert einen Isomorphismus auf ihr Bild. Das können wir verwenden, um einige Aussagen über die lokalen Selmergruppen $\text{Sel}(K_v, F)$ und $\text{Sel}(K_v, V)$ zu beweisen. Wie auch bei den gewöhnlichen elliptischen Kurven, lässt sich die Cup-Produkt-Paarung effektiv auswerten.

Lemma 1.4.13. *Sei K_v ein lokaler Körper der Charakteristik 2. Dann entspricht die Cup-Produkt-Paarung*

$$\cup : H^1(K_v, \ker V) \times H^1(K_v, \ker F) \rightarrow H^2(K_v, \mathbb{G}_m)$$

der Paarung

$$K_v/K_v^2 \times K_v/K_v^2 \rightarrow \mathbb{Z}/2\mathbb{Z}, (f, g) \mapsto \text{Tr res}(f dg/d\pi).$$

Dazu fassen wir $\mathbb{Z}/2\mathbb{Z} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ als Untergruppe von \mathbb{Q}/\mathbb{Z} auf.

Beweis. Das ist die direkte Folgerung aus den in Abschnitt 1.3.4.2 konstruierten Isomorphismen zwischen $\ker F$ und \mathfrak{a}_2 sowie $\ker V$ und \mathfrak{a}_2 . Diese sind mit der Dualitätspaarung verträglich. Somit folgt die Aussage aus der Paarung für \mathfrak{a}_2 , siehe den Beweis von Theorem 2 in [Sha63]. \square

Bemerkung 1.4.14. *Die Paarung auf $K_v/K_v^2 \times K_v/K_v^2$ können wir mit begrenzter Präzision auswerten. Nach der Konstruktion in Abschnitt 1.3.4.2 sind $\text{Sel}(K_v, V)$ und $\text{Sel}(K_v, F)$ orthogonale Komplemente unter ihr.*

Lemma 1.4.15. *Sei A die durch $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ gegebene supersinguläre elliptische Kurve über K_v und $P = (x_P, y_P) \in A(K_v)$. Dann besitzt $x_P \bmod K_v^2$ einen Repräsentanten x'_P mit*

$$v(x'_P) \geq \min \left\{ 0, \frac{v(a_4)}{2}, \frac{v(a_6)}{3}, \frac{2v(a_3)}{3}, v(a_3) + 1, v(a_4) + 2, v(a_6) + 4 \right\}.$$

Da die V - und F -Abstiegs-Abbildung einen Punkt auf seine x -Koordinate bzw. das a_3^{-2} -fache seiner x -Koordinate abbildet, bekommen wir durch diese Ungleichung untere Schranken für die Bewertung der Elemente der lokalen Selmergruppen.

Beweis. Gilt $v(x_P) \geq \min\{0, \frac{v(a_4)}{2}, \frac{v(a_6)}{3}, \frac{2v(a_3)}{3}\}$ so ist nichts zu zeigen. Sei also $v(x_P)$ kleiner als das Minimum. Dann haben wir $v(x_P) = -2k$ und $v(y_P) = -3k$ für ein $k \in \mathbb{N}^{>0}$. Bezeichnen wir mit db abkürzend die Ableitung $db/d\pi$ eines $b \in K_v$ nach einer lokalen Uniformisierenden π , so erhalten wir

$$(da_3)y_P + a_3(dy_P) + x_P^2(dx_P) + (da_4)x_P + a_4(dx_P) + da_6 = 0.$$

Folglich $v(x_P^2(dx_P)) = -4k + v(dx_P) \geq \min\{v(a_3) - 3k - 1, v(a_4) - 2k - 1, v(a_6) - 1\}$. Daraus folgt dann $v(dx_P) \geq \min\{v(a_3), v(a_4) + 1, v(a_6) + 3\}$, also gilt die Behauptung. \square

Lemma 1.4.16. *Sei die Notation wie zuvor mit A eine minimale Weierstraß-Gleichung mit $v(a_3), v(a_4), v(a_6) \geq 0$ und habe A gute Reduktion, d.h. $v(a_3) = 0$. Dann gilt $\text{Sel}(K_v, V) = R_v + K_v^2$ und $\text{Sel}(K_v, F) = a_3^{-2}R_v + K_v^2$.*

Beweis. Sei (x_P, y_P) ein Punkt auf $A(K_v)$. Nach Lemma 1.4.15 besitzt x_P modulo K_v^2 einen Repräsentanten in R_v . Das beweist – zusammen mit den rationalen Funktionen für die Abstiegs-Abbildungen – $\text{Sel}(K_v, V) \subseteq R_v + K_v^2$ und $\text{Sel}(K_v, F) \subseteq a_3^{-2}R_v + K_v^2$. Die andere Richtung folgt dann aus der Orthogonalität. Dafür verwenden wir, dass das orthogonal Komplement von R_v/K_v^2 wieder R_v/K_v^2 ist, wie sich unschwer an der Formel aus Lemma 1.4.13 für die Paarung als Spur des Residuums erkennen lässt. Wir können das aber auch direkt beweisen. Dafür zeigen wir, dass für alle $r \in R_v$ ein $z \in K_v$ existiert mit $r + z^2$ ist die x -Koordinate eines Punktes auf $A^{(2)}(K_v)$. Angenommen die reduzierte Kurve $\bar{A}^{(2)}$ besitzt einen nichttrivialen Punkt (x_0, y_0) . Das ist nach Hasse der Fall, wenn der Restklassenkörper mehr als vier Elemente besitzt. Da der Frobenius auf endlichen Körpern surjektiv ist, finden wir ein $z \in R_v$, so dass $x' = r + z^2$ durch die Restklassenabbildung auf x_0 abgebildet wird. Sei $y \in R_v$ ein Lift von y_0 . Dann gilt $v(y^2 + a_3^2y + x'^3 + a_4^2x' + a_6^2) \geq 1$ und somit ist x' nach Lemma 2.3.1 die x -Koordinate eines Punktes auf $A^{(2)}(K_v)$. Daraus folgt die Behauptung. Sei also der Restklassenkörper von K_v isomorph zu \mathbb{F}_2 oder \mathbb{F}_{2^2} und sei $r \in R_v$ gegeben. Da $A_1(K_v)$ isomorph zu einer formalen Gruppe ist (siehe dazu [Sil86, VII.2.2]) besitzt $A(K_v)$ einen Punkt $P = (x_P, y_P)$ mit $v(x_P) = -2$ und $v(y_P) = -3$. Damit ist $(x', y') := F(P)$ ein Punkt auf $A^{(2)}(K_v)$ mit $v(x') = -4$ und $x' = x_P^2$ ist ein Quadrat. Definiere $z := x_P$, $x := r + z^2$ und $y := y' + \hat{y}$. Einsetzen in die Weierstraß-Gleichung von $A^{(2)}$ liefert das Polynom

$$p(\hat{y}) = \hat{y}^2 + a_3^2\hat{y} + r^3 + r^2z^2 + rz^4 + a_4r$$

in der Variablen \hat{y} . Für $v(r) > -v(z^4) = 8$ gilt $v(r^3 + r^2z^2 + rz^4 + a_4r) \geq 1$ und somit besitzt $p(\hat{y})$ nach Lemma 2.3.1 eine Nullstelle in K_v welche uns einen Punkt auf $A^{(2)}(K_v)$ mit $r + z^2$ als x -Koordinate liefert. Es verbleiben also die Fälle mit $0 \leq v(r) \leq 8$. Ziel ist es, für diese jeweils Elemente $x' \in K_v^2$, $y' \in K_v$ zu bestimmen, mit $x := r + x'$ und $y := y' + \hat{y}$, so dass das Polynom

$$p(\hat{y}) = \hat{y}^2 + a_3\hat{y} + y'^2 + a_3^2y' + x^3 + a_4^2x + a_6^2$$

eine Nullstelle in K_v besitzt. Das ist der Fall, für $v(y'^2 + a_3^2y' + x^3 + a_4^2x + a_6^2) \geq 1$. Daher suchen wir nun nach solchen $x = r + x'$ und y' . Angenommen wir beschränken uns auf $x' \in K_v^2$ mit $v(x') \geq -4$. Dann gilt auch $v(y') \geq -6$. Sei π eine lokale Uniformisierende. Um $v(y'^2 + a_3^2y' + x^3 + a_4^2x + a_6^2) \geq 1$ zu erreichen, sind dann r, x', y', a_3^2, a_4^2 und a_6^2 modulo $\pi^9, \pi^9, \pi, \pi^7, \pi^5$ bzw. π relevant. Zu entscheiden, ob

es für alle a_3, a_4, a_6 und r solche x' und y' gibt, ist nun ein endliches Problem. Ein einfaches Magma-Programm – siehe auch Bemerkung 1.4.17 – zeigt nach wenigen Stunden die Existenz von x' und y' und vervollständigt so unseren Beweis für $\text{Sel}(K_v, F) = a_3^{-2}R_v + K_v^2$. Für $\text{Sel}(K_v, V)$ verfahren wir analog. \square

Bemerkung 1.4.17. *Es genügt nicht, sich auf x' mit $v(x') \geq -2$ zu beschränken. In einigen Fällen wird $v(x') = -4$ benötigt. Wenn wir mit $A^{(2)}$ arbeiten, dann sind die Koeffizienten der Weierstraß-Gleichung Quadrate und somit die Koeffizienten der Reihenentwicklungen an den ungeraden π -Potenzen gleich null. Da wir r modulo Quadrate abändern können, können wir annehmen, dass alle Koeffizienten an geraden π -Potenzen gleich null sind. Wir haben also*

$$\begin{aligned} a_3^2 &= a_{3,0}^2 + a_{3,1}^2\pi^2 + a_{3,2}^2\pi^4 + a_{3,3}^2\pi^6 + O(\pi^7) \\ a_4^2 &= a_{4,0}^2 + a_{4,1}^2\pi^2 + a_{4,2}^2\pi^4 + O(\pi^5) \\ a_6^2 &= a_{6,0}^2 + O(\pi) \\ r &= r_1\pi + r_3\pi^3 + r_5\pi^5 + r_7\pi^7 + O(\pi^9) \\ y' &= y_{-6}\pi^{-6} + y_{-5}\pi^{-5} + y_{-4}\pi^{-4} + y_{-3}\pi^{-3} + y_{-2}\pi^{-2} + y_{-1}\pi^{-1} + y_0 + O(\pi) \\ x' &= x_{-4}\pi^{-4} + x_{-2}\pi^{-2} + x_0 + x_2\pi^2 + x_4\pi^4 + x_6\pi^6 + x_8\pi^8 + O(\pi^9) \end{aligned}$$

Indem wir untersuchen, wann die reduzierte Kurve nichttriviale Punkte besitzt, kennen wir auch $a_{3,0}, a_{4,0}$ und $a_{6,0}$. Wir haben also 9 unbekannte Koeffizienten aus \mathbb{F}_{2^2} für a_3^2, a_4^2, a_6^2 und r . Das liefert uns $4^9 = 262144$ Gleichungssysteme in den 14 Koeffizienten von x' und y' . Sie zu lösen nimmt relativ wenig Zeit in Anspruch. Für \mathbb{F}_2 verfahren wir analog.

Bemerkung 1.4.18. *Einen dritten Beweis für Lemma 1.4.16 liefert das Lemma 1.2 in [Ulm91]. Dort wird bewiesen, dass in der betrachteten Situation die Isomorphie $\text{Sel}(K_v, F) \cong H^1(R_v, \ker F)$ gilt und aufgrund der langen exakten Kohomologiesequenz können wir R_v/R_v^2 als Untergruppe von $H^1(R_v, \ker F)$ auffassen (und für V analog).*

Bemerkung 1.4.19. *Die lokalen V - und F -Selmergruppen sind für supersinguläre elliptische Kurven keine endlichen Gruppen. Für elliptische Kurven, die den Voraussetzungen von Lemma 1.4.16 genügen folgt das direkt aus der Aussage des Lemmas. Für die anderen lässt sich diese Aussage mit derselben Technik verifizieren: Die Kurven A und $A^{(2)}$ besitzen einen K_v -rationalen Punkt und wenn wir zu dessen x -Koordinate ein $r \in R_v$ mit ausreichend großer Bewertung addieren, bekommen wir die x -Koordinate eines weiteren Punktes. Auf diese Weise können wir unendlich viele Punkte konstruieren, deren x -Koordinaten modulo K_v^2 in verschiedenen Klassen liegen.*

1.5 Globale Selmergruppen

In diesem Abschnitt wollen wir die obigen Überlegungen zu den lokalen Selmergruppen kombinieren, um die globalen Selmergruppen zu beschreiben.

1.5.1 n teilerfremd zur Charakteristik

In [CFO⁺08], [CFO⁺09] und [CFO⁺] beschreiben Cremona, Fisher, O’Neil, Simon und Stoll Ideen zur Berechnung der n -Selmergruppe für elliptische Kurven über Zahlkörpern für beliebige n . Ihre Methoden lassen sich auch auf globale Funktionenkörper, deren Charakteristik n nicht teilt, übertragen. Viele der Ergebnisse sind aber eher theoretischer Natur und lassen sich in der Praxis für $n > 5$ nur bedingt verwenden. Die existierenden Implementationen für einen 2-Abstieg über Zahlkörpern können wir mit kleineren Modifikationen auch in unserer Situation anwenden. Sie liefern uns eine Einbettung der globalen 2-Selmergruppe in ein Produkt endlicher Gruppen

$$K_i(S_i, 2) := \{b \in K_i^\times / (K_i^\times)^2 \mid v(b) \equiv 0 \pmod{2} \text{ für alle } v \notin S_i\},$$

wobei K_i ein endlicher Erweiterungskörper von K und S_i eine endliche Menge von Bewertungen von K_i ist. Ausführliche Informationen sowohl zu Eigenschaften der $K_i(S_i, 2)$ als auch zur Berechnung der globalen Selmergruppe finden sich in [Sim98], [Sim02] und [Wom03].

1.5.2 Gewöhnliche elliptische Kurven

Sei A die durch die Weierstraß-Gleichung $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ gegebene gewöhnliche elliptische Kurve über dem globalen Körper K der Charakteristik 2. Ziel ist es, die globalen V^i - und F^i -Selmergruppen für $i = 1, 2$ zu beschreiben. Dazu geben wir jeweils erst endliche Obermengen an und sortieren anschließend die Elemente aus, die nicht in allen lokalen Selmergruppen enthalten sind. In dem gesamten Abschnitt setzen wir für $i = 2$ voraus, dass die V^2 -Torsion von $A^{(4)}$ über K definiert ist, also dass $a_2 = a_1^2(s^2 + s)$ für ein $s \in K$ gilt.

Proposition 1.5.1. *Es gibt (effektive) Divisoren $D_j \in \text{Div}(K)$, so dass alle Elemente aus $\text{Sel}(K, V^i)$ einen Repräsentanten $b = (b_0, \dots, b_{i-1}) \in W_i(K)$ mit b_j in $\mathcal{L}(D_j)$ besitzen. Hier bezeichnet $\mathcal{L}(D_j)$ den Riemann-Roch-Raum des Divisors D_j und es gilt $0 \leq j \leq i-1 \leq 1$. Alle Stellen, an denen A und somit auch $A^{(2^i)}$ gute Reduktion besitzt, liegen nicht im Träger der D_j .*

Beweis. Sei v eine Stelle von K mit $v(\Delta(A)) = 0$ und seien die Koeffizienten a_1, a_2 und a_6 v -ganz. Jedes $b = (b_0, \dots, b_{i-1}) \in \text{Sel}(K, V^i)$ kann auch als Element von $\text{Sel}(K_v, V^i)$ aufgefasst werden. Dann besitzt es aber modulo $\wp(W_i(K_v))$ einen Repräsentanten $b' = (b'_0, \dots, b'_{i-1})$, bei dem die v -Bewertung aller Komponenten nicht negativ ist. Ohne Einschränkung können wir dabei annehmen, dass b' in $W_i(K)$ liegt. Unter Verwendung des starken Approximationssatzes können wir $w(b_j) \leq w(b'_j)$ für alle Stellen $w \in \mathbb{P}_K \setminus \{w_0\}$ fordern. Nach endlich vielen Schritten gilt $w(b'_j) \geq 0$ für alle außer endlich viele Stellen. Die verbleibenden Stellen sind w_0 sowie der Träger von $(\Delta(A))$ und die weiteren Pole der a_i . Mit demselben Vorgehen und unter Verwendung der Bemerkung 1.4.12 können wir die Bewertungen der Komponenten von b' auch an den anderen von w_0 verschiedenen Stellen durch Schranken, die nur von der Bewertung der Koeffizienten abhängen, nach unten beschränken. Durch die Addition geeigneter Elemente aus $\wp(W_i(K))$, deren Komponenten nur an w_0 Pole haben, reduzieren wir die Bewertung von b' an dieser Stelle. Würden wir beliebige Pole erlauben, so könnten wir erneut Bemerkung 1.4.12 verwenden. Da wir aber nur Pole an w_0 zulassen, bekommen wir eine schlechtere Schranke, die zusätzlich zu $w_0(a_1)$ auch von dem Geschlecht von K und dem Grad von w_0 abhängt. Ist w_0 eine Stelle vom Grad 1, so

folgt das direkt unter Betrachtung der Sequenz der Polzahlen. Hat w_0 einen größeren Grad, so hängt die Schranke zusätzlich davon ab, für welches n die Leitkoeffizienten der Laurentreihenentwicklung der Elemente in $\mathcal{L}(nw_0) \setminus \mathcal{L}((n-1)w_0)$ den gesamten Restklassenkörper von w_0 liefern. \square

Bemerkung 1.5.2. Um die Divisoren D_j explizit anzugeben, benötigen wir nur die Pole und Nullstellen von $\Delta(A)$ und von den a_i , so wie das Geschlecht von K .

Lemma 1.5.3. Sei $v \neq w_0$ eine Stelle mit $v(\Delta(A)) = 0$ und $v(a_i) \geq 0$. Weiterhin sei $b = (b_0, \dots, b_{i-1}) \in W_i(K)$ ein Wittvektor mit $b_j \in \mathcal{L}(D_j)$ der Repräsentant einer Nebenklasse modulo $\wp(W_i(K))$. Dann liegt die Klasse von b in $\text{Sel}(K_v, V^i)$.

Beweis. Die Komponenten von b liegen in $\mathcal{L}(D_j)$. Da v nicht im Träger der D_j ist, liegen die b_j auch in R_v . Die Beschreibung von $\text{Sel}(K_v, V^i)$ nach Korollar 1.4.9 beweist die Behauptung. \square

Es verbleiben endlich viele Stellen. Für diese können wir die lokalen V^i -Selmergruppen nach Bemerkung 1.4.12 berechnen und überprüfen, welche der endlich vielen Elemente in allen enthalten sind.

Für die F^i -Selmergruppen verfahren wir ähnlich.

Lemma 1.5.4. Sei $S \subseteq \mathbb{P}_K$ eine endlich Menge der Bewertungen von K . Dann ist die Menge $K(S, p^i) := \{a \in K^\times / (K^\times)^{p^i} \mid v(a) \equiv 0 \pmod{p^i} \text{ für alle } v \notin S\}$ endlich. Sie sitzt in der exakten Sequenz

$$0 \rightarrow \mathcal{O}_{K,S}^\times / (\mathcal{O}_{K,S}^\times)^{p^i} \rightarrow K(S, p^i) \rightarrow \text{Cl}(\mathcal{O}_{K,S}) / p^i \text{Cl}(\mathcal{O}_{K,S}) \rightarrow 0.$$

Hierbei bezeichnen $\mathcal{O}_{K,S}^\times$ und $\text{Cl}(\mathcal{O}_{K,S})$ die S -Einheiten- bzw. S -Klassengruppe.

Beweis. Die Beweise aus [PS97, 12.6] oder [Sim98, II.4.2] lassen sich einfach auf unsere Situation übertragen. \square

Bemerkung 1.5.5. Erzeuger der S -Einheiten- und S -Klassengruppe lassen sich theoretisch und für ausreichend einfaches K auch praktisch berechnen. Mit ihnen können wir die Elemente aus $K(S, p^i)$ darstellen. Für S den Träger des Hauptdivisors von $\Delta(A)$ zusammen mit den Polen der Koeffizienten ist $K(S, 2^i)$ nach Korollar 1.4.9 eine endliche Obermenge von $\text{Sel}(K, F^i)$.

Nun können wir genau wie bei der V^i -Selmergruppe verfahren. Da die lokalen F^i -Selmergruppen unendlich sind, überprüfen wir nicht, welche Elemente aus $K(S, 2^i)$ in allen $\text{Sel}(K_v, F^i)$ liegen, sondern welche der Elemente orthogonal zu allen $\text{Sel}(K_v, V^i)$ sind. Wegen Korollar 1.4.9 können wir uns auf die Stellen, die in S liegen, beschränken. Die Artin-Schreier-Witt-Paarung lässt sich wie bei [Tho05] beschreiben, effizient auswerten. Weitere Details finden sich auch in Abschnitt 2.3.

1.5.3 Supersinguläre elliptische Kurven

Sei A die durch $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ gegebene supersinguläre elliptische Kurve über dem globalen Körper K der Charakteristik 2. Wie auch bei den gewöhnlichen elliptischen Kurven können wir eine endliche Obermenge der globalen Selmergruppen angeben.

Proposition 1.5.6. *Es gibt (effektive) Divisoren D_F und $D_V \in \text{Div}(K)$, so dass alle Elemente aus $\text{Sel}(K, F)$ und $\text{Sel}(K, V)$ einen Repräsentanten in $\mathcal{L}(D_F)$ bzw. $\mathcal{L}(D_V)$ besitzen.*

Beweis. Hier können wir wie bei Aussage 1.5.1 vorgehen. Das Lemma 1.4.15 liefert uns obere Schranken für die Pole der Elemente der globalen Selmergruppe. Wie schon im Beweis von Lemma 1.5.1 bekommen wir unter Verwendung des starken Approximationssatzes eine weitere Stelle w_0 , an der Pole auftreten können. Doch auch hier ist die Polordnung durch einen von der w_0 -Bewertung der Koeffizienten und vom Geschlecht von K abhängigen Wert beschränkt. \square

Bemerkung 1.5.7. *Wir können anhand der Bewertungen der Koeffizienten und Invarianten von K die Divisoren D_F und D_V explizit berechnen.*

Nun wollen wir für ein Element a aus K/K^2 entscheiden, ob es in $\text{Sel}(K, F)$ liegt (für $\text{Sel}(K, V)$ verfahren wir analog). Das Lemma 1.4.16 reduziert dieses Problem auf die Untersuchung endlicher Stellen v . Für diese erzeugen wir – wie auch bei den gewöhnlichen elliptischen Kurven – Punkte und testen auf Orthogonalität unter der Cup-Produkt-Paarung. Dabei sind wir mit einigen kleineren Schwierigkeiten konfrontiert. Details finden sich in Abschnitt 2.3.

1.6 Globale Bilder

1.6.1 Allgemein

Das Berechnen des Bildes einer Abstiegs-Abbildung steht im Zusammenhang mit der Theorie der prinzipal-homogenen Räume. An dieser Stelle geben wir eine kurze Zusammenfassung bekannter Resultate. Für ausführlichere Informationen sei auf Kapitel X in [Sil86] und auf [CFS10] verwiesen. Da wir in einigen Fällen mit unserer speziellen flachen Kohomologietheorie arbeiten, unterscheiden sich unsere Definitionen und Beweise leicht von denen in den angegebenen Quellen. Vergleiche dazu [Mil80, III.4]. Im Folgenden werden wir gelegentlich auch nur von homogenen Räumen sprechen, gemeint seien aber immer prinzipal-homogene Räume. Sei $\psi : A \rightarrow B$ eine Isogenie der über dem globalen Körper K definierten elliptischen Kurven A und B . Den Verbindungshomomorphismus

$$\delta_\psi : B(K) \rightarrow H^1(K, \ker \psi)$$

haben wir ψ -Abstiegs-Abbildung genannt. Ziel dieses Abschnitts ist es, das Bild $\text{Im } \delta_\psi$ für ψ gleich $[n], V^i$ oder gleich F^i zu beschreiben. Wir wissen bereits, dass $\text{Im } \delta_\psi$ eine Untergruppe der endlichen Gruppe $\text{Sel}(K, \psi)$ ist. Die Sequenz

$$0 \rightarrow B(K)/\psi(A(K)) \xrightarrow{\delta_\psi} H^1(K, \ker \psi) \rightarrow H^1(K, A)[\psi] \rightarrow 0,$$

die wir durch das Herausfaktorisieren des Kerns von δ_ψ – wir bezeichnen die resultierende Abbildung wieder mit δ_ψ – und das Einschränken von $H^1(K, A)$ auf den Kern von ψ erhalten, ist exakt. Folglich gilt $\text{Im } \delta_\psi = \ker(H^1(K, \ker \psi) \rightarrow H^1(K, A)[\psi])$. Das Bild von δ_ψ besteht also aus Elementen, deren Bild in $H^1(K, A)$ unter der von der Inklusion $\ker \psi \rightarrow A$ induzierten Abbildung trivial ist. Die Gruppe $H^1(K, A)$ selbst steht in 1 : 1-Korrespondenz zu Isomorphieklassen von prinzipal-homogenen Räumen. Siehe [Sil86, X.3.6] und [Mil80, III.4.6]. Dabei wird das neutrale Element von

$H^1(K, A)$ mit der Klasse von A identifiziert. Ein homogener Raum C ist in derselben Klasse wie A genau dann, wenn $C(K)$ nicht leer ist. Wir können also das Bild von δ_ψ berechnen, indem wir jedes Element ξ aus $\text{Sel}(K, \psi)$ über die Inklusion als Element von $H^1(K, A)$ auffassen, einen Repräsentanten C der zu ξ korrespondierenden Isomorphieklasse homogener Räume wählen und überprüfen, ob C einen K -rationalen Punkt besitzt. In diesem Licht betrachtet, liegt ein Element $\xi \in H^1(K, \ker \psi)$ in $\text{Sel}(K, \psi)$, wenn ein (und damit jeder) Repräsentant C der korrespondierenden Klasse für alle $v \in \mathbb{P}_K$ einen Punkt über K_v besitzt. Die globale Selmergruppe korrespondiert zu den Isomorphieklassen überall lokal trivialer homogener Räume.

Da ein prinzipal-homogener Raum C für $C(K)$ nicht leer zu A isomorph ist, handelt es sich bei ihnen um Twists von A . Das heißt, jeder solche homogene Raum C ist über dem algebraischen Abschluß \bar{K} zu A isomorph. Insbesondere hat C das Geschlecht eins. Im Folgenden werden wir für eine Kurve C vom Geschlecht eins auch Geschlecht-Eins-Kurve schreiben. Besitzt C einen K -rationalen Divisor vom Grad n , so sprechen wir auch von einer Geschlecht-Eins-Kurve vom Grad n . Für konkrete Rechnungen benötigen wir ein explizites Modell für C eingebettet in einen geeigneten projektiven Raum. Ein detaillierter Überblick über verschiedene Modelle und Eigenschaften von Kurven vom Geschlecht eins findet sich in [Fis08] und ein etwas kürzerer in Abschnitt 2.4.1.

Ist C ein homogener Raum für den zuvor erwähnten ψ -Abstieg, dann zeigt uns ein Punkt $P \in C(K)$ nicht nur, dass das zu C korrespondierende Element aus $H^1(K, \ker \psi)$ im Bild von δ_ψ liegt, sondern liefert uns auch ein Urbild unter δ_ψ und somit einen Punkt auf $B(K)$, sofern die Überlagerung $C \rightarrow B$ konkret gegeben ist, was für gewöhnlich der Fall ist. Daher bezeichnen wir die zu den Elementen der ψ -Selmergruppe gehörigen homogenen Räume auch als ψ -Überlagerungen. Es wird angenommen, dass die naive Höhe des Punktes auf $B(K)$ um den Faktor $\deg \psi$ größer ist, als die von P (zumindest unter den richtigen Voraussetzung, die sich hauptsächlich darauf beziehen, dass C ein geeignetes Modell benötigt). Das ist ein weiterer Vorteil dieser Technik.

1.6.2 n teilerfremd zur Charakteristik

In [CFO⁺08], [CFO⁺09] und [CFO⁺] beschreiben die Autoren die Berechnung globaler n -Selmergruppen über Zahlkörpern. Sie geben sehr allgemeine Konstruktionen zur Berechnung von Modellen für die homogenen Räume an. Viele ihrer Resultate lassen sich auf globale Funktionenkörper der Charakteristik p teilerfremd zu n übertragen. Allerdings sind wir dort mit denselben Problemen wie über Zahlkörpern konfrontiert. Zum einen benötigt das Berechnen von algorithmisch günstigen Gleichungen für die homogenen Räume die Berechnung einer Lösung eines Problems über zentral-einfache Algebren, für welches nur in Spezialfällen ein effizienter Algorithmus existiert, zum anderen werden verschiedene andere Rechnungen für wachsendes n für praktische Zwecke schnell undurchführbar.

Das klassische Verfahren zur Berechnung der homogenen Räume für $n = 2$ basiert darauf, die Lösungen einer homogenen Gleichung vom Grad 2 in drei Variablen zu parametrisieren, denn diese definieren Geschlecht null Kurven und sind daher birational äquivalent zu einer projektiven Gerade, und diese dann in eine weitere solche Gleichung einzusetzen. Vergleiche [Sim02] oder [Wom03]. Über einem rationalen Funktionenkörper können wir dabei den in [vHC06] vorgestellten Algorithmus verwenden. Das ist genau das, was in [Rob07] gemacht wird. Für Kegelschnitte über nichttrivialen

Erweiterungen eines rationalen Funktionenkörpers müssen wir etwas anders vorgehen. Der Algorithmus, den wir dafür verwenden, basiert auf dem in Magma implementierten Algorithmus zum Lösen von Kegelschnitten über Zahlkörpern. Die Idee dafür geht zurück auf Legendre und wird in [CR03] mit Legendre-Typ-Reduktion bezeichnet. Dabei verwenden wir Gitterreduktion, um sukzessive die Koeffizienten des Kegelschnittes zu reduzieren. Entweder finden wir dabei eine Lösung oder wir transformieren die reduzierte Gleichung in eine Normgleichung in einer quadratischen Erweiterung und lösen diese mit einem generischen Algorithmus, siehe zum Beispiel [Fie97]. Die Theorie der Gitterreduktion im Zusammenhang mit globalen Funktionenkörpern findet sich in [Sch96].

1.6.3 Gewöhnliche elliptische Kurven

1.6.3.1 Der Fall $m = 1$

Sei K ein globaler Körper der Charakteristik 2. Im Folgenden werden wir die Kohomologiegruppen $H^1(K, \ker V)$ und $H^1(K, \ker F)$ – wie schon zuvor beschrieben – mit den Gruppen $W_1(K)/\wp(W_1(K)) = K/\wp(K)$ bzw. $K^\times/(K^\times)^2$ identifizieren. Für ein Element $v \in K/\wp(K)$ führt die Suche nach einem $P = (x, y) \in A(K)$ mit $\alpha_1(P) = v$ zu den Gleichungen

$$y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0 \text{ und } \alpha_1(x, y) = \frac{x + a_2}{a_1^2} = v + z^2 + z$$

in den Variablen x, y und z . Diese definieren eine Kurve C_v über K . Wir können die Variable x eliminieren und mit Hilfe einiger elementarer K -rationaler Transformationen erhalten wir die glatte, ebene, affine – siehe Abschnitt 2.4.1.4 für die Glattheit – Kurvengleichung

$$y^2 + (a_1z^2 + a_1^2z + (a_1^3v + a_1a_2))y + a_1^2vz^4 + (a_1^3v + a_1^3 + a_1a_2)z^3 + (a_1^4v^2 + a_1^4v + a_2^2)z^2 + (a_1^5v^2 + a_1a_2^2)z + a_1^6v^3 + a_1^2a_2^2v + a_6 = 0.$$

Gleichungen der Form $y^2 + p(z)y + q(z) = 0$ mit $\deg p \leq 2$ und $\deg(q) \leq 4$ beschreiben nach [Fis08] Geschlecht-Eins-Kurven mit einem K -rationalen Divisor vom Grad zwei. Das können wir auch über die Funktionenkörper direkt zeigen.

Lemma 1.6.1. *Die zu C_v gehörige projektive Kurve hat das Geschlecht $g = 1$, ist glatt und besitzt einen K -rationalen Divisor vom Grad 2.*

Beweis. Wir können C_v als die durch $(x + a_2)/a_1^2 = v + z^2 + z$ definierte Überlagerung der elliptischen Kurve A auffassen. Auf der Seite der Funktionenkörper haben wir eine Artin-Schreier-Erweiterung des elliptischen Funktionenkörpers $K(A)$. Der Erweiterungsgrad ist 2. Der Divisor über der unendlichen Stelle von $K(A)$ liefert also einen K -rationalen Divisor dieses Grades. Das Geschlecht können wir über die verzweigten Stellen bestimmen. Wir wenden dazu [Sti93, III.7.8] an. Das Element $(x + a_2)/a_1^2$ hat eine nichtnegative Bewertung an allen Stellen, die nicht über der unendlichen Stelle von $K(A)$ liegen. Die Erweiterung ist dort also unverzweigt. Des Weiteren gilt

$$\left(\frac{y}{a_1x}\right)^2 + \frac{y}{a_1x} + \frac{x + a_4}{a_1^2} = \frac{y^2 + a_1xy + x^3 + a_4x^2}{a_1^2x^2} = \frac{a_6}{a_1^2x^2}.$$

Folglich ist die Erweiterung an allen Stellen unverzweigt, hat also dasselbe Geschlecht wie $K(A)$, nämlich eins. In [Sti93] wird angenommen, dass die Konstantenkörper der

Funktionenkörper vollkommen sind. Das ist in unserer Situation zwar nicht der Fall, die von uns verwendeten Aussagen gelten aber auch für nicht vollkommene Konstantenkörper. Die Glattheit des obigen Modells folgt aus der Diskriminante zusammen mit Abschnitt 2.4.1.4. \square

Für Kurven in der zuvor beschriebenen Form können wir Gleichungen für die Jacobische angeben, siehe [Vil]. Aus der Gleichheit der j -Invariante folgt, dass C_v ein Twist von $A^{(2)}$ ist.

Da C_v eine über K -definierte Überlagerung von A ist, liefert jeder K -rationale Punkt auf C_v auch einen K -rationalen Punkt auf A .

Bemerkung 1.6.2. *Wir können die Glattheit von C_v auch beweisen, ohne die Diskriminante zu verwenden. Dazu verwenden wir, dass A selbst glatt über K ist. Der Morphismus $C_v \rightarrow A$ gegeben durch die Überlagerung C_v von A über die Gleichung $(x + a_2)/a_1^2 = v + z^2 + z$ ist unverzweigt. Das gilt, denn nach obiger Argumentation sind alle Stellen unverzweigt. Ausserdem sind alle Erweiterungen der Restklassenkörper Artin-Schreier-Erweiterungen, also separabel. Weiterhin ist $C_v \rightarrow A$ flach. Der Grund dafür ist, dass A regulär ist, also durch die Spektren diskreter Bewertungsringe R_i überdeckt wird. Damit wird C_v von den Spektren von endlichen, torsionsfreien R_i -Algebren überdeckt und daraus folgt die Flachheit. Somit ist $C_v \rightarrow A$ étale und damit auch glatt. Die Komposition der glatten Morphismen $C_v \rightarrow A$ und $A \rightarrow \text{Spec } K$ ist glatt, also ist C_v glatt über K . Vergleiche auch [Vol90, Bemerkung 1.4]*

Sei nun $b \in K^\times / (K^\times)^2$. Die Suche nach einem $P = (x, y) \in A^{(2)}(K)$ mit $\beta_1(P) = b$ liefert die Gleichungen $y^2 + a_1^2 xy + x^3 + a_2^2 x^2 + a_6^2 = 0$ und $x = bz^2$. Die durch diese Gleichungen definierte Varietät lässt sich durch einige elementare Umformungen in die durch $y^2 + a_1^2 bxy + a_1^2 a_6 bx^4 + a_2^2 b^2 x^2 + b^3 = 0$ definierte ebene, affine, glatte Kurve C_b transformieren. Wie schon zuvor beschrieben, handelt es sich hierbei um eine Geschlecht-Eins-Kurve vom Grad 2 gemäß [Fis08]. Auch das lässt sich mit dem folgenden Lemma direkt zeigen:

Lemma 1.6.3. *Die zu C_b gehörige projektive Kurve hat das Geschlecht $g = 1$, ist glatt und besitzt einen K -rationalen Divisor vom Grad 2.*

Beweis. Der Funktionenkörper $K(C_b)$ ist eine rein inseparable Erweiterung des elliptischen Funktionenkörpers $K(A^{(2)})$ und entsteht durch Adjunktion einer Quadratwurzel von x an $K(A^{(2)})$. Da der Erweiterungsgrad 2 ist, liefert die Konorm der unendlichen Stelle von $K(A^{(2)})$ den gewünschten Divisor. Die Aussage über das Geschlecht beweisen wir mit Tates Geschlechtsformel. Diese findet sich in [Tat52] oder [Sal06, 9.5.20]. Sei g das Geschlecht von $K(C_b)$, dann gilt

$$2g = 2 - \sum_{Q \in \mathbb{P}_{K(A^{(2)})}} s_Q$$

mit

$$s_Q = \begin{cases} r_Q \deg Q & \text{für } 2 \mid r_Q \\ (r_Q - 1) \deg Q & \text{für } 2 \nmid r_Q \end{cases}$$

und

$$r_Q = \max_{u \in K(A^{(2)})} \{v_Q(u^2 + x)\}.$$

Nun berechnen wir r_Q . Ist $Q = \mathcal{O}$ die unendliche Stelle von $K(A^{(2)})$, so gilt für die Bewertung $v_Q((y/x)^2 + x) = v_Q(a_1^2 y/x + a_4^2 + a_6^2/x^2) = -1$. Diese ist ungerade, also maximal. Daher gilt $r_Q = -2$ in diesem Fall. Sei nun Q der nichttriviale 2-Torsionspunkt von $K(A^{(2)})$. Dann gilt $v_Q(x) = 2$ und $v(y + a_6) = 1$. Somit ist $y + a_6$ eine lokale Uniformisierende dieser Stellen. Eine einfache Rechnung zeigt

$$x + 1/(a_1^2 a_6)(y + a_6)^2 = 1/(a_1^2 a_6^2)(y + a_6)^3 + O((y + a_6)^4).$$

Ist also $a_1^2 a_6$ ein Quadrat, so gilt $r_Q = 3$, sonst $r_Q = 2$. Für eine Stelle Q , die nicht im Träger von (x) auftritt, gilt $r_Q \geq 0$. Tates Geschlechtsformel zeigt

$$2g = 2 - \sum_{Q \in \mathbb{P}_{K(A^{(2)})}} s_Q = 2 - 2 + 2 \sum_{Q \in \mathbb{P}_{K(A^{(2)})} \setminus \text{supp}((x))} s_Q \leq 2.$$

Also gilt $g \leq 1$. Wir nehmen einer Konstantenkörpererweiterung mit dem algebraisch Abschluß \bar{K} des Konstantenkörpers vor und erhalten $\bar{K}(C_b)$ als Erweiterung von $\bar{K}(A^{(2)})$. Betrachten wir $\bar{K}(A^{(2)})$ als Erweiterung des rationalen Funktionenkörpers $\bar{K}(x)$, sehen wir, dass es ein $a \in \bar{K}$ gibt, mit $x + a$ ist lokale Uniformisierende von Q . Hier verwenden wir noch, dass über der Stelle $x + a$ von $\bar{K}(x)$ zwei Stellen von $\bar{K}(A^{(2)})$ liegen. Da a ein Quadrat in \bar{K} ist, gilt $a = u^2$ und $v(x + u^2) = 1$. Somit haben wir $r_Q = 1$. Insgesamt gilt $2g' = 2 + 2 - 2$ also $g' = 1$, wobei g' das Geschlecht von $\bar{K}(C_b)$ bezeichnet. Da das Geschlecht bei einer Konstantenkörpererweiterung nicht wachsen kann (vergleiche [Sal06, 8.5.3]) gilt $1 \leq g' \leq g \leq 1$. Die Glattheit des obigen Modells folgt aus der Diskriminante zusammen mit Abschnitt 2.4.1.4. \square

Wie auch bei dem V -Abstieg können wir mit Hilfe der Jacobischen beweisen, dass es sich bei C_b um einen Twist von A handelt. Da wir C_b als über K definierte Überlagerung von $A^{(2)}$ konstruiert haben, liefern K -rationale Punkte auf C_b eben solche auf $A^{(2)}$.

1.6.3.2 Der Fall $m = 2$

Wir gehen davon aus, dass die Weierstraß-Gleichung von A die Form

$$y^2 + a_1 xy + x^3 + a_1^2(s^2 + s)x^2 + a_6 = 0$$

besitzt. Nach Lemma 1.3.3 besitzt $A^{(4)}$ volle V^2 -Torsion und wir identifizieren die Kohomologiegruppen $H^1(K, \ker V^2)$ und $H^1(K, \ker F^2)$ wie zuvor beschrieben mit den Gruppen $W_2(K)/\wp(W_2(K))$ bzw. $K^\times/(K^\times)^4$. Ein $v = (v_0, v_1) \in W_2(K)$ liegt im Bild von α_2 , genau wenn die Gleichungen

$$y^2 + a_1 xy + x^3 + a_1^2(s^2 + s)x^2 + a_6 = 0$$

und

$$\alpha_2(x, y) = \left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{s a_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right) = (v_0, v_1) + \wp(z_0, z_1)$$

eine Lösung $(x, y, z_0, z_1) \in K^4$ besitzen. Fassen wir die Gleichung der Wittvektoren als zwei Gleichungen über dem Körper auf, so erhalten wir drei Gleichungen in vier Variablen. Sie definieren eine Kurve.

Lemma 1.6.4. *Der Funktionenkörper dieser Kurve hat das Geschlecht 1 und besitzt einen K -rationalen Divisor vom Grad 4. Sie ist birational äquivalent zu einer über K definierten glatten Kurve C_v und C_v ist gegeben als der Schnitt der Nullstellenmengen zweier homogener Polynome vom Grad 2 in 4 Variablen im \mathbb{P}^3 .*

Beweis. Mit Blick auf die Konstruktion der V^2 -Abstiegs-Abbildung in Lemma 1.3.2, können wir den Funktionenkörper als eine Erweiterung von $K(A)$ durch einen Turm bestehend aus zwei Artin-Schreier-Erweiterungen auffassen. Die Konorm der unendlichen Stelle von $K(A)$ liefert den gesuchten K -rationalen Divisor vom Grad 4. Wir zeigen nun, dass die Artin-Schreier-Erweiterungen unverzweigt über $K(A)$ sind. Dazu gehen wir wie in Lemma 1.6.1 vor. Nach Aussage 2.1 in [Tho05] genügt es zu zeigen, dass für alle $v_P \in \mathbb{P}_{K(A)}$ ein $z = (z_0, z_1) \in W_2(K(A))$ existiert, so dass die Bewertung der Komponenten von $\alpha_2(x, y) + (v_0, v_1) + \wp(z)$ größer gleich 0 sind. Da $(v_0, v_1) \in W_2(K)$, die Komponenten also konstant in $K(A)$ sind, ist ersichtlich, dass die Aussage auf Grund der Dreiecksungleichung für Bewertungen für alle (v_0, v_1) gilt, wenn sie für $v_0 = 0, v_1 = 0$ gilt. Die Komponenten von

$$\left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{sa_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right)$$

haben Pole nur für $x = 0$, also für die zu dem nichttrivialen 2-Torsionspunkt korrespondierende Stelle von $K(A)$. Wir betrachten nun

$$z = \left(\frac{y}{a_1 x}, \frac{sy}{a_1 x} + \frac{x}{a_1^2} + (s^2 + s) + \frac{a_6}{a_1^2 x^2} \right).$$

Eine längere Rechnung unter Verwendung der Weierstraß-Gleichung und der Rechenregeln für Wittvektoren zeigt

$$\alpha_2(x, y) + \wp(z) = \left(\frac{x + a_2}{a_1^2}, \frac{s^2(x + a_2)}{a_1^2} + \frac{x + a_2}{a_1^2} + \frac{y}{a_1^3} \right)$$

und die Komponenten dieses Wittvektors haben keine Pole für $x = 0$.

Um das beschriebenes Modell C_v für die Kurve zu finden, können wir wie folgt vorgehen. Sei mit D der K -rationale Divisor vom Grad 4 bezeichnet. Mit Hilfe von Magma können wir eine Basis des Riemann-Roch-Raums $\mathcal{L}(D)$ berechnen, welche wir mit b_1, \dots, b_4 bezeichnen. Die Relationen der $b_i b_j$ liefern uns zwei quadratische Formen in den Variablen x_1, \dots, x_4 und das gewünschte Modell ist deren Schnitt, vergleiche [Sad09]. Wir können explizite Gleichungen für das Modell angeben. Als Ergebnis bekommen wir rationale Funktionen in den a_i und den Einträgen des Wittvektors v als Koeffizienten der quadratischen Formen. Da diese sehr lang und unübersichtlich sind, verzichten wir an dieser Stelle darauf, sie hier aufzulisten. Die benötigten Rechnungen können aber mit Magma schnell durchgeführt werden. Die Diskriminante zeigt, dass das Modell glatt ist. Wie in Bemerkung 1.6.2 sehen wir, dass die durch die Gleichung der Wittvektoren definierte Kurve eine étale-Überlagerung von A und somit glatt ist. Da die Kurve als K -rationale Überlagerung von A konstruiert wurde, liefern ihre K -rationalen Punkte auch Elemente aus $A(K)$. Um das explizit zu machen, sehen wir, dass x in $\mathcal{L}(2D)$ enthalten ist und sich daher als Linearkombination der $b_i b_j$ schreiben lässt. \square

Sei $b \in K^\times$ der Repräsentant eines Elements aus $K^\times / (K^\times)^4$. Dann bekommen wir Gleichungen

$$y^2 + a_1^4 xy + x^3 + a_1^8 (s^8 + s^4) x^2 + a_6^4 = 0$$

und

$$\beta_2(x, y) = y + 1/a_1^4 x^2 + a_1^4 s^4 x = bz^4.$$

Diese definieren eine Kurve.

Lemma 1.6.5. *Der Funktionenkörper dieser Kurve hat das Geschlecht 1 und besitzt einen K -rationalen Divisor vom Grad 4. Sie ist birational äquivalent zu einer über K definierten glatten Kurve C_b und C_b ist gegeben als der Schnitt der Nullstellenmengen zweier homogener Polynome vom Grad 2 in 4 Variablen im \mathbb{P}^3 .*

Beweis. Wir schreiben den durch die Weierstraß-Gleichung von $A^{(4)}$ und $\beta_2(x, y) = b$ definierten Funktionenkörper E als rein inseparable Erweiterung von $K(A)$ vom Grad 4. Dann können wir diese Aussage mit der schon bei Lemma 1.6.3 verwendeten Technik beweisen. Für alle $b \in K^\times$ hat das Element $1/b(y + 1/a_1^4 x^2 + a_1^4 s^4 x)$ nach Konstruktion den Divisor $4T - 4\mathcal{O}$, wobei T zu einem nichttrivialen 4-Torsionspunkt auf $K(A^{(4)})$ korrespondiert. Tates Geschlechtsformel beweist die Aussage.

So wie zuvor beschrieben bekommen wir über die Berechnung einer Basis x_1, \dots, x_4 von $\mathcal{L}(D)$ und der Relationen der $x_i x_j$ das gesuchte Modell C_b . Hierbei ist D der K -rationale Divisor vom Grad 4 von E , der über der unendlichen Stelle von $K(A)$ liegt. Als Resultat erhalten wir die durch die Gleichungen

$$\begin{aligned} q_1 &= 1/(a_1^{14} a_6 b) x_1^2 + 1/(a_1^2 a_6) x_2 x_3 + x_4^2, \\ q_2 &= x_1 x_4 + x_2^2 + a_1^4 b x_3^2. \end{aligned}$$

definierte projektive Kurve. Ihre Glattheit folgt unter Verwendung der Diskriminante. \square

1.6.4 Supersinguläre elliptische Kurven

Sei A eine supersinguläre elliptische Kurve über einem Körper der Charakteristik 2. Für ein Element $b \in K/K^2$ führt die Suche nach einem $P = (x, y) \in A(K)$ mit $\alpha_1(P) = b$ zu den Gleichungen

$$y^2 + a_3 y + x^3 + a_4 x + a_6 = 0 \text{ und } \alpha_1(x, y) = x = b + z^2.$$

Diese definieren eine Kurve C_b . Elimination von x gefolgt von der Transformation $y \mapsto y + z^3$ liefert die Kurvengleichung

$$y^2 + a_3 y + bz^4 + a_3 z^3 + (a_4 + b^2)z^2 + a_4 b + a_6 + b^3 = 0.$$

Wie schon bei den gewöhnlichen elliptischen Kurven gesehen, beschreibt solch eine Gleichung nach [Fis08] eine Geschlecht-Eins-Kurve mit einem K -rationalen Divisor vom Grad 2. Auch hier können wir das direkt mit Hilfe der Funktionenkörper nachweisen. Die Argumentation verläuft genau wie bei Lemma 1.6.3. Bei dem supersingulären F -Abstieg verfahren wir analog. Wir bekommen die Gleichungen

$$y^2 + a_3^2 y + x^3 + a_4^2 x + a_6^2 = 0 \text{ und } \beta_1(x, y) = a_3^{-2} x = b + z^2.$$

Diese liefern uns die definierende Gleichung

$$y^2 + a_3^2 y + a_3^6 b z^4 + a_3^5 z^3 + (a_3^6 b^2 + a_3^2 a_4^2) z^2 + a_3^6 b^3 + a_3^2 a_4^2 b + a_6^2 = 0$$

einer Kurve vom Geschlecht eins mit einem K -rationalen Divisor vom Grad 2. Mit Hilfe der Diskriminante zeigen wir, dass die beiden korrespondierenden projektiven Modelle glatt sind. Anders als in den vorherigen Fällen, können wir nicht sicher sein, dass b aus der globalen Selmergruppe stammt, da wir diese nur approximiert haben. Folglich gibt es endlich viele Stellen v – siehe Abschnitt 1.5.3 – für die wir nicht sicher sind, ob C_b einen K_v -rationalen Punkt besitzt. Das können wir analysieren, bevor wir C_b auf K -rationale Punkte untersuchen, siehe dazu Abschnitt 2.3.2.

1.7 Keine volle p^2 -Torsion

Bei dem V^2 - und F^2 -Abstieg gewöhnlicher elliptischer Kurven haben wir vorausgesetzt, dass die volle p^2 -Torsion von $A^{(p^2)}$ über K definiert ist. In diesem Abschnitt zeigen wir, wie man vorgehen kann, falls das nicht der Fall ist. Wir beschränken uns dabei auf die Charakteristik $p = 2$ und verwenden die zuvor beschriebene Weierstraß-Gleichung für gewöhnliche elliptische Kurven. Ist die Charakteristik von 2 verschieden, dann ist ein analoges Vorgehen möglich. Wir haben bereits gezeigt, dass die 2-Torsion von $A^{(4)}$ immer bereits über K definiert ist. Weiterhin wissen wir, dass nach Lemma 1.3.3 $A^{(4)}$ volle 4-Torsion über $L = K(\gamma)$ besitzt, wobei L die durch $\gamma^2 + \gamma + a_2/a_1^2 = 0$ definierte Artin-Schreier-Erweiterung ist. Im Folgenden nehmen wir an, dass L eine echte Erweiterung von K ist und bezeichnen die Galoisgruppe $\text{Gal}(L/K)$ mit $G = \langle g \rangle$. Sei T ein Erzeuger für $\ker V^2(L)$. Es existieren Gruppenhomomorphismen

$$\begin{aligned}\alpha_{i,K} &: A(K) \rightarrow H^1(K, \ker V^i), \\ \alpha_{i,L} &: A(L) \rightarrow H^1(L, \ker V^i), \\ \beta_{i,K} &: A^{(2^i)}(K) \rightarrow H^1(K, \ker F^i), \\ \beta_{i,L} &: A^{(2^i)}(L) \rightarrow H^1(L, \ker F^i).\end{aligned}$$

Diese sind die Verbindungshomomorphismen der Kohomologiesequenzen. Sei ein Isomorphismus der L -Gruppenschemata $\ker V^2$ und $\mathbb{Z}/4\mathbb{Z}$ sowie $\ker F^2$ und μ_4 fixiert. Wie zuvor beschrieben sind $H^1(L, \ker V^2)$ und $H^1(L, \ker F^2)$ zu $W_2(L)/\wp(W_2(L))$ bzw. $L^\times/(L^\times)^4$ isomorph, was wir bereits zur Konstruktion der Abstiegs-Abbildungen in Abschnitt 1.3.2.3 und 1.3.3.3 ausgenutzt haben. Unter Verwendung der zuvor eingeführten Techniken können wir mit Hilfe von $\alpha_{2,L}$ und $\beta_{2,L}$ Informationen über $A(L)$ gewinnen. Diese liefern uns auch Aussagen über den Rang und Erzeuger von $A(K)$.

1.7.1 V^2 -Abstieg

Unser Ziel ist es, die Kardinalität und Erzeuger für $A(K)/V^2(A^{(4)}(K))$ zu bestimmen. Bezeichnen wir mit Φ die Untergruppe $(A(K) \cap V^2(A^{(4)}(L)))/V^2(A^{(4)}(K))$, dann haben wir die folgende exakte Sequenz

$$0 \rightarrow \Phi \rightarrow A(K)/V^2(A^{(4)}(K)) \rightarrow A(L)/V^2(A^{(4)}(L)).$$

Die Kardinalität des Bildes von $A(K)/V^2(A^{(4)}(K))$ in $A(L)/V^2(A^{(4)}(L))$ zusammen mit der von Φ liefern uns die gesuchte Kardinalität von $A(K)/V^2(A^{(4)}(K))$. Ebenso bekommen wir Erzeuger für $A(K)/V^2(A^{(4)}(K))$ wenn wir Erzeuger von Φ und von dem Bild von $A(K)/V^2(A^{(4)}(K))$ in $A(L)/V^2(A^{(4)}(L))$ kennen. Da V^2 eine separable

Isogenie ist, der Kern also étale ist, stimmt die zuvor verwendete flache Kohomologie mit der Galoiskohomologie überein. Siehe Anhang 6.2. Daher arbeiten wir in diesem Abschnitt immer mit letzterer. Als erstes untersuchen wir Φ .

Lemma 1.7.1. *Wir können Φ mit einer Untergruppe von $H^1(G, \ker V^2)$ identifizieren.*

Beweis. Das findet sich bei [Sil86] im Beweis von VIII.1.1. \square

Lemma 1.7.2. *Die Gruppe $H^1(G, \ker V^2)$ besitzt zwei Elemente.*

Beweis. Die 1-Koketten bestehen aus allen Abbildungen ξ von G nach $\ker V^2$. Aufgrund der Kozykelbedingung gilt $\xi(\text{id}) = 0$ für alle $\xi \in Z^1(G, \ker V^2)$. Des Weiteren gibt es zwei Koränder, nämlich $g \mapsto (g(0) - 0) = 0$ und $g \mapsto g(T) - T = 3T - T = 2T$. Somit sind $g \mapsto 0$ und $g \mapsto T$ Repräsentanten der Elemente aus $H^1(G, \ker V^2)$. \square

Die Berechnung eines nichttrivialen Elements in Φ können wir auf das Berechnen von Punkten auf geeigneten homogenen Räumen zurückführen. Dafür bedarf es einiger Überlegungen. Es sei daran erinnert, dass für $P \in A(K)$ und ein Urbild Q von P unter V die Erweiterung $K(Q)$ mit der durch $\alpha_{1,K}(P)$ erzeugten Artin-Schreier-Erweiterung $K(\wp^{-1}(\alpha_{1,K}(P)))$ übereinstimmt, vergleiche Abschnitt 1.3.2. Im Folgenden werden wir die V -Abstiegs-Abbildung auf $A(K)$, $A(L)$, $A^{(2)}(K)$ und $A^{(2)}(L)$ zur Vermeidung unnötiger Indizes mit $\alpha_{1,K}$ oder $\alpha_{1,L}$ bezeichnen und, falls die Situation es erfordert, darauf hinweisen, welche gemeint ist.

Lemma 1.7.3. *Sei P der Repräsentant eines Elements aus Φ und liege P nicht in $V^2(A^{(4)}(K))$. Sei $Q \in A^{(2)}(\bar{K})$ mit $V(Q) = P$. Dann gilt $K(Q) = L$.*

Beweis. Nach Voraussetzung gilt $P \in V^2(A^{(4)}(L))$ und somit $K(R) \subseteq L$ für alle $R \in A^{(4)}$ mit $V^2(R) = P$, und wegen $P \notin V^2(A^{(4)}(K))$ gilt sogar Gleichheit. Folglich gilt $K(Q) = K$ oder $K(Q) = L$. Angenommen wir haben $K(Q) = K$. Sei S der nichttriviale 2-Torsionspunkt von $A^{(2)}$. Dann ist $Q + S$ das zweite Urbild von P unter V in $A^{(2)}(\bar{K})$. Sei T ein Punkt der Ordnung 4 auf $A^{(4)}$, dann gilt $V(T) = S$ und $K(T) = L$. Weiterhin gelte $V(R) = Q$ und $K(R) = L$ für ein geeignetes $R \in A^{(4)}$. Somit erzeugen die Urbilder von Q und S unter V beide L , also $\alpha_{1,K}(Q) = \alpha_{1,K}(S)$ und daher gilt $\alpha_{1,K}(Q + S) = 0$. Die Urbilder von $Q + S$ unter V sind folglich K -rational. Also gilt $P \in V^2(A^{(4)}(K))$ als Widerspruch zur Voraussetzung. \square

Das Lemma kann als notwendiges Kriterium für $\#\Phi = 2$ angesehen werden. Damit Φ einen nichttrivialen Punkt besitzen kann, muss ein $P \in A(K)$ existieren, für das $K(V^{-1}(P)) = L$ gilt. Die Konstruktion solch eines Punktes wollen wir auf das Finden von Punkten auf über K definierten homogenen Räumen zurückführen. Die Frage, ob ein Punkt $P \in A(K)$ mit $K(V^{-1}(P)) = L$ existiert, ist äquivalent zu der Frage, ob ein Element $b \in K/\wp(K)$ im Bild von $\alpha_{1,K}$ auf $A(K)$ liegt. Das wiederum ist äquivalent zu der Frage, ob ein homogener Raum C_b einen K -rationalen Punkt besitzt. Ist das nicht der Fall, wissen wir, dass Φ trivial ist. Können wir aber einen K -rationalen Punkt auf C_b finden, so liefert uns das einen Punkt $P \in A(K)$ mit $K(V^{-1}(P)) = L$. Für einen nichttrivialen Punkt in Φ ist nicht nur das Urbild unter V , sondern auch das Urbild unter V^2 über L definiert. Ersteres gilt für alle Punkte auf $A(K)$, die von K -rationalen Punkten auf C_b kommen. Zweiteres untersuchen wir nun. Unterschiedliche Punkte auf C_b liefern P und P' auf $A(K)$ mit $P - P' \in V(A^{(2)}(K))$ und vice versa. Sei nun solch ein P fest gewählt. Wir fragen uns, ob wir P modulo $V(A^{(2)}(K))$ abändern

können, so dass $P + V(M) \in V^2(A^{(4)}(L))$ liegt mit M in $A^{(2)}(K)$ geeignet. Dann würde $P + V(M)$ ein nichttriviales Element in Φ liefern. Bezeichne $Q + M \in A^{(2)}(L)$ ein Urbild von $P + V(M)$ unter V . Das Urbild von $Q + M$ unter V ist L -rational genau dann, wenn $\alpha_{1,L}(Q + M) \equiv 0 \pmod{\wp(L)}$ gilt. Hier ist mit $\alpha_{1,L}$ die V -Abstiegs-Abbildung auf $A^{(2)}(L)$ bezeichnet. Wir suchen also ein M mit $\alpha_{1,L}(M) = -\alpha_{1,L}(Q)$. Allerdings soll M über K definiert sein, so dass $M = -Q$ keine Möglichkeit ist. Da $\alpha_{1,L}(M) = a_6^2/(a_1^2 x(M))^2$ einen Repräsentanten in K besitzt, ist die Gleichheit $\alpha_{1,L}(M) = -\alpha_{1,L}(Q)$ nur möglich, wenn es ein $z \in L$ gibt, mit $-\alpha_{1,L}(Q) + \wp(z) \in K$.

Lemma 1.7.4. *Die Fasern der von der Einbettung $K \rightarrow L$ induzierten Abbildung $\iota : K/\wp(K) \rightarrow L/\wp(L)$ sind entweder leer oder zweielementig.*

Beweis. Sei $b = b_1 + b_2\gamma \in L$ beliebig. Dann besitzt b ein Urbild unter ι genau wenn es ein z in L mit $b + \wp(z) \in K$ gibt. Wir schreiben $z \in L$ als $z = z_1 + z_2\gamma$ mit z_1 und z_2 in K . Dann haben wir $b + \wp(z) = (b_1 + z_2^2 a_2/a_1^2 + \wp(z_1)) + (b_2 + \wp(z_2))\gamma$. Die Gleichung $b_2 + \wp(z_2) = 0$ besitzt keine oder zwei Lösungen in K . Angenommen es gibt zwei Lösungen. Dann unterscheiden sie sich um den Wert 1. Sie liefern unterschiedliche Urbilder in $K/\wp(K)$, da a_2/a_1^2 nicht in $\wp(K)$ liegt. \square

Gibt es kein $z \in L$ mit $-\alpha_{1,L}(Q) + \wp(z) \in K$, dann ist Φ trivial. Anderenfalls bekommen wir $-\alpha_{1,L}(Q) \equiv c_i \pmod{\wp(K)}$ für explizite Werte $c_i \in K$, $i = 1, 2$. Es gibt ein $M \in A^{(2)}(K)$ mit $\alpha_{1,K}(M) = c_i + \wp(K)$ für ein $i \in \{1, 2\}$ genau dann, wenn der korrespondierende homogene Raum D_i einen K -rationalen Punkt besitzt. In diesem Fall ist die Klasse von $V(Q + M) \in A(K)$ das gesuchte nichttriviale Element in Φ . Zusammengefasst führen wir die folgenden Schritte durch:

1. Berechne $P \in A(K)$ mit $K(V^{-1}(P)) = L$ durch das Finden eines Punktes auf einer über K definierten V -Überlagerung von A .
2. Berechne Q mit $V(Q) = P$ und Urbilder c_1 und c_2 in $K/\wp(K)$ von $\alpha_{1,L}(Q)$ unter $\iota : K/\wp(K) \rightarrow L/\wp(L)$.
3. Berechne $M \in A^{(2)}(K)$ mit $\alpha_{1,K}(M) = c_1$ oder $\alpha_{1,K}(M) = c_2$ durch das Finden eines Punktes auf einer über K definierten V -Überlagerung von $A^{(2)}$.
4. Das gesuchte Element in Φ ist $V(Q + M)$.

Nun untersuchen wir das Bild von $A(K)/V^2(A^{(4)}(K))$ in $A(L)/V^2(A^{(4)}(L))$. Die Inflations-Restriktions-Sequenz (vergleiche [Mil13, Bemerkung 1.35]) ist exakt und liefert uns

$$0 \rightarrow H^1(G, \ker V^2) \rightarrow H^1(G_K, \ker V^2) \xrightarrow{\text{res}} H^1(G_L, \ker V^2)^G.$$

Lemma 1.7.5. *Ein Element $\xi \in H^1(G_L, \ker V^2)$ wird von G fixiert, genau wenn für den zu ξ korrespondierenden Wittvektor $w \in W_2(L)$ gilt $gw - w \in \wp(W_2(L))$. Das heißt, die Wirkung von G auf $H^1(G_L, \ker V^2)$ ist mit dem Isomorphismus nach $W_2(L)/\wp(W_2(L))$ verträglich.*

Beweis. Die Wirkung von G auf $H^1(G_L, \ker V^2)$ erfolgt durch $(g\xi)(\sigma) := g(\xi(g^{-1}\sigma g))$. Sei $w \in W_2(L)$ und v ein Urbild von w unter \wp , so dass $\xi(\sigma) = \sigma v - v$ gilt. Dann gilt $(g\xi)(\sigma) = g(g^{-1}\sigma g v - v) = \sigma g v - g v$. Somit ist ξ invariant unter G , genau wenn $\sigma v - v = \sigma g v - g v$ für alle $\sigma \in G_L$ gilt. Das ist äquivalent zu $g v - v = \sigma(g v - v)$ und somit zu $g v - v \in W_2(L)$, also $\wp(g v - v) = g\wp(v) - \wp(v) = gw - w \in \wp(W_2(L))$. \square

Lemma 1.7.6. *Das Bild von $\text{Sel}(K, V^2)$ unter der Restriktionsabbildung liegt in $\text{Sel}(L, V^2)^G$.*

Beweis. Sei ι_A die Einbettung $A(K) \rightarrow A(L)$. Dann gilt für $P \in A(K)$ die Gleichheit $\alpha_{2,L}(\iota_A(P)) = \text{res}(\alpha_{2,K}(P))$. Diese gilt auch für die Vervollständigungen bezüglich einer Stelle v von K . Damit gilt die Aussage nach der Definition der Selmergruppen. \square

Indem wir die G -invarianten Elemente von $\text{Sel}(L, V^2)$ bestimmen, bekommen wir unter Berücksichtigung des möglicherweise nichttrivialen Kerns der Restriktionsabbildung auf den Selmergruppen eine obere Schranke für die Kardinalität von $\text{Sel}(K, V^2)$. Nun wollen wir für solch ein G -invariantes Element b entscheiden, ob es im Bild von $\alpha_{2,K}$ liegt. Das bedeutet wir untersuchen, ob es ein $P \in A(K)$ gibt mit $\text{res}(\alpha_{2,K}(P)) = \alpha_{2,L}(\iota_A(P)) = b + \wp(z)$. Indem wir $z = (z_1, z_2) \in W_2(L)$ als $z = (z_{11} + z_{12}\gamma, z_{21} + z_{22}\gamma)$ mit $z_{ij} \in K$ schreiben, $\wp(z)$ formal berechnen und die Einträge der Wittvektoren $\alpha_{2,L}(\iota_A(P))$ und $b + \wp(z)$ vergleichen, bekommen wir vier Gleichungen über K in den Variablen z_{11}, \dots, z_{22}, x und y so wie die Weierstraß-Gleichung für A . Sie bilden eine Überlagerung von A durch einen Turm aus vier Artin-Schreier-Erweiterungen.

Lemma 1.7.7. *Für ein $b \in W_2(L)/\wp W_2(L)$, das einem Repräsentanten der Form $b = (b_0, b_1 + b_0\gamma)$ mit $b_0, b_1 \in K$ besitzt, existiert eine glatte, projektive, über K definierte Kurve C_b . Dabei ist C_b der Schnitt zweier Quadriken, hat das Geschlecht 1 und besitzt einen K -rationalen Divisor vom Grad 4. Sei $b \in \text{Sel}(L, V^2)^G$. Das Element b liegt im Bild von $\text{res} \circ \alpha_{2,K}$ genau dann, wenn b die zuvor beschriebene Form hat und die Kurve C_b einen K -rationalen Punkt besitzt.*

Beweis. Liegt $b = (b_{0,0} + b_{0,1}\gamma, b_{1,0} + b_{1,1}\gamma)$ im Bild von $\text{res} \circ \alpha_{2,K} = \alpha_{2,L} \circ \iota_A$, so gibt es $(x, y) \in A(K)$ und $z \in W_2(L)$ mit

$$\left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{\gamma a_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right) = (b_{0,0} + b_{0,1}\gamma, b_{1,0} + b_{1,1}\gamma) + \wp(z).$$

Folglich können wir annehmen, dass b modulo $\wp(z)$ von der Form $b = (b_0, b_1 + b_0\gamma)$ ist, für ein $z \in W_2(L)$. Die Wittvektoren $\hat{z} \in W_2(L)$ für die

$$(b_0, b_1 + b_0\gamma) + \wp(\hat{z}) = (b'_0, b'_1 + b'_0\gamma)$$

mit $b'_0, b'_1 \in K$ gilt, sind genau die der Form $\hat{z} = (z_0, z_1 + z_0\gamma)$, wie eine kurze Rechnung zeigt. Wir suchen also $z_0, z_1 \in K$ mit

$$\left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{\gamma a_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right) = (b_0, b_1 + b_0\gamma) + \wp(z_0, z_1 + z_0\gamma).$$

Formales Ausrechnen und Vergleichen der Einträge liefert uns eine Überlagerung von A durch zwei Artin-Schreier-Erweiterungen in den Variablen z_0 und z_1 . Die korrespondierende Erweiterung des Funktionenkörpers $K(A)$ hat Grad 4. Somit liefert uns die Konorm der unendlichen Stelle von $K(A)$ den gesuchten K -rationalen Divisor D vom Grad 4. Zur Berechnung des Geschlechts gehen wir genauso vor, wie bei rationaler 4-Torsion und zeigen mit einer fast identischen Rechnung, dass die Erweiterung unverzweigt ist. Wie schon bei dem V^2 -Abstieg mit voller 4-Torsion berechnen wir das Modell C_b mit Hilfe einer Basis der Riemann-Roch-Raums $\mathcal{L}(D)$ und zeigen, dass es glatt ist. \square

Bei C_b handelt es sich also mit der Notation von [Fis08] um eine Geschlecht-Eins-Kurve vom Grad 4.

1.7.2 F^2 -Abstieg

Wir sind daran interessiert, den Rang und Erzeuger für $A^{(4)}(K)/F^2(A(K))$ zu bestimmen. Wie bei dem V^2 -Abstieg liefert uns die Einbettung $A^{(4)}(K) \rightarrow A^{(4)}(L)$ eine Abbildung $A^{(4)}(K)/F^2(A(K)) \rightarrow A^{(4)}(L)/F^2(A(L))$.

Lemma 1.7.8. *Die Abbildung $A^{(4)}(K)/F^2(A(K)) \rightarrow A^{(4)}(L)/F^2(A(L))$ ist injektiv.*

Beweis. Ein Punkt $P \in A^{(4)}(K)$ liegt im Kern, wenn $P \in A^{(4)}(K) \cap F^2(A(L))$ gilt. Das bedeutet die Koordinaten von P sind vierte Potenzen in L . Da L/K separabel ist, müssen die Koordinaten schon vierte Potenzen in K sein und somit liegt P in $F^2(A(K))$. \square

Lemma 1.7.9. *Sei $b'_1 + \gamma b'_2 \in L^\times$ mit $b'_i \in K$ der Repräsentant eines Elements, das ein Urbild in $A^{(4)}(K)$ unter der Abstiegs-Abbildung $\beta_{2,L}$ besitzt. Dann gibt es Elemente $b_1, b_2 \in K$ mit $b'_1 + \gamma b'_2 \equiv b_1 + \gamma^4 b_2 \pmod{(L^\times)^4}$ und $b_1^2 + b_1 b_2 + b_2^2 a_2^4 / a_1^8$ ist eine vierte Potenz in K .*

Beweis. Gebe es $(x_0, y_0) \in A^{(4)}(K)$ ein Urbild von $b'_1 + \gamma^4 b'_2$ unter $\beta_{2,L}$. Das heißt es gilt $y_0 + 1/a_1^4 x_0^2 + a_1^4 \gamma^4 x_0 = (b'_1 + \gamma b'_2) z^4$ für ein $z \in L^\times$. Koeffizientenvergleich liefert die Existenz von b_1 und b_2 (alternativ ist γ^4 ebenfalls ein primitives Element von L/K). Unter Verwendung der Weierstraß-Gleichung verifizieren wir

$$(y_0 + 1/a_1^4 x_0^2)^2 + (y_0 + 1/a_1^4 x_0)(a_1^4 x_0) + a_2^4 / a_1^8 (a_1^4 x_0)^2 = 1/a_1^8 x_0^4 + a_6^4 \in K^4.$$

\square

Bemerkung 1.7.10. *Da es einfach ist zu entscheiden, ob zu gegebenen $(b'_1 + \gamma b'_2)$ solch ein $z \in L$ existiert, liefert uns das ein Kriterium, mit dem wir zeigen können, dass bestimmte Elemente aus $\text{Sel}(L, F^2)$ kein Urbild in $A^{(4)}(K)$ besitzen. Das können wir nutzen, um eine bessere Abschätzung für die Kardinalität von $A^{(4)}(K)/F^2(A(K))$ zu bekommen. Des Weiteren sei von nun an immer angenommen, dass die Repräsentanten $b_1 + \gamma^4 b_2$ in dieser Form vorliegen.*

Lemma 1.7.11. *Sei ein Element b aus $\text{Sel}(L, \ker F^2) \subseteq L^\times / (L^\times)^4$ gegeben. Dann besitzt b ein Urbild in $A^{(4)}(K)$ unter β_2 genau dann, wenn sich b modulo $(L^\times)^4$ in die oben beschriebene Form bringen lässt und wenn eine bestimmte über K definierte glatte, projektive Geschlecht-Eins-Kurve C_b vom Grad 4 einen K -rationalen Punkt besitzt. Dabei ist C_b der Schnitt zweier Quadriken.*

Beweis. Mit obigem Lemma können wir ohne Beschränkung der Allgemeinheit annehmen, dass $b = b_1 + \gamma^4 b_2$ in der oben beschriebenen Form vorliegt. Nun gibt es ein Urbild genau dann, wenn es einen Punkt $(x, y) \in A^{(4)}(K)$ und $z_1, z_2 \in K$ gibt mit

$$\begin{aligned} y + 1/a_1^4 x^2 &= b_1 z_1^4 + b_2 a_2^4 / a_1^8 z_2^4, \\ a_1^4 x &= b_1 z_2^4 + b_2 z_2^4 + b_2 z_1^4. \end{aligned}$$

Zusammen mit der Weierstraß-Gleichung für $A^{(4)}$ haben wir also 3 Gleichungen in den Variablen x, y, z_1 und z_2 über K . Nun zeigen wir, dass diese einen Funktionenkörper

vom Geschlecht 1 mit einem K -rationalen Divisor vom Grad 4 definieren. Seien zunächst b_1 und b_2 ungleich null. Der Fall $b_1b_2 = 0$ verläuft ähnlich. Multiplizieren der Gleichungen mit b_2 und b_1 und anschließendes Addieren eliminiert z_1 und liefert

$$b_2(y + 1/a_1^4x^2) + b_1a_1^4x = (b_1^2 + b_1b_2 + a_2^4/a_1^8b_2^2)z_2^4.$$

Aufgrund des obigen Lemmas ist $b_1^2 + b_1b_2 + a_2^4/a_1^8b_2^2$ eine vierte Potenz in K . Wir können z_2 substituieren und erhalten

$$b_2(y + 1/a_1^4x^2) + b_1a_1^4x = (z_2')^4.$$

Das liefert uns eine rein inseparable Überlagerung von $A^{(4)}$ vom Grad 4. Die Konorm der unendlichen Stelle liefert uns den gesuchten K -rationalen Divisor vom Grad 4. Um das Geschlecht zu berechnen, gehen wir wie bei Lemma 1.6.3 vor. Unter Verwendung der zuvor bewiesenen Relation für b_1 und b_2 beweisen wir die Aussage mit Tates Geschlechtsformel. Wie schon zuvor beschrieben, können wir nun für konkrete b_1, b_2 die Kurve in die von Fisher beschriebene Normalform bringen. Alles Weitere läuft genau wie bei einem F^2 -Abstieg ab, bei dem die volle 4-Torsion in $A^{(4)}(K)$ liegt. \square

Zusammengefasst ist die Situation ähnlich wie bei einem 2-Abstieg ohne volle 2-Torsion über einem Zahlkörper K , vergleiche [Sim02]. Für die Berechnung der Selmergruppen muss über einem Erweiterungskörper gerechnet werden, aber die Bestimmung des Bildes der Abstiegs-Abbildung basiert auf der Berechnung von K -rationalen Punkten auf Kurven vom Geschlecht eins, die eine spezielle Form besitzen.

Kapitel 2

Algorithmische Details

In diesem Kapitel beschäftigen wir uns mit dem algorithmischen Aspekt der zuvor beschriebenen Theorie und untersuchen die zu lösenden Teilprobleme. Zusätzlich formulieren wir in den Abschnitten 2.4.2 und 2.4.3 Aufgaben, deren Wichtigkeit erst ersichtlich wird, wenn konkrete Rechnungen durchgeführt werden sollen (vergleiche auch Beispiel 4.4). Wir treffen in den Lemmata 2.2.1 und 2.3.8 Aussagen über die Komplexität einiger Schritte. In Abschnitt 2.6 beschreiben wir kurz unsere Implementation der vorgestellten Algorithmen und vergleichen sie mit bestehenden Programmen.

2.1 Der Algorithmus

Sei A eine elliptische Kurve über dem globalen Funktionenkörper K . Wir wollen einen Algorithmus angeben, der den Rang und eine maximale Menge unabhängiger Punkte von $A(K)$ berechnet. Da angenommen wird, dass diese Probleme algorithmisch sehr schwierig zu berechnen sind, können wir nicht hoffen, sie für alle Instanzen zu lösen. Wenn wir sie nicht lösen können, wollen wir zumindest obere und untere Schranken für den Rang sowie möglichst viele unabhängige Punkte berechnen. Im vorherigen Kapitel haben wir bereits die Lösung dieser Aufgaben auf die Untersuchung von $B(K)/\psi^\vee(A(K))$ und $A(K)/\psi(B(K))$ für eine K -rationale Isogenie $\psi : B \rightarrow A$ reduziert und die theoretischen Grundlagen der dafür verwendeten Methoden beschrieben. Im Folgenden wollen wir uns mit den dabei auftretenden algorithmischen Problemen beschäftigen. Auch wenn viele der Aussagen in beliebiger Charakteristik gelten, formulieren wir unsere Ergebnisse hier für $\text{char}(K) = 2$, da dieser Fall sich am stärksten von den bekannten Resultaten für Zahlkörper unterscheidet. Weiterhin nehmen wir an, dass alle benötigten Torsionspunkte K -rational sind. Die Unterschiede, die auftreten, wenn diese erst über einem Erweiterungskörper L definiert sind, sind in Abschnitt 1.7 aufgeführt. Die Auswirkungen auf die Laufzeit finden sich unter 2.2.2. In diesem Kapitel beschreiben wir noch nicht die Berechnung von Mordell-Weil-Basen. Mit der dafür benötigten Erweiterung des Erzeugendensystems einer Untergruppe endlichen Index von $A(K)$ zu einer Basis beschäftigen wir uns erst in Kapitel 3.

Wie schon zuvor beschrieben, unterscheiden sich unsere Methoden zur Untersuchung von $A(K)/\psi(B(K))$ in verschiedenen entscheidenden Details, abhängig davon, ob A gewöhnlich oder supersingulär ist, K -rationale ψ -Torsion besitzt oder nicht, die Charakteristik von K den Grad von ψ teilt oder nicht. Das grobe Vorgehen bleibt aber immer dasselbe. Statt direkt mit Punkten auf der Kurve zu arbeiten, betten wir

$A(K)/\psi(B(K))$ mit einer Abstiegs-Abbildung δ in eine geeignete Gruppe R ein. Die Berechnung des Bildes von δ lässt sich in drei große Teilschritte zerlegen.

1. Berechnung einer endlichen Untergruppe $R_0 \subseteq R$ mit $\text{Im } \delta \subseteq R_0$.
2. Berechnung aller Elemente $r \in R_0$, die in der ψ -Selmergruppe, also dem Schnitt über die Bilder von δ angewendet auf $A(K_v)/\psi(B(K_v))$ für alle Vervollständigungen K_v , liegen.
3. Berechnung aller Elemente s der Selmergruppe, die ein Urbild unter δ besitzen.

Wir wollen nun auf die einzelnen Teilschritte näher eingehen und auflisten, welche Aufgaben darin jeweils gelöst werden müssen. Wir geben eine grobe Einordnung der Komplexität der auftretenden Probleme und vergleichen diese mit der Komplexität analoger Probleme bei einem 2-Abstieg über einem Zahlkörper. Wir fixieren dabei einen Körper K und untersuchen die Laufzeit für verschiedene elliptische Kurven über K . Die Inputlänge, relativ zu der wir Laufzeiten messen, sei dann die Summe der Grade der Koeffizienten der Kurve. Diese Festlegung hat den Vorteil, dass die Resultate gut mit den Ergebnissen in [SS97] vergleichbar sind. Der Nachteil ist, dass auf diese Weise die Abhängigkeit der Laufzeit von „Eigenschaften“ von K verschleiert wird. Hinter dem Begriff „Eigenschaften“ verbergen sich in diesem Kontext unter anderem das Geschlecht von K , die Kardinalität des Konstantenkörpers und die Höhe der definierenden Gleichung. Vergleiche dazu auch [Hes02]. Da diese Werte in der Praxis einen großen Unterschied machen, gehen wir kurz auch auf ihre Auswirkungen ein. Wenn wir uns mit algorithmischen Problemen befassen, gehen wir davon aus, dass der globale Funktionenkörper K als eine endliche, separable Erweiterung eines rationalen Funktionenkörpers $k(t)$ gegeben ist. Den ganzen Abschluss von $k[t]$ in K bezeichnen wir als die (endliche) Maximalordnung \mathcal{O}_K von K .

2.2 Berechnung der endlichen Untergruppe R_0

Wenn A eine gewöhnliche elliptische Kurve ist, ist das Bild der V^i -Abstiegs-Abbildung eine Untergruppe von $W_i(K)/\wp(W_i(K))$, für eine supersinguläre Kurve bilden die V - und F -Abstiegs-Abbildung beide nach K/K^2 ab. In den Aussagen 1.5.1 und 1.5.6 haben wir bewiesen, dass die Elemente im Bild einen Repräsentanten in einem bestimmten Riemann-Roch-Raum $\mathcal{L}(D)$ besitzen bzw. bei dem die Komponenten des Wittvektors in geeigneten $\mathcal{L}(D_j)$ liegen. Wir sind also mit zwei Aufgaben konfrontiert. Zum einen müssen wir jeweils einen geeigneten Divisor D , zum anderen eine Basis von $\mathcal{L}(D)$ berechnen. In den Beweisen der beiden Aussagen sehen wir, dass sich die gesuchten Divisoren aus den Pol- und Nullstellendivisoren der Koeffizienten und der Diskriminante von A berechnen lassen. Es gibt Algorithmen zur Berechnung des Hauptdivisors eines Elementes eines globalen Funktionenkörpers. Ihre Laufzeit hängt polynomiell vom Grad des Elements und von den Eigenschaften des Funktionenkörpers ab. Ist der Divisor D bestimmt, so kann mit dem in [Hes02] vorgestellten Algorithmus eine Basis für $\mathcal{L}(D)$ effizient berechnet werden. Die Laufzeit dafür ist ebenfalls polynomiell im Grad von D und auch in den „Eigenschaften“ von K . Aus den oben angegebenen Beweisen ist direkt ersichtlich, dass der Grad von D linear vom Grad des Nullstellendivisors der Diskriminante und von den Graden der Poldivisoren der Koeffizienten abhängt. Die Kardinalität der so erzeugten endlichen Obermenge

wächst exponentiell im Grad von D . Die Basis der Exponentialfunktion ist die Kardinalität des Konstantenkörpers, da $\mathcal{L}(D)$ ein Vektorraum über diesem ist.

Für den F^i -Abstieg einer gewöhnlichen elliptischen Kurve lässt sich eine endliche Obermenge des Bildes wie in Bemerkung 1.5.5 beschrieben über die S -Klassen- und S -Einheitengruppe von K berechnen. Hierbei ist S eine endliche Menge von Stellen. Sie lässt sich, wie schon der Divisor D , über die Pole und Nullstellen der Koeffizienten berechnen. Die Klassen- und Einheitengruppe eines globalen Funktionenkörpers K können theoretisch und auch – sofern K nicht zu kompliziert ist – praktisch berechnet werden. Die Laufzeit dafür hängt polynomiell von der Summe der Grade der Stellen in S , also polynomiell von der Inputlänge, ab. Als Resultat erhalten wir ein $\mathbb{Z}/2^i\mathbb{Z}$ -Erzeugendensystem der gesuchten endlichen Menge. Hierbei ist die Länge des Erzeugendensystems polynomiell in der Summe der Grade der Stellen von S und somit im Input, allerdings besitzt die von dem Erzeugendensystem aufgespannte Gruppe eine exponentielle Kardinalität. Die Laufzeit der Berechnung der S -Klassen- und S -Einheitengruppe hängt aber stark vom Geschlecht und von der Kardinalität des Konstantenkörpers ab, siehe [Hes99]. Wir dürfen also nicht vergessen, dass die daraus resultierende Konstante für festes K sehr groß sein und für komplizierte Körper eine Durchführung dieses Schritts unmöglich machen kann.

Die Aufgaben, die wir in diesem Teilschritt lösen müssen, sind fast dieselben, die auch bei einem 2-Abstieg über einem Zahlkörper K' (oder für $\text{char}(K) \geq 5$) anfallen. Dort lässt sich eine endliche Obermenge des Bildes über Gruppen $K'(S, 2)$ beschreiben. Siehe auch Abschnitt 1.5.1. Dabei bekommen wir S über die „Faktorisierung“ der Diskriminante und $K'(S, 2)$ über die S -Klassen- und S -Einheitengruppe. Als Analogon zu dem Lemma 2 in [SS97] erhalten wir als Zusammenfassung unserer vorherigen Überlegungen die folgende Aussage.

Lemma 2.2.1. *Wir können ein Erzeugendensystem einer endlichen Obergruppe der Bilder der F^i - und V^i -Abstiegs-Abbildung aus Schritt 1 mit Laufzeit polynomiell in der Höhe der Koeffizienten berechnen. Die Länge des Erzeugendensystems ist polynomiell.*

Bemerkung 2.2.2. *Wenn wir nicht annehmen, dass die volle 4-Torsion von $A^{(4)}$ K -rational ist, dann hat das einen großen Einfluss auf die asymptotische Laufzeit von Schritt 1 für den F^2 - und V^2 -Abstieg. In diesem Fall sind Rechnungen in dem Erweiterungskörper K' von K , über dem besagte Torsionspunkte definiert sind, notwendig. Wir können die Eigenschaften des Körpers, über dem gerechnet wird, nicht länger als Konstanten auffassen. Sie hängen nun von der Inputlänge ab und beeinflussen die asymptotische Laufzeit, da mit wachsenden Koeffizienten von A auch K' komplizierter wird. Schon die Laufzeit der Berechnung der S -Klassen- und S -Einheitengruppe wächst mindestens subexponentiell im Geschlecht, wir können also nicht länger davon ausgehen, dass dieser Schritt in polynomieller Zeit zu bewerkstelligen ist.*

In den auftretenden Gruppen $W_i(K)/\wp(W_i(K))$, K/K^2 und $K^\times/(K^\times)^{2^i}$ können wir effizient rechnen. Die Berechnung des Gruppengesetzes erfolgt über Repräsentanten und unter Verwendung der Arithmetik von K . Um zu entscheiden, ob ein Repräsentant das neutrale Element beschreibt, müssen wir ein oder zwei Polynome vom Grad 2 oder 4 über K faktorisieren. Für K/K^2 und $K^\times/(K^\times)^{2^i}$ ist das für den Repräsentanten r das Polynom $T^{2^i} - r \in K[T]$. Für $W_i(K)/\wp(W_i(K))$ bekommen wir i Polynome direkt aus einem polynomiellen Ausdruck für \wp .

2.3 Berechnung der Selmergruppe

In diesem Schritt wird überprüft, welche Elemente der zuvor berechneten endlichen Gruppe R_0 die in Abschnitt 1.4.1 beschriebenen lokalen Bedingungen erfüllen, also in der ψ -Selmergruppe liegen. Dies kann auf unterschiedliche Weise geschehen. Die erste Methode geht laut [Wom03] auf Stoll zurück, findet sich aber auch schon in [SS97]. Hier werden die lokalen Bilder direkt berechnet. Die zweite Methode ist klassisch und basiert darauf, homogene Räume auf lokale Lösbarkeit zu untersuchen. Problematisch ist, dass die zu untersuchende Menge exponentiell groß ist. Wie in [SS97, Abschnitt 3] beschrieben, lässt sich das teilweise umgehen, indem wir mit einem Erzeugendensystem arbeiten, siehe auch Abschnitt 2.3.1.4.

2.3.1 Selmergruppen über die Berechnung der lokalen Bilder

Grundidee dieser Methode ist, dass für alle Bewertungen v von K eine Restriktionsabbildung $\text{res} : R \rightarrow R^v$ existiert, so dass das Diagramm

$$\begin{array}{ccc} A(K)/\psi(B(K)) & \xrightarrow{\delta} & R \\ \downarrow & & \downarrow \text{res} \\ A(K_v)/\psi(B(K_v)) & \xrightarrow{\delta_v} & R^v \end{array}$$

kommutiert. Hierbei ist R je nach Situation durch $W_i(K)/\wp(W_i(K)), K^\times/(K^\times)^2$ oder K/K^2 gegeben und R^v analog nur mit K_v statt K definiert. Die Abbildung δ_v ist durch dieselbe rationale Funktion wie δ gegeben. Die Abbildung res resultiert aus der Einbettung $K \rightarrow K_v$. Details finden sich in Abschnitt 1.4.1. Die ψ -Selmergruppe besteht nun aus allen Elementen $r \in R_0$ mit $\text{res}(r) \in \text{Im } \delta_v$ für alle $v \in \mathbb{P}_K$. Wollen wir für ein r feststellen, ob es in $\text{Sel}(K, \psi)$ liegt, so können wir natürlich nicht alle Bewertungen v separat überprüfen. Die Aussagen 1.4.7 und 1.4.9 für gewöhnliche sowie 1.4.16 für supersinguläre Kurven A beschreiben das Bild von δ_v für fast alle Vervollständigungen und zeigen $\text{res}(r) \in \text{Sel}(K_v, \psi)$. Die endlich vielen noch zu untersuchenden Bewertungen können, wie in Bemerkung 1.4.12 beschrieben, berechnet werden, indem wir die Stellen bestimmen, an denen A keine gute Reduktion besitzt. Diese können mit Tates Algorithmus effizient berechnet werden. Das Problem ist also darauf reduziert, für explizit gegebene $r \in R_0$ und $v \in \mathbb{P}_K$ zu entscheiden, ob r im Bild von δ_v liegt. Dazu erzeugen wir randomisierte Punkte auf $A(K_v)$ und berechnen ihr Bild unter δ_v .

2.3.1.1 Lokale Lösbarkeit von Artin-Schreier-Gleichungen

In Charakteristik 2 reduzieren wir die Konstruktion von Punkten auf $A(K_v)$ auf die Approximation von Lösungen der Gleichung $T^2 + aT + b = 0$ über K_v .

Lemma 2.3.1. *Seien $a, b \in K_v$ und gelte $v(a) = 0$. Dann gilt:*

1. Für $v(b) < 0$ und $v(b)$ ungerade besitzt $T^2 + aT + b = 0$ keine Lösung in K_v .
2. Für $v(b) < 0$ und $v(b)$ gerade existiert ein $u \in K_v$ mit $v(b + u^2 + au) > v(b)$. Die Gleichung $T^2 + aT + b = 0$ besitzt eine Lösung in K_v genau dann, wenn $T^2 + aT + (b + u^2 + au) = 0$ eine Lösung in K_v besitzt.

3. Für $v(b) > 0$ besitzt $T^2 + aT + b = 0$ zwei verschiedene Lösungen in K_v .
4. Für $v(b) = 0$ besitzt $T^2 + aT + b = 0$ zwei verschiedene Lösungen in K_v genau dann, wenn die modulo dem Bewertungsideal reduzierte Gleichung zwei verschiedene Lösungen über dem Restklassenkörper besitzt.

Beweis. 1. Für alle $u \in K_v$ gilt $v(u^2 + au + b) \leq v(b)$, also ist die Gleichung nicht lösbar.

2. Der lokale Körper K_v ist zu $k((\pi))$ isomorph, wobei k der Restklassenkörper und π eine lokale Uniformisierende ist. Sei nun $b = b_{-2n}\pi^{-2n} + O(\pi^{-2n+1})$. Da b_{-2n} ein Quadrat in k ist, also $b_{-2n} = u_0^2$, tut $u := u_0\pi^{-n}$ das Gewünschte. Der zweite Teil der Aussage ist klar.
3. Das folgt aus Hensels Lemma.
4. Sei $b = b_0 + O(\pi)$, $a = a_0 + O(\pi)$ und gelte $b_0 = c_0^2 + a_0c_0$ mit $c_0 \in k$. Dann reduziert die Transformation $T \mapsto T + c_0$ das Problem auf die vorherige Aussage. \square

Bemerkung 2.3.2. Ist die Bewertung von a ungleich null, so können wir die Gleichung durch die Transformation $T \mapsto \pi^{v(a)}T$ in die Form des obigen Lemmas bringen. Das Lemma liefert direkt einen Algorithmus, der entscheidet, ob die Gleichung $T^2 + aT + b = 0$ über K_v lösbar ist, und, falls das der Fall ist, eine Lösung approximiert. Ist $b = \sum_{i=-k}^n b_i\pi^i + O(\pi^{n+1})$ und $a = \sum_{i=0}^{n+k/2} a_i\pi^i + O(\pi^{n+k/2+1})$, dann können wir für $n \geq 0$ die Lösbarkeit entscheiden und eine Lösung bis auf $O(\pi^{n+1})$ genau approximieren. Dabei müssen wir nur eine Gleichung der Form $T^2 + a_0T + b'_0 = 0$ und Quadratwurzeln über dem Restklassenkörper lösen bzw. berechnen. Dieses Vorgehen hat den Vorteil, dass keine Laurentreihen aufwendig invertiert werden müssen. Die Berechnung von $a/\pi^{v(a)}$ und $b/\pi^{2v(a)}$ entspricht nur einem Shift und ist im Allgemeinen wesentlich schneller als die Berechnung von b/a^2 .

Sei nun A durch die Weierstraß-Gleichung $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ oder $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ gegeben. Wählen wir zufällig ein $x \in K_v$, so liefert uns das eine Gleichung der oben beschriebenen Form in y . Da die Koeffizienten von A ursprünglich in K liegen, können wir sie mit beliebiger Präzision approximieren. Abhängig davon, wieviele Stellen von x wir festlegen, können wir ein y entsprechend genau bestimmen.

Bemerkung 2.3.3. Der oben beschriebene Algorithmus funktioniert analog für Gleichungen der Form $T^p + aT + b = 0$ in Charakteristik p . Dann kann er zwar nicht ohne Weiteres zur Konstruktion lokaler Punkte verwendet werden. Das ist aber unproblematisch. Für Charakteristik $p \geq 5$ oder $p = 0$ verwenden wir die kurze Weierstraß-Gleichung $y^2 - x^3 - ax - b = 0$ und benutzen schrittweise Approximation, um zu untersuchen, ob $x^3 + ax + b$ für zufällig gewählte x ein Quadrat ist. Der Aufwand dafür ist in etwa derselbe und entspricht dem Aufwand der Berechnung $x^3 + ax + b$.

2.3.1.2 Gewöhnliche elliptische Kurven

Sei also A eine gewöhnliche elliptische Kurve in Charakteristik 2, $\psi = V^i$ für $i = 1, 2$ und $v \in \mathbb{P}_K$. Dann haben wir die Abstiegs-Abbildungen

$$\alpha_{i,v} : A(K_v)/V^i(A^{(2^i)}(K_v)) \rightarrow W_i(K_v)/\wp(W_i(K_v))$$

$$\beta_{i,v} : A^{(2^i)}(K_v)/V^i(A(K_v)) \rightarrow K_v^\times / (K_v^\times)^{2^i}.$$

Nach Bemerkung 1.4.8 kennen wir die endliche Kardinalität von $\text{Sel}(K_v, V^i)$. Wie zuvor beschrieben erzeugen wir nun Punkte $P \in A(K_v)$ und berechnen $\alpha_{i,v}(P)$. Für einen Repräsentanten a von $\alpha_{i,v}(P)$ in $W_i(K_v)$ können wir durch i -faches Anwenden des unter Lemma 2.3.1 beschriebenen Algorithmus entscheiden, ob es ein $c \in W_i(K_v)$ gibt mit $\wp(c) = a$. Somit können wir mit Repräsentanten arbeiten und diese Überlegung für einen effizienten Test auf Gleichheit verwenden. In der Praxis finden wir mit diesem Vorgehen nach kurzer Zeit ein Repräsentantensystem für das Bild von $\alpha_{i,v}$. Ist nun ein $r + \wp(W_i(K)) \in W_i(K)/\wp(W_i(K))$ gegeben, so können wir $\text{res}(r)$ berechnen und durch elementweisen Vergleich testen, ob es im Bild liegt oder nicht.

Da die lokale F^i -Selmergruppe nicht endlich ist, können wir das obige Vorgehen nicht verwenden, um zu entscheiden, ob ein $r \in K^\times / (K^\times)^{2^i}$ im Bild von $\beta_{i,v}$ liegt. Stattdessen testen wir, ob r zu dem zuvor berechneten Bild von $\alpha_{i,v}$ orthogonal unter der Artin-Schreier-Witt-Paarung ist. Da $\text{Im } \beta_{i,v} = (\text{Im } \alpha_{i,v})^\perp$, können wir so unser Problem in endlich vielen Schritten lösen. In [Tho05, S. 699 - 701] beschreibt Thomas, wie die Artin-Schreier-Witt-Paarung algorithmisch ausgewertet werden kann. Dafür wird nur Arithmetik über Laurentreihenkörpern sowie die Spur über endlichen Körpern benötigt.

Die Laufzeit dieses Schritts unterscheidet sich von dem entsprechenden Schritt in Charakteristik 0. Während in Charakteristik 0 die Kardinalität der lokalen Bildmengen in $O(1)$ liegt, hängt sie bei uns exponentiell von der Bewertung von a_1 ab. Es ist nicht klar, ob dieser Teil des Algorithmus sich im Allgemeinen in polynomieller Zeit durchführen lässt. Angenommen, wir verfügen über ein Orakel, das uns ein minimales Erzeugendensystem des lokalen Bildes berechnet. Dann sind dieses Erzeugendensystem und das Erzeugendensystem der endlichen Obermenge beide polynomiell lang, und die Aufgabe ist darauf reduziert, den Schnitt der beiden Erzeugnisse zu berechnen. Auf diese Weise können wir auch das orthogonale Komplement eines lokalen Bildes als Kern einer linearen Abbildung bestimmen.

2.3.1.3 Supersinguläre elliptische Kurven

Für eine supersinguläre elliptische Kurve A in Charakteristik 2 und $\psi = V$ haben wir lokale Abstiegs-Abbildungen

$$\alpha_{1,v} : A(K_v)/V(A^{(2)}(K_v)) \rightarrow K_v/K_v^2 \text{ und } \beta_{1,v} : A^{(2)}(K_v)/V(A(K_v)) \rightarrow K_v/K_v^2.$$

Die Berechnung der V - und F -Selmergruppe verläuft analog, so dass wir das hier nur exemplarisch für $\text{Sel}(K, V)$ beschreiben. Wollen wir für ein Element $r \in K/K^2$ testen, ob es in der V -Selmergruppe liegt, sind wir mit zwei Problemen konfrontiert. Zum einen gestaltet sich das Rechnen in K_v/K_v^2 schwierig. Ist ein Element a in K_v nur mit beliebig hoher, aber begrenzter Präzision bekannt, dann können wir nicht zeigen, dass es in K_v^2 liegt, es also Repräsentant des neutralen Elements aus K_v/K_v^2 ist. Ein Element aus K_v , geschrieben als Laurentreihe in einer lokalen Uniformisierenden π , ist genau dann ein Quadrat, wenn alle Koeffizienten ungerader π -Potenzen 0 sind. Das lässt sich nicht mit endlicher Präzision entscheiden. Somit können wir nicht ohne weiteres in K_v/K_v^2 mit Repräsentanten in K_v arbeiten. Zum anderen sind nach Bemerkung 1.4.19 weder $\text{Sel}(K_v, V)$ noch $\text{Sel}(K_v, F)$ endlich. Wir behelfen uns, indem wir – ähnlich wie bei dem gewöhnlichen F -Abstieg – von der Cup-Produkt-Paarung Gebrauch machen. Wie zuvor beschrieben, erzeugen wir Punkte P auf $A^{(2)}(K_v)$ und

berechnen ihr Bild unter $\beta_{1,v}$. Da $\text{Sel}(K_v, F)$ und $\text{Sel}(K_v, V)$ orthogonale Komplemente sind, können wir alle Elemente r entfernen, deren Einbettung $\text{res}(r)$ in K_v nicht orthogonal zu $\beta_{1,v}(P)$ steht. Das lässt sich auch mit begrenzter Präzision bewerkstelligen. Für die Auswertung der Paarung wird Arithmetik über K_v und die Spur über dem Restklassenkörper benötigt. Auf diese Weise bekommen wir nach endlich vielen Schritten nur eine verbesserte Approximation der globalen Selmergruppe. Die verbleibenden Elemente können mit der unter Abschnitt 2.3.2 beschriebenen Methode weiter untersucht werden.

2.3.1.4 Optimierung

Das oben beschriebene Vorgehen lässt sich an einigen Stellen beschleunigen. Es bietet sich zum Beispiel bei der Konstruktion von Punkten auf A an, die x -Koordinate nicht vollständig zufällig zu wählen (wie auch immer das zu bewerkstelligen wäre).

Lemma 2.3.4. *Sei A durch die Gleichung $y^2 + a_1xy + x^3 + a_2x^2 + a_6 = 0$ über dem lokalen Körper K_v der Charakteristik 2 gegeben und gelte $v(a_i) \geq 0$ für $i \in \{1, 2, 6\}$. Sei $(X, Y) \in A(K_v)$.*

1. *Für $v(X) = s < 0$ gilt $s \equiv 0 \pmod{2}$ und für $X = \sum_{i=s}^{\infty} x_i \pi^i$ mit π eine lokale Uniformisierende gilt $x_j = 0$ für $s < j < \frac{s}{2}$ und j ungerade.*
2. *Sei $v(X) = s > 0$ und $a_6 = \sum_{i=0}^{\infty} a_{6,i} \pi^i$. Sei a_6 kein Quadrat in K_v , dann ist $s_{\max} := \min\{j \in \mathbb{N} \mid j \text{ ist ungerade und } a_{6,j} \neq 0\}$ wohldefiniert. Es gilt die Ungleichung $v(X) \leq s_{\max}$.*

Beweis. Sei also $v(X) = s < 0$. Da $v(a_i) \geq 0$ und (X, Y) der Weierstraß-Gleichung genügen, gilt $v(X^3) = 3s = v(Y^2) = 2r \equiv 0 \pmod{2}$. Für die anderen Terme gilt dann $v(a_1XY) \geq \frac{5}{2}s$, $v(a_2X^2) \geq 2s$, $v(a_6) \geq 0$. Also gilt $Y^2 = X^3 + O(\pi^{\frac{5}{2}s})$ und somit sind die Koeffizienten aller π^j von X^3 mit $3s < j < \frac{5}{2}s$ gleich null. Da s nach Voraussetzung gerade ist, zeigt formales Ausmultiplizieren von X^3 den ersten Teil der Behauptung. Sei nun $v(X) > s_{\max} > 0$. Dann gilt auch $v(Y) \geq 0$ und somit $v(a_1XY) > s_{\max}$, $v(X^3) > s_{\max}$ und $v(a_2X^2) > s_{\max}$. Damit haben wir aber $Y^2 = a_6 + O(\pi^{s_{\max}+1})$. Da s_{\max} nach Konstruktion ungerade und $a_{6,s_{\max}} \neq 0$ ist, stellt das einen Widerspruch dar und damit gilt auch der zweite Teil der Behauptung. \square

Bemerkung 2.3.5. *Eine analoge Aussage lässt sich auch für supersinguläre Kurven mit Weierstraß-Gleichung $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ formulieren und mit derselben Technik beweisen.*

Geben wir uns eine untere Schranke s_{\min} vor und senken diese, falls nötig, weiter ab, so haben wir $s_{\min} \leq v(x) \leq s_{\max}$. Da wir x nur bis zu einer gewissen vorgegebenen Präzision benötigen, können wir die endlich vielen Koeffizienten ungleich null zufällig und gleichverteilt aus dem endlichen Restklassenkörper wählen.

Eine weitere Optimierung lässt sich durch die Ausnutzung der Gruppenstruktur erreichen. Wir wissen, dass es sich bei den globalen und lokalen Selmergruppen – wie der Name schon sagt – um Gruppen und bei den Abstiegs-Abbildungen um Gruppenhomomorphismen handelt. Das kann auf zwei Arten benutzt werden. Angenommen, wir wollen das Bild von δ_v ermitteln und wir kennen bereits eine Untergruppe $U = \langle l_1, \dots, l_n \rangle \subseteq \text{Im } \delta_v$. Ist nun $P \in A(K_v)$ mit $\delta_v(P) = l \notin U$, dann gilt $\langle l, l_1, \dots, l_n \rangle \subseteq \text{Im } \delta_v$. Wir müssen also nicht für jedes Element des Bildes einen korrespondierenden Urbildpunkt konstruieren. Für $P \in A(K_v)$ mit $v(x(P)) < 0$ ist die

Bewertung der x -Koordinate von nP in etwa $nv(x(P))$. Wir kommen durch die Ausnutzung der Gruppenstruktur im Allgemeinen also mit einer höheren unteren Schranke für die Bewertung der x -Koordinate aus. Haben wir das Bild von δ_v bestimmt und wollen für Elemente testen, ob sie darin liegen, so hilft uns die Gruppenstruktur erneut. Angenommen, wir haben bereits gezeigt, dass für $\{r_1, \dots, r_M\}$ die Bedingung $\text{res}(r_i) \in \text{Im } \delta_v$ erfüllt ist, dann ist sie auch für alle Elemente in der von den r_i erzeugten Untergruppe erfüllt. Das ist besonders nützlich, wenn die zu testenden Elemente nicht als eine Liste, sondern über ein Erzeugendensystem gegeben sind. Das ist bei uns der Fall, da die unter Abschnitt 2.2 konstruierten endlichen Obermengen über Riemann-Roch-Räume oder Mengen der Form $K(S, 2^i)$ gegeben sind und wir für diese jeweils ein Erzeugendensystem berechnen können. Auch bei der Berechnung der Elemente, die orthogonal zum Bild einer Abstiegs-Abbildung sind, erweisen sich Erzeugendensysteme als hilfreich. Indem wir Erzeuger des lokalen Bilds in die Paarung einsetzen, können wir diese als Linearformen auffassen. Die Berechnung der orthogonalen Elemente reduziert sich, wenn sie über ein Erzeugendensystem gegeben sind, auf das Berechnen von Kernen von Matrizen.

2.3.2 Selmergruppen über die lokale Lösbarkeit von homogenen Räumen

Die zweite Methode funktioniert unabhängig davon, ob wir in der Lage sind, die lokalen Bilder der Abstiegs-Abbildung zu berechnen oder nicht. Sie verwendet die in Abschnitt 1.6.1 vorgestellte Theorie der homogenen Räume. Sei $\delta : A(K)/\psi(B(K)) \rightarrow R$ die ψ -Abstiegs-Abbildung und $r \in R$ gegeben. Dann liegt r im Bild von δ genau dann, wenn $C_r(K) \neq \emptyset$ gilt für C_r eine zu r korrespondierende Kurve vom Geschlecht eins über K . Notwendig für die Existenz eines K -rationalen Punktes auf C_r ist die Existenz von K_v -rationalen Punkten für alle Vervollständigungen K_v von K . Die lokalen Bedingungen an ein Element r sind nun, dass $C_r(K_v) \neq \emptyset$ für alle Bewertungen v gilt. Diese Bedingung ist für fast alle Stellen erfüllt. Das folgt aus der in Abschnitt 2.3.1 gegebenen Argumentation. Alternativ können wir auch benutzen, dass die Reduktion von C_r für fast alle v eine Kurve vom Geschlecht eins über dem Restklassenkörper ist, die nach dem Satz von Hasse Punkte besitzt, welche sich mit Hensels Lemma zu Punkten über K_v liften lassen. Wir müssen also auch mit dieser Methode lokale Bedingungen nur an endlich vielen Bewertungen v überprüfen und können die benötigten v , wie schon zuvor beschrieben, finden. Wie in Abschnitt 1.6 gezeigt, kann C_r entweder als Nullstellenmenge eines Polynoms der Form

$$q = y^2 + (ax^2 + bx + c)y + dx^4 + ex^3 + fx^2 + gx + h$$

oder zweier Polynome

$$q_1 = \sum_{1 \leq i < j \leq 4} a_{i,j} x_i x_j \quad \text{und} \quad q_2 = \sum_{1 \leq i < j \leq 4} b_{i,j} x_i x_j$$

beschrieben werden. Weitere Informationen dazu finden sich im Abschnitt 2.4.1. Ist C_r in ersterer Form, so liefert die Transformation $u := x^2$ und anschließendes Homogenisieren eine Beschreibung von C_r als Schnitt der Quadriken

$$\begin{aligned} q_1 &= y^2 + auy + bxy + cyv + du^2 + exu + fuv + gxv + hv^2 \\ q_2 &= x^2 + uv \end{aligned}$$

Wir geben daher nur an, wie diese Modelle auf lokale Lösbarkeit über K_v untersucht werden können.

Sei also K ein globaler Körper und $q = (q_1, q_2)$ das Modell einer Geschlecht-Eins-Kurve über K gegeben als der Schnitt zweier homogener Gleichungen q_1 und q_2 vom Grad 2 in vier Variablen. Wir schreiben

$$q_1 = \sum_{1 \leq i \leq j \leq 4} a_{i,j} x_i x_j$$

und q_2 analog mit Koeffizienten $b_{i,j}$. Sei v eine Bewertung von K mit lokaler Uniformisierender π und bezeichne K_v die Vervollständigung von K bezüglich v . Nach einer Skalierung können wir annehmen, dass die Koeffizienten $a_{i,j}$ und $b_{i,j}$ in R_v liegen. In [Sik95] gibt Siksek einen Algorithmus an, der entscheidet, ob q eine Lösung über K_v besitzt. Dabei setzt er voraus, dass die Charakteristik des Restklassenkörpers von K_v ungleich 2 ist. Doch auch ohne diese Voraussetzung arbeitet der Algorithmus korrekt. Der Beweis dafür unterscheidet sich nur in wenigen Details von dem in [Sik95] gegebenen. Grund für die Unterschiede ist, dass wir in Charakteristik 2 die quadratischen Formen q_1 und q_2 nicht mehr als $q_i = x^T M_i x$, mit $x^T = (x_1 \ x_2 \ x_3 \ x_4)$ und M_i eine symmetrische Matrix, schreiben können. Gelte im Folgenden $\text{char}(K_v) = 2$. Wir definieren Matrizen

$$A := \begin{pmatrix} 0 & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{1,2} & 0 & a_{2,3} & a_{2,4} \\ a_{1,3} & a_{2,3} & 0 & a_{3,4} \\ a_{1,4} & a_{2,4} & a_{3,4} & 0 \end{pmatrix}$$

und B analog. Grundidee für den Algorithmus ist eine Verallgemeinerung von Hensels Lemma.

Lemma 2.3.6. *Sei $X_0 \in R_v^4 \setminus \pi R_v^4$ mit*

$$q_1(X_0) \equiv q_2(X_0) \equiv 0 \pmod{\pi^{2\delta+1}}.$$

Existieren weiterhin keine Elemente λ und μ in R_v mit $\min\{v(\lambda), v(\mu)\} = 0$ und $\lambda A X_0 - \mu B X_0 \equiv 0 \pmod{\pi^{\delta+1}}$. Dann gibt es $X \in R_v^4$ mit $q_1(X) = q_2(X) = 0$ und $X \equiv X_0 \pmod{\pi^{\delta+1}}$.

Beweis. Wie bei [Sik95] folgt diese Aussage direkt aus Theorem 5.21 in [Gre69]. \square

Mit Hilfe dieser Aussage können wir entscheiden, ob es ein $X \in K_v^4$ gibt mit $q_1(X) = q_2(X) = 0$, indem wir solch ein X modulo geeigneter π -Potenzen approximieren. Letzteres ist ein endliches Problem und lässt sich im Zweifel über eine Brute-Force-Suche in exponentieller Zeit lösen. Eine ausführliche Beschreibung des Algorithmus findet sich in [Sik95, 5.2.1]. Die folgende Aussage dient als Abbruchkriterium.

Lemma 2.3.7. *Seien $X_0 \in R_v^4$ mit*

$$q_1(X_0) \equiv q_2(X_0) \equiv 0 \pmod{\pi^\alpha}$$

und $\lambda, \mu \in R_v$ mit $\min\{v(\lambda), v(\mu)\} = 0$ gegeben, so dass $\lambda A X_0 - \mu B X_0 \equiv 0 \pmod{\pi^\beta}$ gilt. Dann gilt

$$\min(\alpha, \beta) \leq v(\Delta(q)).$$

Beweis. Diese Aussage findet sich unter 5.2.1 in [Sik95] und der Beweis in Charakteristik 2 verläuft analog. Nur an einer Stelle gibt es einen kleinen Unterschied: Da wir nicht von dem dort in B.0.1 definierten „Combinant“ Gebrauch machen können, definieren wir die Diskriminante $\Delta(q)$ eines solchen Modells wie in [Fis08]. Siehe auch Abschnitt 2.4.1.4. Der Rest des Beweises aus [Sik95] kann direkt übernommen werden. Mit Hilfe von Magma berechnen wir unter Verwendung der Voraussetzungen, dass die Ungleichung $v(\Delta(q')) \geq \kappa$ mit $\kappa = \min(\alpha, \beta)$ auf für die allgemeiner definierte Diskriminante gilt. \square

Der obige Algorithmus approximiert eine Lösung, aber eigentlich genügt es uns, ein Entscheidungsproblem zu lösen. In [MSS96] findet sich ein Algorithmus, der genau das in polynomieller Zeit macht. Doch selbst wenn sich dieser auch auf Charakteristik 2 übertragen ließe, verbliebe hier das Problem, dass die exponentiell vielen Elemente aus R_0 untersucht werden müssen.

In der Praxis ist diese Methode deutlich langsamer als die unter Abschnitt 2.3.1 beschriebene. Zwar können wir auch hier von der Gruppenstruktur Gebrauch machen, um die Anzahl der tatsächlich zu überprüfenden Kurven zu reduzieren. Dennoch ist es im Allgemeinen effizienter, erstere Methode zu verwenden, wann immer das möglich ist. Zusammengefasst bekommen wir die folgende Aussage:

Lemma 2.3.8. *Wir können ein Erzeugendensystem der F^i - und V^i -Selmergruppen aus Schritt 2 mit Laufzeit exponentiell in der Höhe der Koeffizienten berechnen. Die Länge des Erzeugendensystems ist polynomiell.*

2.4 Globales Bild

In diesem Schritt wird überprüft, welche Elemente r der ψ -Selmergruppe wirklich im Bild von δ liegen. Wie in Abschnitt 1.6 beschrieben, korrespondiert das zu der Frage, welcher überall lokal lösbare homogene Raum einen K -rationalen Punkt besitzt. Das Geschlecht dieser homogenen Räume ist eins. Es ist hinlänglich bekannt, dass das Lokal-Global-Prinzip nicht für Geschlecht-Eins-Kurven gilt, siehe [Sik95, 4.8] oder Absatz 4.1 für ein Beispiel in Charakteristik 2. Somit kann das Bild von δ eine echte Teilmenge der ψ -Selmergruppe sein.

In Abschnitt 1.6 geben wir an, wie in den verschiedenen Situationen definierende Gleichungen für die prinzipal-homogenen Räume konstruiert werden können. Für ein Element r der ψ -Selmergruppe und $\delta : A(K)/\psi(B(K)) \rightarrow R$ ergeben sich diese aus der Weierstraß-Gleichung $A(x, y) = 0$ und der Gleichung $\delta(x, y) = r$. Die so konstruierten Kurven lassen sich auf bestimmte Normalformen bringen.

In diesem Abschnitt verzichten wir auf eine genaue Analyse der Laufzeiten. Grund dafür ist, dass kein Algorithmus bekannt ist, der die zentrale Aufgabe – das Entscheiden, ob eine überall lokal lösbare Geschlecht-Eins-Kurve einen globalen Punkt besitzt oder nicht – für alle Instanzen lösen kann. Wir beschränken uns darauf, anzugeben, welche Schritte in der Praxis mehr oder weniger Probleme bereiten.

2.4.1 Modelle für Kurven vom Geschlecht eins

In diesem Abschnitt fassen wir kurz einige Resultate über Modelle für Kurven vom Geschlecht eins zusammen. Die wichtigsten Quellen sind [Fis08] und [CFS10]. Wir

beschränken uns dabei auf eine Auswahl an für unsere Zwecke relevante Aussagen und Modelle. Für umfangreichere Informationen sei auf obige Arbeiten verwiesen.

Sei C eine glatte Kurve vom Geschlecht eins definiert über dem Körper K und sei D ein K -rationaler Divisor vom Grad n auf C . Für $n \geq 3$ bezeichnen wir das durch das vollständige lineare System $|D|$ definierte Modell in \mathbb{P}^{n-1} als Geschlecht-Eins-Modell vom Grad n . Für $n = 1$ besitzt C einen K -rationalen Punkt, also auch eine Weierstraß-Gleichung, für $n = 2$ liefert $|D|$ eine zweifache Überlagerung von \mathbb{P}^1 . Diese bezeichnen wir als Geschlecht-Eins-Modell vom Grad eins bzw. zwei. Für manche Aufgaben arbeiten wir mit einem geeigneten affinen Teil. Diesen bezeichnen wir dann ebenfalls als Geschlecht-Eins-Modell vom Grad n . Folglich ist diese Definition konsistent mit der in Abschnitt 1.6.1 gegebenen für eine Geschlecht-Eins-Kurve vom Grad n .

2.4.1.1 $n = 1$

Der Fall $n = 1$ ist klassisch und wird schon bei [Sil86] behandelt. Sind $1, x$ und $1, x, y$ Basen der Riemann-Roch-Räume $\mathcal{L}(2D)$ und $\mathcal{L}(3D)$, so genügen die Elemente $1, x, x^2, x^3, y, xy, y^2 \in \mathcal{L}(6D)$ einer linearen Relation und diese liefert uns nach einer geeigneten Skalierung eine Weierstraß-Gleichung der Kurve. Wir nennen zwei solche Modelle K -äquivalent, wenn sie über die Substitution

$$x = u^2 x' + r, \quad y = u^3 y' + u^2 s x' + t$$

mit $u, r, s, t \in K$, $u \neq 0$ zusammenhängen. Sind dabei $r, s, t \in \mathcal{O}_K$ und $u \in \mathcal{O}_K^\times$, so sprechen wir von \mathcal{O}_K -Äquivalenz. Für die durch $[u, r, s, t]$ wie oben gegebene Transformation wird die Determinante als $\det([u, r, s, t]) := u^{-1}$ definiert.

2.4.1.2 $n = 2$

Ähnlich wie für $n = 2$ besitzen die Riemann-Roch-Räume $\mathcal{L}(D)$ und $\mathcal{L}(2D)$ Basen $1, x$ und $1, x, y, x^2$. Die Elemente $1, x, x^2, x^3, x^4, y, xy, x^2 y, y^2$ liegen in dem 8-dimensionalen Riemann-Roch-Raum $\mathcal{L}(4D)$. Sie genügen also einer linearen Relation. Bei dieser ist der Koeffizient von y^2 ungleich null, da sich sonst y als Quotient zweier Polynome in x schreiben ließe und das führt zu einem Widerspruch. Somit bekommen wir eine Gleichung der Form

$$y^2 + (ax^2 + bx + c)y + dx^4 + ex^3 + fx^2 + gx + h = y^2 + p(x)y + q(x) = 0.$$

Homogenisieren der Polynome $p(x)$ und $q(x)$ zu $P(x, z)$ und $Q(x, z)$ liefert ein Modell der Kurve in einem gewichteten projektiven Raum. Wir nennen zwei Modelle K -äquivalent, wenn sie sich durch eine Transformation der Form

$$\begin{aligned} (x', z') &= (x, z)B \\ y' &= \mu^{-1}y + r_0x^2 + r_1xz + r_2z^2 \end{aligned}$$

mit $B \in \mathrm{GL}(2, K)$, $\mu, r_0, r_1, r_2 \in K$, $\mu \neq 0$ ineinander überführen lassen. Für solch eine Transformation ist die Determinante als $\det([\mu, r_0, r_1, r_2, B]) := \mu \det B$ definiert. Wir sprechen von \mathcal{O}_K -Äquivalenz, wenn $B \in \mathrm{GL}(2, \mathcal{O}_K)$, $r_0, r_1, r_2 \in \mathcal{O}_K$, $\mu \in \mathcal{O}_K^\times$ gilt.

2.4.1.3 $n = 4$

Ist D ein K -rationaler Divisor vom Grad 4 auf C , so besitzt $\mathcal{L}(D)$ eine Basis der Form x_1, \dots, x_4 . Die 10 Elemente $x_i x_j$ für $1 \leq i < j \leq 4$ liegen in dem 8-dimensionalen Riemann-Roch-Raum $\mathcal{L}(2D)$, daher erfüllen sie zwei unabhängige lineare Relationen. Diese liefern uns Gleichungen der Form

$$\begin{aligned} q_1(x_1, x_2, x_3, x_4) &= \sum_{1 \leq i < j \leq 4} a_{i,j} x_i x_j = 0 \\ q_2(x_1, x_2, x_3, x_4) &= \sum_{1 \leq i < j \leq 4} b_{i,j} x_i x_j = 0 \end{aligned}$$

Der Schnitt der durch diese Gleichungen definierten Quadriken liefert uns ein Modell unserer Kurve im \mathbb{P}^3 . Wir nennen zwei Modelle $(q_1(x_1, \dots, x_4), q_2(x_1, \dots, x_4))$ und $(q'_1(x'_1, \dots, x'_4), q'_2(x'_1, \dots, x'_4))$ K -äquivalent, wenn sie sich um eine Transformation der Form

$$\begin{aligned} (q'_1, q'_2) &= (q_1, q_2)A \\ (x'_1, \dots, x'_4) &= (x_1, \dots, x_4)B \end{aligned}$$

mit $A \in \mathrm{GL}(2, K)$ und $B \in \mathrm{GL}(4, K)$ unterscheiden. Sind A und B invertierbare Matrizen über \mathcal{O}_K , so bezeichnen wir die Modelle als \mathcal{O}_K -äquivalent. Die Determinante der durch A und B gegebenen Transformation ist als $\det([A, B]) := \det A \det B$ definiert.

2.4.1.4 Invarianten und Transformationen

Eine Invariante vom Gewicht k eines Geschlecht-Eins-Modells ist ein polynomieller Ausdruck F in den Koeffizienten, der in Bezug auf die oben genannten Transformationen g der Gleichung $F \circ g = \det(g)^k F$ genügt. Analog zur Diskriminante für die Weierstraß-Gleichung einer elliptischen Kurve werden in [CFS10] Diskriminanten auch für Geschlecht-Eins-Modelle vom Grad 2 und 4 definiert. Dort wird gezeigt, dass diese Diskriminanten Δ für $n = 1, 2$ und 4 je eine Invariante vom Gewicht 12 sind. Sie ist als explizit gegebener polynomieller Ausdruck in den Koeffizienten für ein konkretes Modell einfach zu berechnen. Wie bei Weierstraß-Gleichungen elliptischer Kurven ist die Diskriminante von null verschieden, genau wenn die Kurve glatt ist. Vergleiche [Fis08, Seite 3]. Wir interessieren uns besonders für Modelle, die Twists elliptischer Kurven beschreiben. Deren Diskriminante ist ungleich null, vergleiche Theorem 1.1 in [CFS10].

Wollen wir nun zeigen, dass ein Element r der V^i - oder F^i -Selmergruppe im Bild der Abstiegs-Abbildung liegt, so müssen wir beweisen, dass eine korrespondierende Geschlecht-Eins-Kurve C_r mit einem Divisor vom Grad 2 oder 4 einen K -rationalen Punkt besitzt. Dazu könnten wir ein Modell für C_r wählen und einen Punkt darauf angeben. Dabei besitzen Modelle mit kleinen Koeffizienten mit höherer Wahrscheinlichkeit einen Punkt mit kleinen Koordinaten als Modelle mit großen. Klein bedeutet für ein Element a des Funktionenkörpers K , dass der Grad des Poldivisors $(a)_\infty$, also die naive Höhe von a , klein ist. Wir sind daher an einem Modell für C_r mit möglichst kleinen Koeffizienten interessiert. Um ein solches zu finden, starten wir mit einem beliebigen Modell und wenden die jeweiligen Transformationen an, um ein äquivalentes

mit kleineren Koeffizienten zu konstruieren. Dabei gehen wir in zwei Schritten vor. Im ersten – genannt Minimierung – bestimmen wir ein K -äquivalentes Modell mit kleinerer Diskriminante. Im zweiten Schritt – genannt Reduktion – wenden wir dann Transformationen an, die die Diskriminante invariant lassen, um ein Modell mit kleineren Koeffizienten zu bestimmen. Beide Schritte sind notwendig. Ist die Diskriminante groß, so können die Koeffizienten auch nicht sehr klein werden. Transformationen, die die Diskriminante reduzieren, können in diesem Zuge sehr große Koeffizienten produzieren, was eine anschließende Reduktion notwendig macht. Wir bezeichnen ein Modell als ganz, wenn die Koeffizienten in \mathcal{O}_K liegen. Offensichtlich besitzt jede Geschlecht-Eins-Kurve ein ganzes Modell. Solch eines sei unser Ausgangspunkt für die Minimierung und Reduktion. Um die Analogie zu den Zahlkörpern zu wahren, beschäftigen wir uns erst einmal nur mit solchen Transformationen, die unser Modell wieder in ein ganzes überführen.

2.4.2 Minimierung

In [CFS10] wird ein Algorithmus angegeben, der Geschlecht-Eins-Modelle vom Grad 2 und 4 über einem lokalen Körper K_v beliebiger Charakteristik minimiert. Dabei wird ein Modell mit Koeffizienten in R_v in ein anderes solches transformiert. Für das transformierte Modell ist die Bewertung der Diskriminante minimal unter allen K_v -äquivalenten Modellen mit Koeffizienten in R_v . Dieser Algorithmus ist eine Verallgemeinerung von Tates Algorithmus zur Berechnung lokaler minimaler Weierstraß-Gleichungen elliptischer Kurven. Durch die sukzessive Minimierung bezüglich aller Stellen, an denen die Bewertung der Diskriminante größer gleich 12 ist, bekommen wir einen Minimierungsalgorithmus für globale Funktionenkörper. Ist dabei die Klassengruppe von \mathcal{O}_K trivial, dann berechnen wir auf diese Weise ein global minimales, ganzes Modell. Ist die Klassengruppe nicht trivial, so müssen wir entweder endlich viele weitere Pole zulassen und bekommen nur ein S -ganzes Modell oder wir geben uns mit einem Modell zufrieden, das zwar ganz ist, dessen Diskriminante aber nicht bezüglich aller Bewertungen minimal sein muss. Da der Minimierungsalgorithmus in [CFS10] detailliert und in der benötigten Allgemeinheit beschrieben ist, verzichten wir an dieser Stelle auf eine ausführliche Beschreibung. Um zu entscheiden, bezüglich welcher Stellen minimiert werden muss, ist es notwendig, den Nullstellendivisor $(\Delta)_0$ der Diskriminante zu berechnen. Selbst wenn die Diskriminante unserer ursprünglichen elliptischen Kurve A klein ist, kann die eines homogenen Raums sehr groß werden. Daher kann diese Berechnung mitunter Schwierigkeiten bereiten. Die Anzahl der Reduktionsschritte des Algorithmus lässt sich durch den Grad von $(\Delta)_0$ beschränken. In jedem Schritt müssen die Koeffizienten in den Restklassenkörper abgebildet und nach einigen Rechnungen wieder nach \mathcal{O}_K geliftet werden. Es werden einfache Rechnungen in K und über dem Restklassenkörper durchgeführt. Für eine globale Minimierung ist es notwendig, geeignete lokale Uniformisierende mit dem starken Approximationssatz zu berechnen. Alle diese Operationen können durchgeführt werden und in der Praxis dauert dieser Schritt meist nicht sehr lang. Die Charakteristik hat hier kaum Einfluss auf die Laufzeit. Diese ist also in etwa dieselbe wie über einem Zahlkörper.

2.4.3 Reduktion

In [CFS10] geben Cremona, Fisher und Stoll einen Algorithmus zur Reduktion von Geschlecht-Eins-Modellen vom Grad n über \mathbb{Q} an. Dazu zeigen sie, dass die Koeffizien-

ten der Gleichung betragsmäßig klein werden, wenn ein bestimmtes Skalarprodukt $\phi_{\mathbb{C}}$ in \mathbb{C}^n „nah“ am Standardskalarprodukt ist. Anhand der Operation der Torsionspunkte auf den Punkten der Geschlecht-Eins-Kurve berechnen sie eine Gram-Matrix für $\phi_{\mathbb{C}}$ und reduzieren diese mit Hilfe von LLL. Diese Methode lässt sich nicht ohne weiteres auf Zahlkörper oder globale Funktionenkörper übertragen. Es treten verschiedene Probleme auf: Weder lassen sich die darstellenden Matrizen der Operation der Torsionspunkte ausreichend schnell berechnen, noch ist klar, welches damit zusammenhängende Objekt berechnet und reduziert werden muss, damit auch die Koeffizienten des Modells reduziert werden. Daher geben wir an dieser Stelle eine andere Methode an. Diese unterscheidet sich, je nach Grad des zu reduzierenden Modells und abhängig davon, ob K ein rationaler Funktionenkörper ist oder nicht. Wir beschränken uns auf Modelle vom Grad 2 oder 4 über globalen Funktionenkörpern der Charakteristik 2, auch wenn sich alles ohne Schwierigkeiten in beliebiger Charakteristik verwenden lässt.

2.4.3.1 $n = 2$

Beschreibe $q = y^2 + P(x, z)y + Q(x, z)$ ein Geschlecht-Eins-Modell vom Grad 2 über einem rationalen Funktionenkörper $k(t)$. Hierbei sei $k = \mathbb{F}_{2^m}$ ein endlicher Körper und $P(x, z) = ax^2 + bxz + cz^2$, $Q(x, z) = dx^4 + ex^3z + fx^2z^2 + gxz^3 + hz^4$ mit $a, \dots, h \in k[t]$. Wir wollen nun eine Transformation

$$(x, z) \mapsto (x, z)B, y \mapsto \mu^{-1}y + r_0x^2 + r_1xz + r_2z^2$$

bestimmen, so dass das transformierte Modell q' „schöner“ wird. Da wir q zuvor minimiert haben, verlangen wir, dass sich $\Delta(q)$ und $\Delta(q')$ nur um eine Einheit in $k[t]$ unterscheiden und dass die Koeffizienten von q' ebenfalls in $k[t]$ liegen. Die Modelle q und q' sollen daher $k[t]$ -äquivalent sein. In einem späteren Schritt wollen wir auf dem Modell q' nach $k(t)$ -rationalen Punkten suchen. Das geht einfacher, je kleiner die Koeffizienten sind. Der von uns verwendete Suchalgorithmus, siehe Abschnitt 2.4.5, behandelt alle Koeffizienten gleich, daher ist unser Ziel, das Maximum der Grade der Koeffizienten zu minimieren. Damit ist erklärt, wann ein Modell „schöner“ als ein anderes ist. Wir bezeichnen das Maximum der Grade der Koeffizienten eines Grad-2-Modells auch als seine *Höhe*. Der von uns vorgestellte Algorithmus ist ein Greedy-Algorithmus, der in drei Schritten vorgeht.

Im ersten Schritt reduzieren wir die Grade der Koeffizienten a, b und c von $P(x, z)$ mit einer unimodularen Transformation $(x, z) \mapsto (x, z)B$. Ausmultiplizieren zeigt, dass solche Transformationen den Koeffizienten b invariant lassen, wir dessen Grad also nicht reduzieren können. Verbleiben a und c . Da

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

unimodular ist, können wir davon ausgehen, dass $\deg a \geq \deg c$ gilt. Nun transformieren wir mit

$$B = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix},$$

wobei $\lambda = \lambda_0 t^\mu$ so gewählt ist, dass $\max\{\deg(b\lambda), \deg(c\lambda^2)\} = \deg(a)$ gilt und $\lambda_0 \in k$ eine Nullstelle der Gleichung der Leitkoeffizienten von $a + b\lambda + c\lambda^2$ ist. Existieren

solch ein μ oder λ_0 nicht, beenden wir diesen Schritt und gehen zum nächsten über, ansonsten iterieren wir dieses Vorgehen, solange es geht.

Im zweiten Schritt reduzieren wir die Grade der Koeffizienten d, \dots, h von $Q(x, z)$ durch geeignete Transformationen $y \mapsto y + r_0x^2 + r_1xz + r_2z^2$. Diese lassen a, b und c invariant. Wie im vorherigen Schritt bestimmen wir $r_0 = r_{0,0}t^{\mu_0}$, $r_1 = r_{1,0}t^{\mu_1}$ und $r_2 = r_{2,0}t^{\mu_2}$ mit $r_{i,0} \in k$ und $\mu_i \in \mathbb{N}$, so dass die Grade der transformierten Koeffizienten kleiner gleich den der ursprünglichen Koeffizienten sind und der maximale Grad sogar echt kleiner ist. Die $r_{i,0}$ bekommen wir, indem wir das Gleichungssystem der Leitkoeffizienten lösen. Es besteht aus fünf Gleichungen vom Grad kleiner gleich 2 in drei Variablen über k und meist sind einige der Gleichungen trivial. Diesen Schritt wiederholen wir, solange das Gleichungssystem der Leitkoeffizienten eine Lösung besitzt, und gehen dann zum dritten Schritt über.

Der dritte Schritt ist relevant, wenn nach dem zweiten das Maximum der Grade der Koeffizienten von $Q(x, z)$ größer ist als die Grade der Koeffizienten von $P(x, z)$. In diesem Fall schreiben wir die Einträge von B sowie die r_i als Polynome beschränkten Grades mit unbekanntem Koeffizienten. Die Bedingung $\deg \det B = 0$ zusammen mit der Bedingung, dass der maximale Grad der Koeffizienten durch die Transformation kleiner wird, liefern ein Gleichungssystem über k . Besitzt es keine Lösung, erhöhen wir die Grade der r_i und der Einträge von B . Diesen Schritt wiederholen wir, bis der maximale Grad der Koeffizienten von $Q(x, z)$ kleiner gleich einer vorgegebenen Schranke ist oder bis die auftretenden Gleichungssysteme zu schwierig werden.

Die ersten beiden Schritte des Algorithmus laufen sehr schnell, da die auftretenden Gleichungen einfach zu lösen sind. Doch der dritte Schritt ist kritisch. Für eine große Anzahl von Variablen sind selbst Systeme von Gleichungen kleinen Grades über endlichen Körpern nicht mehr lösbar. Das Lösen basiert auf der Berechnung von Gröbnerbasen und der Aufwand dafür wächst sehr stark. Je nach Situation müssen wir entscheiden, wieviel Zeit wir diesem Schritt geben wollen.

Der beschriebene Algorithmus arbeitet heuristisch. In Bezug auf seine Approximationsgüte lassen sich einige Aussagen treffen.

Lemma 2.4.1. *Sei $P(x, z) = ax^2 + bxz + cz^2$ mit $\deg a \geq \deg c$ gegeben und sei es nicht möglich, durch eine Transformation der Form $z \mapsto z + \lambda x$ den Grad des größten Koeffizienten zu reduzieren. Dann ist das auch mit beliebigen $\text{GL}(2, k[t])$ -Transformationen nicht möglich.*

Beweis. Für $\deg(b) \geq \deg(a)$ ist keine Reduktion möglich, da alle $\text{GL}(2, k[t])$ -Transformationen b invariant lassen. Somit gelte $\deg(a) > \deg(b)$. Wenn wir durch eine Transformation $z \mapsto z + \lambda x$ den Grad von a nicht reduzieren können, dann gibt es dafür zwei mögliche Gründe:

1. Es gilt $2(\deg(a) - \deg(b)) + \deg(c) > \deg(a)$ und $\deg(a) \not\equiv \deg(c) \pmod{2}$. Die erste Bedingung sagt dabei, dass für eine mögliche Reduktion $\deg(a) = \deg(c\lambda^2)$ gelten muss, die zweite, dass das nicht möglich ist.
2. Oder es gilt $2(\deg(a) - \deg(b)) + \deg(c) = \deg(a)$, aber die Gleichung der Leitkoeffizienten besitzt keine Lösung im k .

In den anderen Fällen können wir direkt eine Transformation angeben, die den Grad von a reduziert. Sei nun $B \in \text{GL}(2, k[t])$ beliebig. Dann wird a zu $\mu^2a + \mu\lambda b + \lambda^2c$. Für alle Polynome μ gilt dieselbe Aussage über die Grade und die Leitkoeffizienten wie oben, so dass keine Reduktion möglich ist. \square

Bemerkung 2.4.2. *Optimalität für die Grade der Koeffizienten von $P(x, z)$ lässt sich also einfach erreichen. Sind nach dem ersten Schritt die Grade aller Koeffizienten von Q kleiner gleich dem maximalen Grad der Koeffizienten von P , so ist durch die Schritte zwei und drei keine weitere Reduktion möglich. Wir können diese also weglassen. Das liefert uns ein vorzeitiges Abbruchkriterium, unter dem der Output unseres Algorithmus optimal ist. Des Weiteren liefert uns die Höhe der Koeffizienten von P nach dem ersten Schritt eine untere Schranke für die Höhe aller Koeffizienten $k[t]$ -äquivalenter Modelle.*

Da der dritte Schritt am aufwendigsten ist, können wir schon nach dem zweiten stoppen und uns mit der bis dahin berechneten Reduktion zufrieden geben. Oft ist das sinnvoll, für einige Beispiele liefert dieses Vorgehen aber ziemlich schlechte Ergebnisse.

Beispiel 1. *Sei $q = y^2 + (t^{10}x^2 + xz)y + t^{11}x^4 + t^9z^4$ über $\mathbb{F}_2(t)$. Im ersten Schritt reduzieren wir den Grad von a durch $z \mapsto z + t^{10}x$. Das liefert uns die Gleichung $y^2 + (xz)y = (t^{49} + t^{11})x^4 + t^9z^4$. Die Koeffizienten von $P(x, z)$ lassen sich nicht weiter reduzieren. Durch eine Transformation $y \mapsto y + r_0x^2 + r_1xz + r_2z^2$ lässt sich der Grad von d nicht reduzieren.*

Alternativ können wir uns auf $\text{GL}(2, k[t])$ -Transformationen beschränken und diese zur simultanen Reduktion der Koeffizienten von P und Q verwenden. Auch das liefert für bestimmte Beispiele schlechte Ergebnisse.

Beispiel 2. *Sei $q = y^2 + xzy + t^{2n}x^4 + t^n x^3z + tz^4$ über $\mathbb{F}_2(t)$ mit $n \in \mathbb{N}$. Durch eine $\text{GL}(2, k[t])$ -Transformation lässt sich der Grad von d nicht reduzieren. Das liegt daran, dass $\deg d \not\equiv \deg h \pmod{4}$ und aufgrund der Grade daher keine Reduktion möglich ist. Vergleiche dazu den Beweis von Lemma 2.4.1. Die Substitution $y \mapsto y + t^n x^2$ liefert die Gleichung $y^2 + xzy + tz^4$ und somit für ein großes n eine deutliche Verbesserung.*

Das Problem der Reduktion von Geschlecht-Eins-Modellen lässt sich auch über beliebigen globalen Funktionenkörpern K formulieren. Hier hat das Modell Koeffizienten in der endlichen Maximalordnung \mathcal{O}_K und wir suchen ein \mathcal{O}_K -äquivalentes Modell mit kleinen Koeffizienten. Die Rolle des Grads eines Polynoms nimmt der Grad des Poldivisors eines Elements in K ein. Der oben beschriebene Algorithmus lässt sich für diese Situation anpassen. In jedem Schritt suchen wir Transformationen, die den maximalen Pol der Koeffizienten reduzieren. Dabei machen wir von der in [Sch96] beschriebenen Gitterreduktion über globalen Funktionenkörpern Gebrauch. Wenn wir über rationalen Funktionenkörpern zur Reduktion ein λ der Form $\lambda_0 t^\mu$ bestimmen mussten, dann müssen wir über K ein λ der Form $\lambda_1 t^{\mu_1} b_1 + \dots + \lambda_n t^{\mu_n} b_n$ bestimmen. Hierbei ist $\{b_1, \dots, b_n\}$ eine reduzierte $k[t]$ -Basis von \mathcal{O}_K . Die $\lambda_i \in k$ bestimmen wir wieder als Lösungen eines Systems von Gleichungen kleinen Grads. Der Aufwand dafür wächst mit dem Grad $[K : k(t)]$. Die anderen Schritte lassen sich analog anpassen.

Der vorgestellte Algorithmus basiert darauf, die Pole der Koeffizienten schrittweise durch das Lösen von Gleichungssystemen über endlichen Körpern zu reduzieren. Dieses Vorgehen lässt sich nicht ohne Weiteres auf Zahlkörper übertragen. Daher ist es schwierig, ihn mit dem Algorithmus aus [CFS10] zu vergleichen. Ein Vorteil ist, dass auch von den Transformationen $y \mapsto y + r_0x^2 + r_1xz + r_2z^2$ Gebrauch gemacht wird, während sich der Algorithmus aus [CFS10] auf die von der GL_2 erzeugte Untergruppe der Transformationsgruppe beschränkt. Vergleiche dazu Beispiel 2. Des Weiteren arbeitet man bei der Reduktion über Zahlkörpern mit Matrizen mit Einträgen aus \mathbb{R}

und \mathbb{C} , was eine sorgfältige Analyse der benötigten Präzision notwendig macht. Dieses Problem haben wir mit unserem Ansatz nicht.

2.4.3.2 $n = 4$

Beschreibe der Schnitt der Quadriken

$$q_1 = \sum_{1 \leq i < j \leq 4} a_{i,j} x_i x_j, \quad q_2 = \sum_{1 \leq i < j \leq 4} b_{i,j} x_i x_j$$

mit $a_{i,j}, b_{i,j} \in k[t]$ das Modell einer Geschlecht-Eins-Kurve vom Grad 4. Ziel ist es, ein $k[t]$ -äquivalentes Modell zu finden, das das Maximum über die Grade der Koeffizienten minimiert. Wie zuvor bezeichnen wir das Maximum der Grade der Koeffizienten als die *Höhe* des Modells. In [CFS10] wird ein Reduktionsalgorithmus für Grad-4-Modelle über \mathbb{Q} vorgestellt. Dieser berechnet zuerst eine geeignete Transformationsmatrix $A \in \text{GL}(2, \mathbb{Z})$ und $(q'_1, q'_2) = (q_1, q_2)A$, ordnet dann (q'_1, q'_2) ein Skalarprodukt zu und reduziert die dazugehörige Gram-Matrix mit LLL. Wie schon für Modelle vom Grad 2 treten Schwierigkeiten auf, wenn wir dieses Vorgehen auf über globalen Funktionenkörpern definierte Schnitte von Quadriken übertragen wollen. Wir geben daher eine andere Methode an.

Wir gehen dabei ähnlich, wie bei den Grad-2-Modellen vor. Das heißt, wir machen Ansätze für Transformationsmatrizen, bei denen wir die Einträge als Polynome beschränkten Grads mit unbekanntem Koeffizienten auffassen. Formales Ausmultiplizieren liefert uns ein Gleichungssystem über dem endlichen Konstantenkörper, dessen Lösungen zu Transformation, die den maximalen Grad der Koeffizienten reduzieren, korrespondierenden. Bei den Transformationsmatrizen beschränken wir uns auf unimodulare obere Dreiecksmatrizen mit Einträgen beschränkten Grads. Der Grund dafür ist, dass auf diese Weise die resultierenden Gleichungssysteme relativ einfach zu lösen sind. Bei Experimenten mit allgemeineren unimodularen Transformationen sind wir schnell auf Gleichungssysteme gestoßen, für deren Lösung Magma sehr viel Zeit benötigt. Wann immer wir keine Transformation finden, die den maximalen Grad der Koeffizienten reduziert, führen wir eine zufällige Transformation durch, die den Maximalgrad invariant lässt und beginnen unsere Suche von Neuem. Auf diese Weise sollen allgemeinere Transformationen modelliert werden.

Diese Heuristik ist für kleine Konstantenkörper in der Praxis ziemlich schnell. Vergleiche Abschnitt 4.3. Es ist einfach, Modelle zu konstruieren, bei denen sich der Maximalgrad nicht durch obere Dreiecksmatrizen reduzieren lässt, nach einer Permutation aber eine Reduktion möglich ist. Zum Beispiel besitzt

$$\begin{aligned} t^{d_1} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= 0 \\ t^{d_2} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= 0 \end{aligned}$$

für $d_2 > d_1 \gg 1$ diese Eigenschaft. Offensichtlich lässt sich weder durch eine Addition eines $k[t]$ -Vielfachen der zweiten Gleichung zur ersten noch durch eine Substitution $x_i \mapsto x_i + \sum_{j>i} \lambda_j x_j$ der Maximalgrad d_2 reduzieren. Die Addition des $t^{d_2-d_1}$ -fachen der ersten Gleichung zur zweiten liefert aber eine unimodulare Transformation, die den Maximalgrad reduziert. Die zufälligen Permutationen sind also notwendig. Darüber hinaus zeigen Beispiele aus der Praxis, dass es von Vorteil ist, sich nicht auf zufällige

Permutationen zu beschränken, sondern zufällige Transformationen, die Höhe nicht erhöhen, zuzulassen.

Die Vor- und Nachteile dieser Methode im Vergleich zu der in [CFS10] für Zahlkörper entsprechen denen im Fall $n = 2$. Auch die Übertragung auf beliebige globale Funktionenkörper läuft so, wie es dort beschrieben ist.

2.4.4 Wahl der Maximalordnung

Bei der Reduktion und Minimierung einer Geschlecht-Eins-Kurve haben wir versucht, ein Modell mit möglichst kleinen Koeffizienten in \mathcal{O}_K zu finden. Dabei sind wir analog zum Zahlkörperfall vorgegangen. Im Gegensatz zu Zahlkörpern hängt für einen globalen Funktionenkörper K die endliche Maximalordnung \mathcal{O}_K von der Darstellung von K ab. Durch einen geeigneten Wechsel des separierenden Elements von K können wir eine beliebige endliche Menge von Stellen zu den „unendlichen Stellen“ machen. Dadurch ist mitunter eine bessere Reduktion und Minimierung möglich.

Beispiel 3. Sei $K = \mathbb{F}_2(t)$ und C das durch $y^2 + txy + x^3 + t^5(t+1)$ gegebene Modell einer Geschlecht-Eins-Kurve vom Grad eins. Die Diskriminante dieses Modells ist $t^{11}(t+1)$, es gibt also kein äquivalentes Modell mit Koeffizienten in $\mathbb{F}_2[t]$ und einer Diskriminante kleineren Grads. Die Transformation $(x, y) \mapsto (t^2x, t^3y)$ liefert die neue Gleichung $y^2 + xy + x^3 + (t+1)/t$. Für $u := (t+1)/t$ ist $\mathbb{F}_2(t)$ isomorph zu dem rationalen Funktionenkörper $\mathbb{F}_2(u)$. Die Gleichung besitzt Koeffizienten in $\mathbb{F}_2[u]$ und ihre Diskriminante ist gleich u , also von kleinerem Grad.

Wir wissen, dass die Diskriminante Δ eine Invariante vom Gewicht 12 ist. Es bietet sich also an, zu untersuchen, ob es ein Element $u \in K$ gibt, mit $\deg(u^{12}\Delta) < \deg(\Delta)$. Angenommen solch ein u existiert. Nach einer Transformation mit der Determinante u bekommen wir eine endliche Menge an Stellen S bestehend aus den Polen der Koeffizienten des transformierten Modells. Wählen wir ein geeignetes separierendes Element, so können wir die Reduktion wie zuvor beschrieben durchführen.

2.4.5 Berechnung rationaler Punkte beschränkter Höhe auf Geschlecht-Eins-Kurven

Wie bereits erwähnt liegt ein Element r der ψ -Selmergruppe im Bild der Abstiegs-Abbildung $\delta : A(K)/\psi(B(K)) \rightarrow R$ genau wenn eine bestimmte Geschlecht-Eins-Kurve C_r einen K -rationalen Punkt P besitzt. Aus diesem Punkt P lässt sich dann einfach der Repräsentant eines Urbilds von r auf $A(K)$ berechnen. Für die in dieser Arbeit betrachteten Isogenien besitzen die Kurven C_r spezielle Modelle, die wir als Geschlecht-Eins-Modelle vom Grad 2 und 4 bezeichnet haben. Da wir – wie zuvor beschrieben – jedes Grad-2-Modell in eines vom Grad 4 transformieren können, ist unser Problem darauf reduziert, einen K -rationalen Punkt auf dem Schnitt zweier Quadriken (q_1, q_2) zu bestimmen. Diese Aufgabe wird als sehr schwierig angesehen. Zur Lösung wird für Punkte $X = (x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3(K)$ getestet, ob sie auf beiden Quadriken liegen, das heißt, ob $q_1(X) = q_2(X) = 0$ gilt. Da die Quadriken aufgrund vorheriger Minimierung und Reduktion kleine Koeffizienten besitzen, besteht die Hoffnung, dass, falls solch ein Punkt existiert, auch einer mit kleiner Höhe existiert. Unsere Suche beginnt also mit solchen X und falls wir dabei nicht fündig werden, gehen wir zu Punkten mit größerer Höhe über. Um die Suche effizient zu gestalten, machen wir von einem Siebalgorithmus Gebrauch, der auf Elkies zurück geht –

siehe [Elk00] – und schon in [Wom03] für $K = \mathbb{Q}$ und in [Rob07] für einen rationalen Funktionenkörper K beschrieben ist. Dieser Algorithmus lässt sich auf Geschlecht-Eins-Modelle vom Grad 4 über beliebigen globalen Funktionenkörpern übertragen. Wir geben an dieser Stelle nur eine kurze Zusammenfassung des Vorgehens an. Für umfangreichere Informationen sei auf die oben zitierten Arbeiten verwiesen. Die Idee hinter dem Siebalgorithmus ist, dass für $X \in \mathbb{P}^3(K)$ mit $q_1(X) = q_2(X) = 0$ auch $v_P(q_1(X)) = v_P(q_2(X)) = \infty$ gilt, wobei v_P die zu einer Stelle $P \in \mathbb{P}_K$ gehörige Bewertung ist. Statt also beliebige $X \in \mathbb{P}^3(K)$ durchzuprobieren, beschränken wir uns auf Teilmengen, deren Vereinigung alle Punkte mit $v_P(q_1(X)), v_P(q_2(X)) \geq d$ für ein bestimmtes festes $d \in \mathbb{N}$ enthält. Die Konstruktion dieser Teilmengen geschieht in mehreren Schritten. Bezeichne k_P den endlichen Restklassenkörper von P und (\bar{q}_1, \bar{q}_2) die reduzierten Quadriken über k_P . Nach Konstruktion haben q_1 und q_2 Koeffizienten in \mathcal{O}_K . Die Stelle P sei eine endliche, an der das Geschlecht-Eins-Modell (q_1, q_2) gute Reduktion hat. Als erstes berechnen wir die Menge aller $X_0 \in \mathbb{P}^3(k_P)$ mit $\bar{q}_1(X_0) = \bar{q}_2(X_0) = 0$. Das ist ein endliches Problem. Unter Verwendung der Resultante können wir es durch die Faktorisierung von $O(\#k_P)$ vielen Polynomen vom Grad kleiner gleich 4 über k_P lösen. Nun berechnen wir für jedes X_0 ein Gitter $L_{X_0}^1 \subseteq \mathcal{O}_K^4$, das von alle Lifts von X_0 aufgespannt wird. Unter Berechnung der Taylor-Entwicklung erster Ordnung von (q_1, q_2) berechnen wir ein echtes Untergitter von $L_{X_0}^1$, in dem für jeden Gitterpunkt y gilt $v_P(q_1(y)) \geq 2, v_P(q_2(y)) \geq 2$ und in dem jeder Vektor $y \in \mathcal{O}_K^4$ mit $v_P(q_1(y)) \geq 2, v_P(q_2(y)) \geq 2$ und y kongruent zu einem Vielfachen von X_0 modulo P enthalten ist. Durch Taylor-Entwicklungen höherer Ordnung können weitere Untergitter konstruiert werden, so dass $v_P(q_1(y)) \geq d, v_P(q_2(y)) \geq d$ gilt. Das \mathcal{O}_K -Untergitter, wieder mit L_{X_0} bezeichnet, das wir am Ende erhalten, ist über eine Basis $\{b_1, \dots, b_4\}$ gegeben. Wir wollen nun für alle Gitterpunkte y beschränkter Höhe testen, ob $q_1(y) = q_2(y) = 0$ erfüllt ist. Sei also eine Schranke für die Höhe gegeben. Wir wollen alle Gitterpunkte unterhalb dieser Schranke erzeugen. Ist $K = k(t)$ ein rationaler Funktionenkörper über dem endlichen Konstantenkörper k , dann ist \mathcal{O}_K gleich dem Polynomring $k[t]$. Wir können mit der in [Rob07, Kapitel 7] beschriebenen Methode die Basismatrix in „weak Popov Form“ überführen. Sei die resultierende Basis mit $\{b'_1, \dots, b'_4\}$ bezeichnet. Dann bekommen wir Schranken d_1, \dots, d_4 , so dass alle gesuchten Gitterpunkte in der Menge $\{\lambda_1 b'_1 + \dots + \lambda_4 b'_4 \mid \lambda_i \in k[t], \deg \lambda_i \leq d_i\}$ liegen, also leicht zu erzeugen sind. Dieses Vorgehen lässt sich auf beliebige globale Funktionenkörper K übertragen. Sei dazu $K = k(t, u)$ eine Erweiterung des rationalen Funktionenkörpers $k(t)$ vom Grad n . Dann ist \mathcal{O}_K ein freier $k[t]$ -Modul vom Rang n . Bezeichne eine $k[t]$ -Basis von \mathcal{O}_K mit $\{u_1, \dots, u_n\}$ und eine \mathcal{O}_K -Basis von L_{X_0} mit $\{b_1, \dots, b_4\}$. Dann ist $\{u_i b_j\}$ eine $k[t]$ -Basis des Gitters. Mit dem in [Sch96] beschriebenen Algorithmus können wir daraus eine reduzierte Gitterbasis $\{b'_1, \dots, b'_{4n}\}$ berechnen. Da die Laufzeit der Gitterreduktion über globalen Funktionenkörpern polynomiell vom Rang des Gitters abhängt, ist dieses Vorgehen unproblematisch. Der Reduktionsalgorithmus arbeitet mit Laurentreihenentwicklungen von Elementen aus K , daher müssen wir uns ein paar Gedanken über die benötigte Präzision machen, aber auch das bereitet keine Schwierigkeiten. Aus den Höhen der reduzierten Basisvektoren bekommen wir Schranken für die Grade der Koeffizienten einer $k[t]$ -Linearkombination eines Punktes, dessen Höhe unter unserer vorgegebenen Schranke liegt. In [Rob07] werden verschiedene Methoden angegeben, wie das Durchprobieren der Gitterpunkte effizient gestaltet werden kann. Grob gesprochen sind das die folgenden: Bezeichne b'_1, \dots, b'_{4n} eine reduzierte $k[t]$ -Basis und $\hat{b}_1, \dots, \hat{b}_4$ eine reduzierte \mathcal{O}_K -Basis des Gitters. Entweder wir iterieren über alle Koeffizienten λ_i in $k[t]$ mit

Grad kleiner gleich d_i und testen ob $q_1(\sum_{i=1}^{4n} \lambda_i b'_i) = q_2(\sum_{i=1}^{4n} \lambda_i b'_i) = 0$ gilt. Oder wir schreiben einen Punkt $X = \sum_{i=1}^4 \lambda_i \hat{b}_i$ mit λ_i eine Unbekannte in \mathcal{O}_K . Diesen generischen Punkt setzen wir dann in q_1 und q_2 ein, um neue Quadriken in den Variablen λ_i zu bekommen. Darauf suchen wir dann nach Punkten, zum Beispiel, indem wir über alle Werte für ein oder zwei der λ_i iterieren und die resultierenden Gleichungen mit Hilfe von Resultanten oder Techniken für Kegelschnitte untersuchen. Als dritte Möglichkeit können wir auch einen Punkt X als $X = \sum_{i=1}^{4n} \lambda_i b'_i$ schreiben, wobei die $\lambda_i = \sum_{j=0}^{d_i} \lambda_{i,j} t^j$ Polynome mit unbekanntem Koeffizienten sind. Diesen Punkt setzen wir dann in q_1 und q_2 ein und bekommen ein System von Gleichungen in den $\lambda_{i,j}$, das wir versuchen zu lösen. Am leichtesten lassen sich die erste und die dritte Methode vergleichen. Bei beiden versuchen wir dasselbe Gleichungssystem in den $\lambda_{i,j}$ zu lösen, bei der ersten durch vollständige Enumeration, bei der dritten über Gröbnerbasen. Im Allgemeinen wird daher die dritte Methode deutlich schneller sein, dafür kommt die erste mit konstant viel Speicher aus, wohingegen der Speicheraufwand zur Berechnung von Gröbnerbasen stark mit der Anzahl der Variablen wächst. Außerdem lässt sich die erste Methode leicht parallelisieren. Wobei das nur bedingt relevant ist, da die beschriebenen Methoden beide eine große Anzahl an Gittern untersuchen müssen und das für beide einfaches Parallelisieren ermöglicht. Für einen Vergleich anhand einiger Beispiele siehe Abschnitt 4.5. Es verbleibt die Frage, wie die Stelle P zu wählen ist. Wie schon bei [Rob07] beschrieben, wächst mit steigendem Grad von P nach Hasse auch die Anzahl der Punkte auf dem Schnitt der reduzierten Quadriken und damit die Anzahl der zu untersuchenden Gitter. Da eine Kurve vom Geschlecht eins über einem Körper mit q Elementen $O(q)$ viele rationale Punkte besitzt, ist dieses Wachstum exponentiell in $\deg P$. Andererseits wächst die Diskriminante der Gitter mit dem Grad der Stelle P und somit sinkt die Anzahl der Gitterpunkte mit beschränkter Höhe. Unter Abschnitt 4.5 wird die Wahl der Stelle anhand einiger Beispiele untersucht.

2.5 Kombinieren von Abstiegs-Abbildungen

2.5.1 V - und V^2 -Abstieg

Seien $\psi_1 : B \rightarrow A$ und $\psi_2 : C \rightarrow B$ Isogenien der elliptischen Kurven A, B und C über dem Körper K . In Absatz 1.4.1 haben wir die exakte Sequenz

$$0 \rightarrow A(K)/\psi_1(B(K)) \rightarrow \text{Sel}(K, \psi_1) \rightarrow \text{III}(K, B)[\psi_1] \rightarrow 0$$

angegeben. Bezeichnen wir die Komposition $\psi_1 \circ \psi_2$ mit $\psi : C \rightarrow A$, so erhalten wir folgendes kommutatives Diagramm:

$$\begin{array}{ccccccc} A(K)/\psi(C(K)) & \longrightarrow & \text{Sel}(K, \psi) & \longrightarrow & \text{III}(K, C)[\psi] & \longrightarrow & 0 \\ \downarrow \text{id} & & \downarrow \psi_2 & & \downarrow \psi_2 & & \\ A(K)/\psi_1(B(K)) & \longrightarrow & \text{Sel}(K, \psi_1) & \longrightarrow & \text{III}(K, B)[\psi_1] & \longrightarrow & 0 \end{array}$$

Die vertikalen Abbildungen sind dabei durch die Identität auf $A(K)$ und durch ψ_2 auf den Kohomologiegruppen induziert. Ein Beweis für die Kommutativität für $\psi_1 = [m]$ und $\psi = [m^n]$ findet sich in [Sil86, X.4]. Der allgemeine Fall lässt sich durch eine einfache Rechnung mit Čech-Kozykeln verifizieren. Damit ist auch die Sequenz

$$0 \rightarrow A(K)/\psi_1(B(K)) \rightarrow \psi_2(\text{Sel}(K, \psi)) \rightarrow \psi_2(\text{III}(K, C)[\psi]) \rightarrow 0$$

exakt, vergleiche [Sil86, X.4.12]. Können wir also das Bild von $\text{Sel}(K, \psi)$ unter der von ψ_2 induzierten Abbildung berechnen, so liefert uns das eine Approximation für das Bild von $A(K)/\psi_1(B(K))$, die mitunter genauer ist als die ψ_1 -Selmergruppe.

Seien A eine gewöhnliche elliptische Kurve über einem globalen Körper K der Charakteristik 2 und ψ_1 und ψ_2 die Verschiebung $V : A^{(2)} \rightarrow A$ und $V : A^{(4)} \rightarrow A^{(2)}$. Gelte weiterhin $\#A^{(4)}[V^2](K) = 4$. In dieser Situation können wir

$$V : \text{Sel}(K, \ker V^2) \rightarrow \text{Sel}(K, \ker V)$$

explizit beschreiben. Diese Abbildung ist die Einschränkung von

$$V : H^1(G_K, \ker V^2) \rightarrow H^1(G_K, \ker V), (\sigma \mapsto T_\sigma) \mapsto (\sigma \mapsto V(T_\sigma))$$

auf die Selmergruppen. Wie schon in Abschnitt 1.3.2 beschrieben gilt

$$\ker V^2 \simeq W_2(\mathbb{F}_2) \text{ und } \ker V \simeq W_1(\mathbb{F}_2) = \mathbb{F}_2.$$

Für

$$f : W_2(\mathbb{F}_2) \rightarrow \mathbb{F}_2, (v_0, v_1) \mapsto v_0$$

kommutiert das Diagramm

$$\begin{array}{ccc} \ker V^2 & \xrightarrow{V} & \ker V \\ \downarrow \simeq & & \downarrow \simeq \\ W_2(\mathbb{F}_2) & \xrightarrow{f} & \mathbb{F}_2 \end{array}$$

Betrachten wir das dazugehörige Diagramm der ersten Kohomologiegruppen, so sehen wir, dass die Abbildung

$$H^1(G_K, W_2(\mathbb{F}_2)) \rightarrow H^1(G_K, \mathbb{F}_2)$$

durch

$$(\sigma \mapsto (v_{\sigma,0}, v_{\sigma,1})) \mapsto (\sigma \mapsto v_{\sigma,0})$$

gegeben ist. In dem kommutativen Diagramm

$$\begin{array}{ccc} H^1(G_K, \ker V^2) & \xrightarrow{V} & H^1(G_K, \ker V) \\ \downarrow \simeq & & \downarrow \simeq \\ W_2(K)/\wp(W_2(K)) & \longrightarrow & K/\wp(K) \end{array}$$

ist somit die untere horizontale Abbildung durch $(v_0, v_1) \mapsto v_0$ gegeben.

Angenommen unsere Aufgabe ist die Berechnung der Kardinalität und der Erzeuger von $A(K)/V(A^{(2)}(K))$. Dazu wollen wir für ein Element $r \in \text{Sel}(K, V) \subseteq K/\wp(K)$ untersuchen, ob es im Bild der V -Abstiegs-Abbildung liegt. Nach Abschnitt 1.6 müssen wir dazu einen K -rationalen Punkt auf einer Geschlecht-Eins-Kurve C_r finden. Falls unsere Suche erfolglos bleibt, können wir die V^2 -Selmergruppe berechnen. Da die Abstiegs-Abbildungen durch

$$\begin{aligned} \alpha_1 : A(K)/V(A^{(2)}(K)) &\rightarrow W_1(K)/\wp(W_1(K)) \\ (x, y) &\mapsto \frac{a_6}{a_1^2 x^2} \end{aligned}$$

$$\alpha_2 : A(K)/V^2(A^{(4)}(K)) \rightarrow W_2(K)/\wp(W_2(K)),$$

$$(x, y) \mapsto \left(\frac{a_6}{a_1^2 x^2}, \frac{a_6 y}{a_1^3 x^3} + \frac{a_6}{a_1^4 x} + \frac{sa_6 + a_6}{a_1^2 x^2} + \frac{a_6^2}{a_1^4 x^4} \right)$$

gegeben sind, sehen wir direkt, dass $r \in K$ der Repräsentant eines Elements aus dem Bild von $V : \text{Sel}(K, V^2) \rightarrow \text{Sel}(K, V)$ ist, genau wenn es ein Element in $\text{Sel}(K, V^2)$ gibt mit Repräsentanten $(r, r') \in W_2(K)$, r' beliebig. Gibt es keinen solchen Wittvektor, dann wissen wir, dass C_r keinen K -rationalen Punkt besitzt. Ist (r, r') ein Urbild von r unter V und $P \in A(K)$ mit $\alpha_2(P) = (r, r')$, dann gilt $\alpha_1(P) = r$. Da es auf dem zu (r, r') korrespondierenden homogenen Raum $C_{(r, r')}$ im Allgemeinen K -rationale Punkte kleinerer Höhe als auf C_r gibt, bietet es sich manchmal an, auf diese Weise Erzeuger von $A(K)/V(A^{(2)}(K))$ zu bestimmen. Ein analoges Vorgehen ist möglich, wenn $A^{(4)}(K)$ keine volle V^2 -Torsion besitzt.

2.5.2 F - und F^2 -Abstieg

Seien die Isogenien $\psi_1 : B \rightarrow A$, $\psi_2 : C \rightarrow B$ und $\psi : C \rightarrow A$ wie zuvor und bezeichnen ψ_1^\vee , ψ_2^\vee und ψ^\vee die dualen Isogenien. Angenommen, wir sind daran interessiert, eine Mordell-Weil-Basis für $A(K)$ zu berechnen, indem wir Erzeuger für $A(K)/[\text{deg } \psi_1]A(K)$ ermitteln. Wir haben bereits einen ψ_1 -Abstieg durchgeführt und auf diese Weise Erzeuger für $A(K)/\psi_1(B(K))$ berechnet. Nun sind wir an Erzeugern für $B(K)/\psi_1^\vee(A(K))$ interessiert, da uns deren Bilder unter ψ_1 ein Erzeugendensystem für $\psi_1(B(K))/[\text{deg } \psi_1]A(K)$ liefern. Die Menge $[\text{deg } \psi_1]A(K)$ zerfällt modulo $[\text{deg } \psi]A(K)$ in $\text{deg } \psi_2$ viele disjunkte Klassen. Anders ausgedrückt: Jede Klasse in $A(K)/[\text{deg } \psi_1]$ besitzt $\text{deg } \psi_2$ viele Urbilder unter der kanonischen Abbildung

$$\pi_{\psi_1} : A(K)/[\text{deg } \psi]A(K) \rightarrow A(K)/[\text{deg } \psi_1]A(K).$$

Ist ein $b \in \text{Sel}(K, \psi_1^\vee)$ gegeben und sei $P \in B(K)$ der Repräsentant eines Urbilds von b unter der ψ_1^\vee -Abstiegs-Abbildung, dann definiert $\psi_1(P)$ eine eindeutige Klasse modulo $[\text{deg } \psi_1]A(K)$. Anstatt direkt nach P zu suchen, können wir auch ermitteln, in welche Klassen $\psi_1(P) + [\text{deg } \psi_1]A(K)$ modulo $[\text{deg } \psi]A(K)$ zerfällt, also welche Urbilder $\psi_1(P)$ unter π_{ψ_1} besitzt, und versuchen, ein $Q \in C(K)$ zu bestimmen, für das $\psi(Q)$ in einer dieser Klassen enthalten ist. Der Vorteil liegt darin, dass es auf diese Weise mitunter möglich ist, das Problem auf das Finden von Punkten kleinerer Höhe zu reduzieren. Angewendet auf obige Situation bekommen wir $\psi_1^\vee = F$ und $\psi^\vee = F^2$. Seien nun Elemente $b_1 \in K^\times/(K^\times)^4$ und $b \in K^\times/(K^\times)^2$ gegeben mit $b_1 = \beta_2(Q)$ und $b = \beta_1(P)$ für $Q \in A^{(4)}(K)$ und $P \in A^{(2)}(K)$. Im Folgenden identifizieren wir die Klassen modulo $(K^\times)^4$ und modulo $(K^\times)^2$ jeweils mit einem Repräsentanten in K und schreiben für beides nur b_1 bzw. b .

Lemma 2.5.1. *Die Punkte $V(Q)$ und P liegen in derselben Klasse modulo $F(A(K))$, genau wenn $b_1 \equiv b \pmod{(K^\times)^2}$ gilt.*

Beweis. Angenommen $V(Q) \equiv P \pmod{F(A(K))}$ und sei $Q = (x, y) \in A^{(4)}(K)$. Dann gilt $\beta_1(P) = \beta_1(V(Q)) = \frac{x^2 + a_1^4 a_6^2}{a_1^4 x}$. Weiterhin gilt $\beta_2(Q) = y + 1/a_1^4 x^2 + a_1^4 s^4 x$ und da $a_1^4 x(y + 1/a_1^4 x^2 + a_1^4 s^4 x) = y^2 + a_1^8 s^8 x^2 + a_6^4$ und $x^2 + a_1^4 a_6^2$ beides Quadrate in K sind, gilt die Behauptung. Gelte nun $b_1 \equiv b \pmod{(K^\times)^2}$ und $b_1 = \beta_2(Q)$, $b = \beta_1(P)$. Dann haben $V(Q)$ und P dasselbe Bild unter β_1 , liegen also in derselben Klasse. \square

Bemerkung 2.5.2. Eine äquivalente Formulierung der Aussage des Lemmas ist, dass das Diagramm

$$\begin{array}{ccc} A^{(4)}(K)/F^2(A(K)) & \xrightarrow{\beta_2} & K^\times/(K^\times)^4 \\ \downarrow V & & \downarrow \pi_K \\ A^{(2)}(K)/F(A(K)) & \xrightarrow{\beta_1} & K^\times/(K^\times)^2 \end{array}$$

kommutiert. Hierbei ist π_K durch

$$\pi_K : K^\times/(K^\times)^4 \rightarrow K^\times/(K^\times)^2, a(K^\times)^4 \mapsto a(K^\times)^2$$

gegeben.

Ist nun ein $b \in \text{Sel}(K, F) \subseteq K^\times/(K^\times)^2$ gegeben und wir können keinen K -rationalen Punkt auf dem korrespondierenden homogenen Raum C_b bestimmen. Dann können wir $\text{Sel}(K, F^2) \subseteq K^\times/(K^\times)^4$ berechnen. Mit Hilfe von Polynomfaktorisierung lässt sich entscheiden, welche Repräsentanten der Klassen aus $\text{Sel}(K, F^2)$ sich nur um ein Quadrat von einem Repräsentanten für b unterscheiden. Ist C_{b_1} der homogene Raum solch eines Elements b_1 und $R \in C_{b_1}(K)$. Dann liefert uns R einen Punkt Q auf $A^{(4)}(K)$ und $V(Q) \in A^{(2)}(K)$ ist der Repräsentant eines Urbilds von b unter β_1 . Wir bekommen auf diese Weise sogar ein notwendiges Kriterium dafür, dass ein b aus $K^\times/(K^\times)^2$ im Bild von β_1 liegt:

Lemma 2.5.3. Sei $b \in K^\times/(K^\times)^2$. Angenommen b liegt im Bild von β_1 . Dann gibt es ein Element $\hat{b}_1 \in \text{Sel}(K, F^2)$ mit \hat{b}_1 ist ein Quadrat in K^\times also $\hat{b}_1 = b_1^2$ und $b_1 b$ ist ebenfalls ein Quadrat in K^\times .

Beweis. Sei $P = (x_0, y_0)$ ein Punkt auf $A^{(2)}(K)$ mit $\beta_1(P) = x_0 = b$. Dann ist das Bild $F(P) = (x_0^2, y_0^2)$ von P unter F ein Punkt auf $A^{(4)}(K)$ und es gilt

$$\begin{aligned} \beta_2(F(P)) &= y_0^2 + \frac{1}{a_1^4} x_0^4 + a_1^4 s^4 x_0^2 \\ &= \left(y_0 + \frac{1}{a_1^2} x_0^2 + a_1^2 s^2 x_0 \right)^2 \end{aligned}$$

Unter Verwendung der Weierstraß-Gleichung für $A^{(2)}$ sehen wir direkt, dass das Element $\hat{b}_1 := (y_0 + 1/a_1^2 x_0^2 + a_1^2 s^2 x_0)^2$ sowohl im Bild von β_2 liegt, als auch ein Quadrat ist, dessen Wurzel sich nur um ein Quadrat von b unterscheidet. \square

Bemerkung 2.5.4. Diese Aussage lässt sich auch durch die Untersuchung des obigen Diagramms beweisen.

2.6 Implementation

Zum gegenwärtigen Zeitpunkt existieren nur sehr wenige Implementierungen von Algorithmen zur Berechnung von Mordell-Weil-Basen für elliptische Kurven über globalen Funktionenkörpern. Zum einen sind die Algorithmen aus [Rob07], die eine maximale Menge unabhängiger Punkte für Kurven über rationalen Funktionenkörpern mit voller 2-Torsion und Charakteristik größer gleich 5, und zum anderen ist die Idee

aus [Kra77] zur Berechnung der V - und F -Selmergruppe für gewöhnliche elliptische Kurven über rationalen Funktionenkörpern der Charakteristik 2 in Magma [BCP97] implementiert. Des Weiteren verfügt Magma über einen Algorithmus, der auf anderem Wege – siehe auch Abschnitt 5.1 – in sehr speziellen Situationen Aussagen über den Rang und über unabhängige Punkte trifft. Implementationen für diese Aufgaben existieren unseres Wissens nach in keinem anderen Computeralgebrasystem.

Im Zuge dieser Arbeit wurde ein Großteil der vorgestellten Algorithmen in Magma implementiert. In Charakteristik größer gleich 5 wurden die Algorithmen von Roberts von uns auf beliebige globale Funktionenkörper und unabhängig von den Torsionspunkten erweitert. Für Charakteristik 2 haben wir uns auf rationale Funktionenkörper beschränkt. Wir haben eine eigene Implementation der Berechnung der V - und F -Selmergruppen gewöhnlicher elliptischer Kurven – siehe Absatz 4.7 für einen Vergleich der Geschwindigkeiten – sowie eine Implementation zur Berechnung der V^2 - und F^2 -Selmergruppe und der V - und F -Selmergruppe supersingulärer elliptischer Kurven angefertigt. Des Weiteren wurden Algorithmen zur Berechnung von Modellen für die homogenen Räume und für die Minimierung und Reduktion dieser sowie für die Suche nach Punkten auf ihnen von uns implementiert. Darüber hinaus wurde ein Algorithmus von Siksek für den unendlichen Abstieg – siehe Abschnitt 3.1 – von uns auf Funktionenkörper verallgemeinert.

Kapitel 3

Höhen und Anwendungen

Dieses Kapitel unterteilt sich grob in zwei Hälften. In der ersten schätzen wir in Lemma 3.1.1 die Differenz der naiven und der kanonischen Höhe in Charakteristik p ab und wenden das auf den unendlichen Abstieg an. In der zweiten ermitteln wir explizite Schranken für die Höhe S -ganzer Punkte in Charakteristik 2. Das resultiert in den Aussagen 3.2.3 und 3.2.4. Des Weiteren stellen wir verschiedene Methoden zur Berechnung aller S -ganzen Punkte vor.

Bei der Definition der *Höhe* halten wir uns an [Sil86, VIII.6, VIII.9] und [Sil94, III.4]. So ist die Höhe $h(a)$ für ein Element a eines (globalen) Funktionenkörpers definiert als der Grad der Funktion a , also als der Grad des Poldivisors von a . Die naive Höhe $h(P)$ eines Punktes P auf einer elliptischen Kurve A ist definiert als die Höhe seiner x -Koordinate und die kanonische Höhe $\hat{h}(P)$ ist über den Grenzwert

$$\hat{h}(P) := \lim_{N \rightarrow \infty} N^{-2} h([N]P)$$

definiert.

3.1 Unendlicher Abstieg

Eine maximale unabhängige Menge $\{P_1, \dots, P_r\}$ von K -rationalen Punkten auf A stellt ein Erzeugendensystem einer Untergruppe des freien Anteils von $A(K)$ dar. Diese Untergruppe hat endlichen Index, da sie eine maximale unabhängige Menge von Punkten enthält. Um solch ein Erzeugendensystem zu einer Mordell-Weil-Basis zu erweitern, können wir so, wie bei Siksek [Sik95] beschrieben, vorgehen. Die dort beschriebene Methode basiert darauf, den Index der von den gegebenen Punkten erzeugten Untergruppe nach oben abzuschätzen. Das liefert eine endliche Menge positiver S -ganzer Zahlen n , für die getestet werden muss, ob es Koeffizienten $\lambda_1, \dots, \lambda_r$ und $Q \in A(K)$ gibt, mit $\lambda_1 P_1 + \dots + \lambda_r P_r = nQ$ und nicht alle λ_i durch n teilbar. Ist das der Fall, so wird die Untergruppe entsprechend vergrößert. Siksek stellt den Algorithmus in seiner Arbeit für elliptische Kurven über Zahlkörpern vor. Aber er lässt sich ohne große Schwierigkeiten auch in Charakteristik p anwenden. Die Idee ähnelt der zur Berechnung der Einheitengruppe für einen Zahlkörper wie zum Beispiel in [PZ97] und [vS91] beschrieben. Wir fassen den freien Anteil von $A(K)$ zusammen mit der kanonischen Höhe als ein Gitter auf und benutzen Methoden aus der Geometrie der Zahlen. Eine untere Schranke für die Höhe eines Punktes unendlicher Ordnung in

$A(K)$ liefert uns eine Abschätzung für den Regulator. Nun berechnen wir den Regulator des von P_1, \dots, P_r erzeugten Untergitters und bekommen so eine obere Schranke für den Index. Diese Methode funktioniert unabhängig von der Charakteristik von K . Alles was wir benötigen ist eine Abschätzung der Differenz der kanonischen und der naiven Höhe. In [Sil90] zeigt Silverman, wie solch eine Abschätzung über Zahlkörpern berechnet werden kann. Dazu zerlegt er die kanonische Höhe in die Summe der lokalen Höhen und schätzt für diese jeweils die Differenz ab (siehe dazu [Lan78, III.4, III.5]). Dasselbe Vorgehen ist auch über globalen Funktionenkörpern möglich:

Lemma 3.1.1. *Sei A eine elliptische Kurve über einem globalen Funktionenkörper K gegeben durch eine Weierstraß-Gleichung, deren Koeffizienten S -ganz sind. Sei Δ die Diskriminante und j die j -Invariante von A . Dann gilt für alle $P = (x, y) \in A(K)$ die Ungleichung*

$$-\frac{1}{12}h(j) - C_1 \leq \hat{h}(P) - h(P) \leq \frac{1}{6}h(\Delta) + C_2.$$

Hierbei sind C_1 und C_2 Konstanten, die von den Polen der Koeffizienten der Weierstraß-Gleichung abhängen und explizit berechnet werden können.

Beweis. Wir gehen wie bei [Sil90] beschrieben vor.

$$\begin{aligned} \hat{h}(P) - h(P) &= 2 \sum_v \lambda_v(P) - \sum_v \log^+ |x|_v \\ &\geq 2 \sum_{v \notin S} -\frac{1}{24} \log^+ |j|_v + \sum_{v \in S} 2\lambda'_v(c_v^{-2}x, c_v^{-3}y) - \log^+ |x|_v \\ &\geq 2 \sum_{v \notin S} -\frac{1}{24} \log^+ |j|_v + \sum_{v \in S} 2\lambda'_v(c_v^{-2}x, c_v^{-3}y) - \log^+ |c_v^{-2}x|_v - 2v(c_v) \\ &= -\frac{1}{12}h(j) - \sum_{v \in S} 2v(c_v) \end{aligned}$$

Dabei nutzen wir die Eindeutigkeit lokaler Höhen aus. Aufgrund dieser gilt für einen Isomorphismus $f : A \rightarrow A'$ von elliptischen Kurven die Gleichheit $\lambda_v = \lambda'_v \circ f$ für passende lokale Höhen auf A bzw. A' . Weiterhin wird verwendet, dass isomorphe Kurven dieselbe j -Invariante haben und dass $v(c_v) \geq 0$ gilt. Das Element c_v ist durch den Isomorphismus, der A auf ein v -ganzes Modell abbildet, gegeben. Für die andere Ungleichung gilt

$$\begin{aligned} \hat{h}(P) - h(P) &= 2 \sum_v \lambda_v(P) - \sum_v \log^+ |x|_v \\ &\leq 2 \sum_{v \notin S} \frac{1}{12} \log^+ |\Delta|_v + \sum_{v \in S} 2\lambda'_v(c_v^{-2}x, c_v^{-3}y) - \log^+ |x|_v \\ &\leq 2 \sum_{v \notin S} \frac{1}{12} \log^+ |\Delta|_v + \sum_{v \in S} 2\lambda'_v(c_v^{-2}x, c_v^{-3}y) - \log^+ |c_v^{-2}x|_v + 2v(c_v) \\ &\leq \frac{1}{6}h(\Delta) + \sum_{v \in S} 4v(c_v) \end{aligned}$$

Hier benutzen wir wieder den Isomorphismus von oben und beachten, wie er die Diskriminante transformiert. \square

In seiner Arbeit stellt Siksek eine weitere Abschätzung der Differenz der kanonischen und der naiven Höhe vor. Diese basiert nicht auf einer Zerlegung in lokale Höhen, sondern darauf, die Differenz zwischen $h(2P)$ und $4h(P)$ durch explizite Rechnungen abzuschätzen. Diese Methode funktioniert mit minimalen Modifikationen auch in Charakteristik p . Unterschiede entstehen dadurch, dass wir in Charakteristik 2 nicht mehr mit einer kurzen Weierstraß-Gleichung arbeiten können. Dadurch bekommen wir andere Gleichungen, die wir mit Hensel auf lokale Lösbarkeit über der Vervollständigung untersuchen müssen. Statt zu untersuchen, wann ein Element ein Quadrat ist (Gleichung von der Form $y^2 = f(x)$) untersuchen wir nun, wann eine Gleichung der Form $y^2 + y = f(x)$ lösbar ist. Das bereitet unter Verwendung von Abschnitt 2.3.1.1 keine großen Schwierigkeiten.

Mit Hilfe der Abschätzung für die Differenz der Höhen ist es einfach, den Algorithmus von Siksek auf globale Funktionenkörper zu übertragen. Damit sind wir in der Lage, eine maximale Menge unabhängiger Punkte zu einer Mordell-Weil-Basis zu erweitern. In meinem Programm verwende ich eine modifizierte Version von Steve Donnellys Implementation von Sikseks Algorithmus zur Erweiterungen von Mordell-Weil-Basen über Zahlkörpern. Wie auch bei der Einheitengruppenberechnung – siehe [vS91] – wird dabei die Suche nach Koeffizienten λ_i mit $\lambda_1 P_1 + \dots + \lambda_r P_r = nQ$ durch die Reduktion modulo verschiedener Stellen und die Verwendung von linearer Algebra deutlich beschleunigt. Vergleiche [Sik95, 2.3.1].

3.2 Ganze Punkte

Sei $A : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ eine elliptische Kurve über einem Zahlkörper K und seien die Koeffizienten a_i aus der Maximalordnung \mathcal{O}_K . Dann nennen wir einen Punkt $P = (x, y) \in A(K)$ ganz, wenn x und damit auch y in \mathcal{O}_K liegen. Nach Siegel wissen wir, dass es in dieser Situation nur endlich viele ganze Punkte gibt, siehe zum Beispiel [Sil86, IX.3.2.1]. Es können sogar explizite Schranken für ihre Höhe angegeben werden. Das Konzept der ganzen Punkte lässt sich auch auf elliptische Kurven über einem globalen Funktionenkörper K übertragen. Hier fixieren wir eine Weierstraß-Gleichung und eine endliche Menge von Stellen S , verlangen, dass die Koeffizienten der Weierstraß-Gleichung nur Pole an diesen Stellen haben, und nennen einen Punkt $P = (x, y) \in A(K)$ S -ganz, wenn x und damit auch y keine Pole außerhalb von S besitzt. Im Folgenden bezeichnet – wenn nichts anderes gesagt wird – die Höhe eines Punkts auf einer elliptischen Kurve immer seine naive Höhe, also die Höhe seiner x -Koordinate.

3.2.1 Höhenschranken für S -ganze Punkte

Elliptische Kurven über globalen Funktionenkörpern können unendlich viele S -ganze Punkte besitzen, allerdings nur, wenn ihre j -Invariante algebraisch über dem Konstantenkörper ist. Falls die j -Invariante transzendent und die Charakteristik von K größer als 3 ist, können wir dieselben Techniken wie über Zahlkörpern verwenden, um zu zeigen, dass es nur endlich viele S -ganze Punkte gibt und um eine Schranke für ihre Höhe anzugeben. Wir wollen nun die Situation in Charakteristik 2 betrachten.

3.2.1.1 Gewöhnliche elliptische Kurven

In [Vol90] beweist Voloch die Endlichkeit der Anzahl der S -ganzen Punkte für nicht isotriviale gewöhnliche elliptische Kurven mit einer anderen Methode. Im Folgenden werden wir diese Methode verwenden, um Höhenschranken für eben solche elliptische Kurven in Charakteristik 2 zu berechnen. Sei also $A : y^2 + a_1xy = x^3 + a_2x^2 + a_6$ eine feste Weierstraß-Gleichung einer elliptischen Kurve über einem globalen Funktionenkörper K der Charakteristik 2. In [Kra77, Lemma 1.2] wird gezeigt, dass es sich bei der Abbildung

$$\gamma : A(K) \rightarrow H, (x, y) \mapsto \left(x, \frac{a_6}{a_1^2 x^2} \right)$$

für H einen Quotienten von $K^\times \times a_6 K^2$ um einen Gruppenhomomorphismus mit $\ker \gamma = 2A(K)$ handelt. Voloch zeigt in [Vol90, Bemerkung 3.3], dass die Abbildung

$$f : H \rightarrow K, (u, v) \mapsto v + \wp \left(\frac{a_6 \delta u}{u} \right)$$

mit $\delta = \frac{d}{da_6}$ für a_6 kein Quadrat ein Isomorphismus ist und Hintereinanderausführung liefert

$$\mu : A(K) \rightarrow K, (x, y) \mapsto \frac{a_6}{a_1^2 x^2} + \wp \left(\frac{a_6 \delta x}{x} \right)$$

Um mit μ zu arbeiten, nehmen wir erst einmal an, dass a_6 kein Quadrat ist und zeigen später wie das Argument sonst modifiziert werden muss. Wir gehen hier analog zu Voloch vor, mit dem Unterschied, dass wir explizite Schranken berechnen.

Lemma 3.2.1. *Sei $(x, y) \in A(K)$ ein S -ganzer Punkt, $v \in S$ und $n \in \mathbb{N}$ ausreichend groß. Dann gilt für $v(x) \leq -n$ auch $v(\mu(x, y)) \geq n/2 - C$ wobei C eine explizit berechenbare Konstante ist, die nur von den Koeffizienten der Weierstraß-Gleichung abhängt.*

Bemerkung 3.2.2. *Das bedeutet, dass die Abbildung μ stetig in der v -adischen Topologie ist. Für $v(x) \rightarrow -\infty$ also für $P \rightarrow \mathcal{O}$ geht das Bild unter μ gegen null.*

Beweis. Wir verwenden die Bezeichnungen $v(x) =: -n$, $v(y) =: -m$, $v(a_i) =: -d_i$ und verlangen, dass $3n > \max\{d_1 + m + n, d_2 + 2n, d_6\}$ gilt. Das ist für ausreichend großes n der Fall. Dann gilt $2m = 3n$. Das bedeutet y^2 und x^3 haben dieselbe v -Bewertung und alle anderen Summanden haben eine größere. Daraus folgt $m = \frac{3}{2}n$ und $n > d := \max\{2d_1, d_2, \frac{d_6}{3}\}$. Nun schreiben wir $n = d + c$, $m = \frac{3}{2}(d + c)$. Dann gilt $v(x^3) = v(y^2) = 3d + 3c$ und das Minimum der Bewertungen der anderen Summanden ist größer gleich dem Maximum von $\frac{d}{2} + d + c + \frac{3}{2}(d + c) = 3d + \frac{5}{2}c$ und $d + 2(d + c) = 3d + 2c$ und $3d$ also $3d + \frac{5}{2}c$. Als Reihen in einer lokalen Uniformisierenden π beginnen also x^3 und y^2 bei $\pi^{-(3d+3c)}$ und die anderen erst $\frac{1}{2}c$ viele Koeffizienten später. Da die Charakteristik 2 ist, hat y^2 nur Koeffizienten an den geraden π -Potenzen. Da (x, y) die Weierstraß-Gleichung erfüllen, müssen bei x^3 auch von den ersten $\frac{1}{2}c$ Koeffizienten die an den ungeraden π -Potenzen null sein. Folglich können wir $c = 2c_1$ schreiben. Bezeichnen wir mit x' die Ableitung von x nach π und für a_6 analog. Dann gilt $v(x'/x) \geq c_1 - 1$ und mit $c_2 := v(a_6/a_6')$ gilt $v((a_6 x')/(a_6' x)) \geq c_1 + c_2 - 1$. Die Bewertung der anderen Summanden ist größer, also liefert uns das die gewünschte Abschätzung für die Summe. \square

Kennen wir eine maximale Menge unabhängiger Elemente von $A(K)/2A(K)$, zum Beispiel eine Mordell-Weil-Basis, dann können wir das endliche Bild von μ berechnen und bekommen Schranken für die v -Bewertung der Elemente des Bildes. Mit obigem Lemma liefert uns das eine untere Schranke für das Minimum

$$\min\{v(x) \mid (x, y) \text{ ist } S\text{-ganzer Punkt in } A(K) \setminus 2A(K)\}.$$

Kombinieren wir diese Schranken für alle Stellen aus S , so bekommen wir eine Schranke für die Höhe eines S -ganzen Punkts. Kennen wir nicht genügend unabhängige Punkte, so liefern die folgenden Lemmata Aussagen über das Bild von μ .

Lemma 3.2.3. *Sei $v \notin S$ eine Bewertung, für die A gute Reduktion besitzt. Gelte außerdem $v(\mathrm{d}a_6/\mathrm{d}\pi) = 0$ für π eine lokale Uniformisierende von v . Dann gilt $v(\mu(P)) \geq 0$ für alle $P = (x, y) \in A(K)$.*

Beweis. Da A nach Voraussetzung gute Reduktion an v besitzt, gilt für die Bewertung der Diskriminante $v(\Delta(A)) = v(a_1^6 a_6) = 0$. Folglich gilt $v(a_1) = v(a_6) = 0$, da v nicht in S liegt.

1. Fall: $v(x) = 0$

Dann haben wir $v(\frac{a_6}{a_1^2 x^2}) = 0$. Nach Voraussetzung gilt $v(a_6) - v(\frac{\mathrm{d}a_6}{\mathrm{d}\pi}) = 0$. Weiterhin gilt $v(\frac{\mathrm{d}x}{\mathrm{d}\pi}) - v(x) \geq 0$. Also gilt $v(\mu(P)) \geq 0$ wie behauptet.

2. Fall: $v(x) < 0$

Dann gilt $v(\frac{a_6}{a_1^2 x^2}) \geq 0$. Weiterhin gilt $v(\frac{x}{y}) > 0$. Daher ist auch die v -Bewertung des Elements $x(\frac{x}{y})^2 = 1 + a_1 \frac{x}{y} + a_2 (\frac{x}{y})^2 + a_6 (\frac{1}{y})^2$ größer gleich null. Unter Verwendung der Ableitungsregeln sehen wir, dass $v(\frac{\mathrm{d}x}{\mathrm{d}\pi}) - v(x) = v(\frac{\mathrm{d}xz^2}{\mathrm{d}\pi}) - v(xz^2)$ für $z \in K^\times$ gilt. Wählen wir $z = \frac{x}{y}$, so folgt $v(\frac{\mathrm{d}x}{x \mathrm{d}\pi}) \geq 0$ mit obiger Rechnung.

3. Fall: $v(x) > 0$

Wir schreiben die Elemente jeweils als Reihen in π . Als erstes erkennen wir, dass aus $v(a_6) = 0$ und $v(\frac{\mathrm{d}a_6}{\mathrm{d}\pi}) = 0$ auch $a_6 = a_{6,0} + a_{6,1}\pi + \dots$ mit $a_{6,0} \neq 0$ und $a_{6,1} \neq 0$ folgt. Sei nun $v(x) \geq 1$. Dann ist x von der Form $x = x_1\pi + \dots$ und $y = y_0 + y_1\pi + \dots$. Da x und y der Weierstraß-Gleichung genügen, gilt $y_0^2 + a_{1,0}x_1y_0\pi + a_{6,0} + a_{6,1}\pi = 0$. Daher gilt $x_1 \neq 0$, also $v(x) = 1$ und $x_1^2 = a_{6,1}^2 / (a_{6,0}a_{1,0}^2)$. Nun berechnen wir

$$\frac{a_6}{(a_1 x)^2} = \frac{a_{6,0}}{a_{1,0}^2 x_1^2} \pi^{-2} + \frac{a_{6,1}}{a_{1,0}^2 x_1^2} \pi^{-1} + O(\pi^0)$$

und

$$\wp\left(\frac{a_6 \mathrm{d}x}{\mathrm{d}\pi} / \frac{\mathrm{d}a_6 x}{\mathrm{d}\pi}\right) = \frac{a_{6,0}^2}{a_{6,1}} \pi^{-2} + \frac{a_{6,0}}{a_{6,1}} \pi^{-1} + O(\pi^0).$$

Ein Vergleich der Koeffizienten liefert $v(\mu(x, y)) \geq 0$. □

Lemma 3.2.4. *Sei v eine Stelle, die nicht die Voraussetzungen des vorherigen Lemmas erfüllt, d.h. $v \in S$ oder A hat keine gute Reduktion an v oder $v(\mathrm{d}a_6/\mathrm{d}\pi) \neq 0$. Dann ist $v(\mu(P))$ nach unten beschränkt, präziser $v(\mu(P)) \geq b_v$.*

Beweis. Wir unterscheiden wieder dieselben Fälle.

1. Fall: $v(x) = 0$

Dann gilt $v(\frac{a_6}{a_1^2 x^2}) = v(a_6) - 2v(a_1)$ und $v(\frac{\mathrm{d}x}{x \mathrm{d}\pi}) \geq 0$. Insgesamt gilt für die Bewertung von $\mu(x, y)$ also $v(\mu(x, y)) \geq \min\{0, v(a_6) - 2v(a_1), 2v(\frac{a_6 \mathrm{d}\pi}{\mathrm{d}a_6})\}$.

2. Fall: $v(x) < 0$

Dann gilt $v(\frac{a_6}{a_1^2 x^2}) \geq v(a_6) - 2v(a_1)$ und wegen $v(\frac{dx}{d\pi}) \geq v(x) - 1$ gilt $v(\frac{dx}{x d\pi}) \geq -1$.

Wir bekommen $v(\mu(x, y)) \geq \min\{0, v(a_6) - 2v(a_1), 2v(\frac{a_6 d\pi}{da_6}) - 2\}$

3. Fall: $v(x) > 0$

Hier verwenden wir, dass a_6 kein Quadrat ist, d.h. $v(\frac{da_6}{d\pi}) = m < \infty$ und dann auch $v(y^2 + a_6) < m + 1$. Aufgrund der Weierstraß-Gleichung ist dann $v(x)$ nach oben beschränkt. Die Schranke lässt sich einfach berechnen und hängt von den Bewertungen der a_i ab. Somit haben wir eine untere Schranke für $v(\frac{a_6}{a_1^2 x^2})$. Es gilt $v(\frac{dx}{x d\pi}) \geq -1$. Insgesamt haben wir $v(\mu(x, y)) \geq b_v$ mit b_v abhängig von $v(a_1), v(a_2), v(a_6)$ und $v(\frac{da_6}{d\pi})$. \square

Nun gilt es noch eine obere Schranke für die Höhe der S -ganzen Elemente in $2A(K)$ anzugeben.

Lemma 3.2.5. *Sei $Q = 2P$ ein S -ganzer Punkt in $2A(K)$. Das heißt, für alle Stellen w nicht in S gilt $w(x(Q)) \geq 0$. Dann ist auch P ein S -ganzer Punkt.*

Beweis. Sei $P = (x, y)$ und gelte $w(x) < 0$, dann $x(2P) = \frac{x^4 + a_1^2 a_6}{a_1^2 x^2}$. Da wir $w(a_i) \geq 0$ voraussetzen, gilt auch $w(x(2P)) < 0$. \square

Lemma 3.2.6. *Seien sowohl $P = (x, y)$ als auch $2P$ S -ganze Punkte und $v \in S$. Dann ist $v(x)$ nach unten beschränkt.*

Beweis. Wir wollen zeigen, dass $w(x) \leq n_w$ für alle Stellen $w \notin S$ gilt. Nach den Voraussetzungen gilt $w(x) \geq 0$ und $w(\frac{x^4 + a_1^2 a_6}{a_1^2 x^2}) \geq 0$ sowie $w(a_i) \geq 0$. Für den Zähler gilt dann $w(x^4 + a_1^2 a_6) \leq w(a_1^2 a_6)$ oder $4w(x) = w(a_1^2 a_6)$ während die Bewertung des Nenners $w(a_1^2 x^2) = 2(w(a_1) + w(x))$ erfüllt. Also haben wir $w(x) \leq \frac{1}{2}w(a_6)$ oder $w(x) = \frac{1}{4}w(a_1^2 a_6)$. Damit bekommen wir eine Schranke für die endlich vielen Nullstellen von x und somit auch eine für die Pole. \square

Wenn die 2-Torsion von A K -rational, also wenn a_6 ein Quadrat ist, dann müssen wir die obige Argumentation etwas modifizieren:

Lemma 3.2.7. *Sei $A : y^2 + a_1 xy + x^3 + a_2 x^2 + a_6^2 = 0$ eine elliptische Kurve mit rationalem 2-Torsionspunkt $P = (0, a_6)$. Dann gibt es eine elliptische Kurve A' mit Weierstraß-Gleichung*

$$y^2 + a_1 xy + x^3 + a_2 x^2 + a_1^3 a_6$$

und eine rationale Isogenie

$$V : A \rightarrow A', (x, y) \mapsto \left(\frac{x^2 + a_1 a_6}{x}, \frac{x^2 + a_1 a_6}{x^2} y + \frac{a_1^2 a_6 x + a_1^2 a_6^2}{x^2} + a_6 \right).$$

Die duale Isogenie ist durch

$$F : A' \rightarrow A, (x, y) \mapsto \left(\frac{x^2}{a_1^2}, y' \right)$$

gegeben.

Beweis. Das kann mit Velus Formel – siehe zum Beispiel [Koh96, S. 14] – nachgerechnet werden. \square

Lemma 3.2.8. *Sei A eine elliptische Kurve mit rationaler 2-Torsion. Dann ist die Menge der S -ganzen Punkte P auf $A(K)$ mit $P \notin F(A'(K))$ endlich und ihre Höhe durch eine berechenbare Konstante beschränkt.*

Beweis. Der Beweis verläuft analog zu dem Fall mit trivialer 2-Torsion und geht auf Voloch zurück. Statt der Abbildung μ verwenden wir nun die modifizierte Abbildung $\mu' : A(K) \rightarrow K, (x, y) \mapsto \frac{\alpha}{\alpha'} \frac{x'}{x}$ mit α ist kein Quadrat. Die Abbildung ist ein Homomorphismus mit Kern $F(A'(K))$. Explizite Schranken können wir zum Beispiel bekommen, indem wir mit Hilfe einer maximalen unabhängigen Menge das Bild von μ' bestimmen. \square

Lemma 3.2.9. *Sei $P = F(Q)$ ein S -ganzer Punkt in $F(A'(K))$. Dann ist Q ebenfalls S -ganz.*

Beweis. $F(x, y) = \frac{x^2}{a_1^2}$. Multiplizieren mit dem S -ganzen Element a_1^2 zeigt, dass x^2 S -ganz ist. \square

Lemma 3.2.10. *Die Menge der S -ganzen Punkte in $F(A'(K))$ ist endlich. Die Höhe ihre Punkte ist durch eine nur von der Weierstraß-Gleichung abhängige Konstante nach oben beschränkt.*

Beweis. Wir wissen, wenn $P \in A(K)$ S -ganz ist, so ist auch jedes $Q \in A'(K)$ mit $P = F(Q)$ S -ganz. Hat nun A' triviale 2-Torsion, dann können wir obige Aussage anwenden, um die Höhe von Q abzuschätzen. Ansonsten finden wir eine Isogenie auf eine Kurve A'' und wenden das Argument auf A'' an. Die j -Invariante der isogenen Kurve ist jeweils die Wurzel der j -Invariante der ausgehenden Kurve. Daher endet das Verfahren nach endlich vielen Schritten. Die auftretenden Kurven haben jeweils dieselbe Struktur in sofern, dass sich nur a_6 ändert. Daher gilt immer $x(F(x, y)) = \frac{x^2}{a_1^2}$. Haben wir nach endlich vielen Schritten eine Schranke für das Urbild ermittelt, so laufen wir den ganzen Weg zurück und bekommen eine Schranke für P . \square

3.2.1.2 Supersinguläre elliptische Kurven

Sei A eine supersinguläre elliptische Kurve über einem globalen Körper K der Charakteristik 2. Dann können wir annehmen, dass A durch eine Weierstraß-Gleichung der Form $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ gegeben ist. Die j -Invariante von A ist null und liegt somit im Konstantenkörper. Daher kann es unendlich viele S -ganze Punkte auf A geben. Wir bezeichnen einen Punkt $(x_0, y_0) \in A(K)$ als *nicht-quadratisch*, wenn x_0 kein Quadrat in K ist und werden nun beweisen, dass $A(K)$ für $K = \mathbb{F}_{2^d}(t)$ nur endlich viele nicht-quadratische S -ganze Punkte besitzt.

Lemma 3.2.11. *Die durch die Weierstraß-Gleichung $y^2 + a_3y + x^3 + a_4x + a_6 = 0$ über $\mathbb{F}_{2^d}(t)$ gegebene elliptische Kurve mit $a_3, a_4, a_6 \in \mathbb{F}_{2^d}[t]$ besitzt nur endlich viele Punkte (x_0, y_0) für die $x_0, y_0 \in \mathbb{F}_{2^d}[t]$ gilt und x_0 kein Quadrat ist. Der Grad von x_0 ist durch eine explizit berechenbare Konstante beschränkt.*

Beweis. Gelte $\deg(x_0) > \max\{\frac{1}{2} \deg(a_4), \frac{1}{3} \deg(a_6), \frac{2}{3} \deg(a_3)\}$. Dann ist der Grad von x_0 gerade. Es gilt $\deg(x_0) = 2n$ und $\deg(y_0) = 3n$. Da x_0 nach Voraussetzung kein Quadrat ist, ist $m := \deg \frac{dx_0}{dt}$ eine gerade natürliche Zahl. Das bedeutet $t^{(m+1)}$

ist das Monom von x_0 mit größtem ungeraden Grad und einem von null verschiedenen Koeffizienten. Aufgrund der Weierstraß-Gleichung gilt

$$\frac{d(a_3y_0)}{dt} = \frac{x_0^2 dx_0}{dt} + \frac{d(a_4x_0 + a_6)}{dt}$$

Daraus folgt

$$4n + m = \deg \frac{x_0^2 dx_0}{dt} \leq \max\{3n + \deg(a_3) - 1, 2n + \deg(a_4) - 1, \deg(a_6)\}.$$

Also ist n nach oben beschränkt und damit die Behauptung bewiesen. \square

Bemerkung 3.2.12. *Mit Blick auf die Abstiegs-Abbildung aus Lemma 1.3.12 sehen wir, dass alle außer endlich vielen S -ganzen Punkten im Kern von α_1 liegen. Wir haben also möglicherweise unendlich viele S -ganze Punkte auf $A(K)$, die die Bilder von Punkten auf $A^{(2)}(K)$ unter der Verschiebung sind und endlich viele weitere.*

3.2.2 Berechnung aller S -ganzen Punkte

In diesem Abschnitt beschränken wir uns auf gewöhnliche elliptische Kurven. Für die Berechnung aller nicht-quadratischer S -ganzer Punkte einer supersingulären elliptischen Kurve ist ein analoges Vorgehen möglich.

Nun da wir obere Schranken für die naive Höhe eines S -ganzen Punktes haben, können wir diese verwenden, um alle S -ganzen Punkte einer bestimmten Weierstraß-Gleichung der oben beschriebenen Form zu berechnen. Dazu gibt es verschiedene Möglichkeiten. Ein Vergleich der Verfahren an einem Beispiel findet sich in Abschnitt 4.6.

3.2.2.1 Direkt

Die Menge der möglichen x -Koordinaten S -ganzer Punkte ist endlich. Wir können über alle Kandidaten iterieren und durch Faktorisieren der Weierstraß-Gleichung diejenigen bestimmen, die K -rationale Punkte auf der elliptischen Kurve liefern. Die Menge der Kandidaten können wir – wie schon bei dem Siebalgorithmus beschrieben – unter Verwendung reduzierter Ganzheitsbasen explizit konstruieren. Durch Reduktion der Kurve modulo verschiedener Stellen kann diese Menge weiter eingeschränkt werden. Alternativ können wir Ansätze für die x - und y -Koordinaten S -ganzer Punkte machen. Einsetzen in die Weierstraß-Gleichung liefert ein Gleichungssystem in den Koeffizienten. Dieses können wir mit Hilfe von Gröbnerbasen lösen. Asymptotisch sind beide Methoden sehr langsam. In der Praxis ist vor allem die Zweite für nicht zu große Beispiele durchaus anwendbar.

3.2.2.2 Unter Verwendung der homogenen Räume

Sei α_1 die V -Abstiegs-Abbildung und C_b ein homogener Raum für das Element b der V -Selmergruppe der elliptischen Kurve A . Ist (x_0, y_0) ein S -ganzer Punkt auf A und gelte $\alpha_1(x_0, y_0) = (x + a_2)/a_1^2 = b + z_0^2 + z_0$ für ein $z_0 \in K$. Wir sehen direkt, dass z_0 nur an endlich vielen Stellen außerhalb von S Pole besitzen kann. Diese Stellen und eine untere Schranke für die Polordnung von z_0 lassen sich direkt anhand der Bewertungen von a_1 und b ablesen. Des Weiteren liefern uns die unteren Schranken für die Polordnung von x_0 an den Stellen aus S eben solche für z_0 . Diese sind in etwa halb so hoch. Statt also nach S -ganzen Punkten auf A zu suchen, können wir auch

mit den zuvor beschriebenen Methoden nach S_b -ganzen Punkten auf allen homogenen Räumen C_b suchen. Auf diese Weise können deutlich größere S -ganze Punkte gefunden werden.

3.2.2.3 Unter Verwendung von Mordell-Weil-Basen

Wir haben eine obere Schranke für die naive Höhe der S -ganzen Punkte auf einer elliptischen Kurve A . Kombinieren wir diese mit den in Abschnitt 3.1 angegebenen Schranken für die Differenz zwischen der naiven und der kanonischen Höhe, so bekommen wir eine obere Schranke für die kanonische Höhe der S -ganzen Punkte. Sei nun $\{P_1, \dots, P_r\}$ eine Mordell-Weil-Basis von $A(K)$, dann lässt sich jeder Punkt $P \in A(K)$ schreiben als $P = n_1P_1 + \dots + n_rP_r + T$ mit T ein Torsionspunkt und die n_i aus \mathbb{Z} . In der Arbeit von Gebel, Pethő und Zimmer [GPZ94] wird bewiesen, wie sich aus einer Schranke für die kanonische Höhe eine obere Schranke für die Beträge der Koeffizienten einer Darstellung bezüglich der gegebenen Mordell-Weil-Basis berechnen lässt. Das von ihnen vorgeschlagene Verfahren funktioniert ohne Weiteres in Charakteristik p und somit können wir nun in Abhängigkeit von einer zuvor berechneten Mordell-Weil-Basis $\{P_1, \dots, P_r\}$ ein $n \in \mathbb{Z}^{\geq 0}$ angeben, so dass für alle S -ganzen Punkte P mit $P = n_1P_1 + \dots + n_rP_r + T$ die n_i betraglich kleiner gleich n sind. Dieses Verfahren lässt sich mit den in [Ker09] beschriebenen Methoden weiter beschleunigen. Durch die Reduktion der Kurve modulo verschiedener Stellen und Berechnung der Bilder der Mordell-Weil-Basis unter der Reduktionsabbildung lässt sich die Menge der möglichen Koeffizienten weiter einschränken. Dabei wird nur von der Struktur der reduzierten Kurve Gebrauch gemacht, so dass sich die Argumentation ohne Weiteres von Charakteristik 0 auf Charakteristik p übertragen lässt. Allerdings ist diese Technik in unserem Fall nicht so entscheidend, da aufgrund der besseren Abschätzung für die naive Höhe S -ganzer Punkte im Funktionenkörperfall, auch die Schranken für die Koeffizienten einer Darstellung in der Mordell-Weil-Basis wesentlich kleiner sind. Der Hauptteil der Arbeit besteht darin, das Gruppengesetz anzuwenden. Das bietet Raum für weitere Optimierung.

3.2.3 Mordell-Kurven

In [Wil97] beschreibt Wildanger eine auf Mordell zurückgehende Methode zur Berechnung aller S -ganzen Punkte auf speziellen elliptischen Kurven über Zahlkörpern. Diese wird in [FGP13] von Fieker, Gaal und Pohst auf rationale Funktionenkörper über endlichen Körpern der Charakteristik größer 3 übertragen. An dieser Stelle untersuchen wir, wie ein analoges Vorgehen in Charakteristik 2 aussehen könnte.

Definition 3.2.13. *Eine elliptische Kurve A_{a_6} über einem Körper der Charakteristik 2 gegeben durch eine Weierstraß-Gleichung der Form $y^2 + xy + x^3 = a_6$ bezeichnen wir als Mordell-Kurve.*

Im Folgenden sei $K = \mathbb{F}_{2^d}(t)$ der rationale Funktionenkörper über einem endlichen Körper der Charakteristik 2. Sei A_{a_6} eine Mordell-Kurve über K und $(X, Y) \in \mathbb{F}_{2^d}[t]^2$ ein S -ganzer Punkt auf A . Dann besitzt das kubische Polynom

$$f(T) := T^3 + XT^2 + YT + Y^2 + X^3$$

die Diskriminante a_6^2 , wie sich leicht nachrechnen lässt. Wie in den zuvor zitierten Arbeiten ist somit das Problem der Bestimmung aller S -ganzen Punkte auf A_{a_6} darauf reduziert, Polynome vorgegebener Diskriminante zu berechnen. Leider scheint

das in Charakteristik 2 relativ schwierig zu sein. Normalerweise werden dazu alle kubischen Erweiterungen vorgegebener Diskriminante konstruiert und in diesen dann eine Indexformgleichung gelöst. Wenn wir aber nur die Diskriminante der endlichen Maximalordnung vorschreiben, dann gibt es unendlich viele nichtisomorphe kubische Erweiterungen von $\mathbb{F}_{2^d}(t)$. Wir könnten die zuvor berechnete Höhenschranke für den Grad der x -Koordinate verwenden, um Aussagen über die Verzweigung der unendlichen Stellen der Erweiterungen zu machen, aber es scheint, als wäre das Vorgehen dann aufwendiger, als das Durchprobieren sämtlicher möglicher x -Koordinaten wie zuvor beschrieben.

3.3 Berechnung von Endomorphismen

In [Soo13] präsentiert Soomro einen auf Manin zurückgehenden Beweis von Hasses Theorem über die Anzahl rationaler Punkte auf elliptischen Kurven über endlichen Körpern. Im Zuge dieses Beweises wird ein Zusammenhang zwischen Endomorphismen elliptischer Kurven über einem endlichen Körper k und $k(t)$ -rationalen Punkten auf eine korrespondierenden Kurve über $k(t)$ aufgezeigt. Genauer gesagt, sei E eine elliptische Kurve über k . Aus den Koeffizienten einer Weierstraß-Gleichung von E können wir direkt die Koeffizienten der Weierstraß-Gleichung einer elliptischen Kurve E^{tw} über $k(t)$ ablesen, so dass gilt

$$E^{\text{tw}}(k(t)) \cong \Psi := \{\psi \in \text{Mor}_k(E, E) \mid [-1] \circ \psi = \psi \circ [-1]\}.$$

Diese Isomorphie ist ebenfalls explizit und kann in beide Richtungen durchgeführt werden. Wir sehen direkt, dass $\text{End}_k(E)$, der Ring der k -rationalen Endomorphismen in Ψ enthalten ist. Für konkrete Beispiele ist es aber nicht schwierig, Morphismen in Ψ zu finden, die \mathcal{O} nicht auf \mathcal{O} abbilden, im Allgemeinen ist also $\text{End}_k(E)$ eine echte Untergruppe endlichen Index von Ψ , siehe [Soo13, Kapitel 5]. Wir können unseren Algorithmus zur Berechnung von Mordell-Weil-Basen verwenden, um den Rang von $\text{End}_k(E)$ und unabhängige Endomorphismen für elliptische Kurven über endlichen Körpern k zu bestimmen. Die Koeffizienten von E^{tw} haben für alle E kleine Grade, daher sollte für k nicht zu groß in der Praxis zumindest die Berechnung der Selmergruppen einfach sein. Es sei bemerkt, dass wir auf diese Weise Aussagen über $\text{End}_k(E)$ treffen, während in der Literatur – siehe [Koh96] – die Berechnung von $\text{End}_{\bar{k}}(E)$ von Interesse ist. Für nichtkommutative Endomorphismenringe besteht hier ein echter Unterschied.

Kapitel 4

Rechnungen

In diesem Kapitel geben wir einige Beispielrechnungen an. Diese sind auf einem Intel Core2Duo (64-Bit) System mit 3.00 GHz Taktung mit unserer Magma-Implementation [BCP97] durchgeführt worden. Die Laufzeit verschiedener Schritte ist nicht deterministisch und kann bei einigen Beispielen stark schwanken. Bei der Selmergruppenberechnung sind die Unterschiede für verschiedene Durchläufe desselben Beispiels klein, doch bei dem Reduktionsalgorithmus kann es einen großen Unterschied machen.

4.1 Ein Beispiel von Kramer

In [Kra77] untersucht Kramer die gewöhnliche elliptische Kurve

$$A : y^2 + xy + x^3 + t(t^5 + t^2 + 1)(t^7 + t^4 + 1) = 0$$

über dem rationalen Funktionenkörper $\mathbb{F}_2(t)$. Er berechnet Erzeuger für die V - und die F -Selmergruppe. Die V -Selmergruppe hat den Rang 1 und ist von der Klasse von t erzeugt. Die F -Selmergruppe ist von den Klassen von t , $t^5 + t^2 + 1$ und $t^7 + t^4 + 1$ erzeugt, hat also den Rang 3. Unser Algorithmus liefert nach 0,5 Sekunden dieselben Ergebnisse. Anschließend beweist Kramer, dass das Bild der F -Abstiegs-Abbildung β_1 von der Klasse von $t(t^5 + t^2 + 1)(t^7 + t^4 + 1)$ erzeugt ist. Ein Urbild ist zum Beispiel der nichttriviale 2-Torsionspunkt $(0, t(t^5 + t^2 + 1)(t^7 + t^4 + 1))$ auf $A^{(2)}(\mathbb{F}_2(t))$. Somit besitzt die Shafarevich-Tate-Gruppe $\text{III}(\mathbb{F}_2(t), A)$ nichttriviale F -Torsion welche von t und $t^5 + t^2 + 1$ erzeugt ist. Die korrespondierenden homogenen Räume liefern überall lokal lösbare Gleichungen ohne globale Lösung. So stellt die auf diese Weise entstehende Kurve

$$C : y^2 + xzy + (t^2 + t)x^4 + tx^3z + (t^{12} + t^7 + t^6 + t^5 + t^4 + t^2 + 1)z^4 = 0$$

eine Gegenbeispiel für das Lokal-Global-Prinzip für Geschlecht-Eins-Kurven in Charakteristik 2 dar.

Die Kurve $A^{(4)}$ besitzt die volle 4-Torsion über $\mathbb{F}_2(t)$. Unser Algorithmus berechnet in 52 Sekunden Erzeuger für die V^2 - und F^2 -Selmergruppe. Die V^2 -Selmergruppe besitzt 4 Elemente, die F^2 -Selmergruppe nur 16. Während ein V - und F -Abstieg uns eine obere Schranke von 3 für den Rang von $A(\mathbb{F}_2(t))$ geliefert haben, beträgt die

obere Schranke für den Rang nach einem V^2 - und F^2 -Abstieg nur noch 2. Der durch

$$\begin{aligned} x_1x_4 + x_2^2 + x_3^2 &= 0 \\ (t^7 + t^4 + 1)x_1^2 + x_2x_3 + (t^6 + t^3 + t)x_4^2 &= 0 \end{aligned}$$

gegebene homogene Raum repräsentiert ein nichttriviales Element der F^2 -Torsion von $\text{III}(\mathbb{F}_2(t), A)$.

Kramer äußert die Vermutung, dass der Rang von $A(\mathbb{F}_2(t))$ eins ist und schreibt, es wäre interessant, einen Punkt unendlicher Ordnung auf $A(\mathbb{F}_2(t))$ zu finden. Wir wissen bereits, dass das Bild von β_1 und β_2 von den Bildern der 2- bzw. 4-Torsionspunkte auf $A^{(2)}$ bzw. $A^{(4)}$ erzeugt wird. Wir suchen also ein Urbild eines nichttrivialen Elements von $\text{Sel}(\mathbb{F}_2(t), V)$ bzw. $\text{Sel}(\mathbb{F}_2(t), V^2)$. Wir berechnen die korrespondierenden homogenen Räume, minimieren und reduzieren diese und erhalten die Modelle

$$\begin{aligned} 0 &= t^4x_1^2 + (t^3 + 1)x_1x_3 + (t^5 + t^2 + t)x_3^2 + tx_3x_4 + x_4^2 \\ 0 &= (t^4 + t^3 + t^2)x_1^2 + (t^3 + t^2 + 1)x_1x_2 + (t^5 + t^4 + t^2 + t)x_1x_3 + (t^3 + 1)x_1x_4 + x_2^2 \\ &\quad + (t^5 + t^4 + t^2 + t)x_2x_3 + (t + 1)x_2x_4 + (t^4 + t^3 + t)x_3^2 + (t^4 + t^3)x_3x_4 + (t^2 + t)x_4^2 \end{aligned}$$

und

$$\begin{aligned} 0 &= (t^4 + t^3 + t)x_1^2 + (t^6 + t^5 + t^4 + 1)x_1x_2 + (t^6 + t^4 + t^3 + t^2)x_1x_3 + x_1x_4 \\ &\quad + (t^6 + t^3 + t^2 + 1)x_2^2 + (t^3 + t^2 + t)x_2x_3 + t^2x_2x_4 + (t^5 + t^4 + t^3 + t)x_3^2 \\ &\quad + (t^6 + t^5 + t^4 + t^2 + t)x_3x_4 + x_4^2 \\ 0 &= tx_1^2 + x_1x_2 + x_1x_3 + (t^5 + t^2 + 1)x_2^2 + tx_2x_3 + (t^6 + t^3 + t)x_3^2 + x_3x_4 \end{aligned}$$

Dabei benötigt die Minimierung jeweils weniger als eine Sekunde und die Reduktion zwischen 20 und 30 Sekunden. Auf diesen Kurven suchen wir nach Punkten und finden auf der ersten nach circa 7 Minuten den Punkt

$$\begin{aligned} (t^{11} + t^{10} + t^7 + t^5 + t^4 + t, t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^6 + t^4 + t^3 + t^2 + t, \\ t^5, t^{13} + t^{12} + t^9 + t^8 + t^7 + t^5) \end{aligned}$$

und auf der zweiten nach weniger als einer Sekunde den Punkt

$$(t^4 + 1, t^2, t^3 + t^2 + t + 1, t^4 + t^3 + t^2 + t + 1).$$

Beide liefern dann den Punkt

$$\left(\frac{t^{10} + t^8 + t^7 + t^6 + t^5 + t^2 + 1}{t^4}, \frac{t^{15} + t^{14} + t^{13} + t^{10} + t^7 + t^5 + t^4 + t^3 + 1}{t^6} \right)$$

auf $A(\mathbb{F}_2(t))$. Dieser hat die kanonische Höhe 10 und mit dem in Abschnitt 3.1 beschriebenen Vorgehen zeigen wir, dass er eine Mordell-Weil-Basis bildet.

4.2 Ein Beispiel von Ulmer

In dem Artikel [Ulm02] konstruiert Ulmer die Familie A_n von elliptischen Kurven über $\mathbb{F}_q(t)$ definiert durch die Weierstraß-Gleichung

$$A_n : y^2 + xy = x^3 + t^{2n+1}.$$

Er beweist, dass der Rang von $A_n(\mathbb{F}_q(t))$ größer gleich $\frac{2^n-1}{2^n}$ ist, ohne explizite Punkte zu konstruieren. Wir benutzen unsere Implementation, um für $q = 2$ und $n = 1, \dots, 5$ Mordell-Weil-Basen zu berechnen. Als Resultat erhalten wir:

$n = 1 :$

Mordell-Weil-Basis: $(t, 0)$

$n = 2 :$

Mordell-Weil-Basis: (t^2, t^3)

$n = 3 :$

Mordell-Weil-Basis: $(t^3, 0), (t^4, t^6 + t^5)$

$n = 4 :$

Mordell-Weil-Basis: $(t^6 + t^5 + t^4 + t^2, t^9 + t^5 + t^2), (t^8, t^{12} + t^{10} + t^9)$

$n = 5 :$

Mordell-Weil-Basis: $(t^{12} + t^9, t^{18} + t^{12} + t^9), (t^{11}, 0), (t^{16}, t^{24} + t^{20} + t^{18} + t^{17})$

$\left(\frac{t^{22} + t^{20} + t^{16} + t^{15} + t^{11} + t^{10} + t^6}{t^8 + t^6 + 1}, \frac{t^{33} + t^{32} + t^{31} + t^{26} + t^{24} + t^{23} + t^{16} + t^{15} + t^{12}}{(t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^6 + t^4 + t^3 + 1)} \right)$

Ein einfaches Argument mit Teleskopsummen zeigt uns, dass A_n den $\mathbb{F}_{2^d}(t)$ -rationalen Punkt

$$P_n := (t^{2^{n-1}}, t^{2^{n-1}+1} + t^{2^{n-1}+1+2^0} + t^{2^{n-1}+1+2^0+2^1} + \dots + t^{2^{n-1}+1+2^0+\dots+2^{n-2}})$$

unendlicher Ordnung besitzt. Um zu zeigen, dass P_n keine Torsionspunkt ist, können wir wie folgt vorgehen: Ist P_n ein Torsionspunkt, so auch $[4]P_n$. Wir zeigen nun, dass es eine Stelle v gibt, an der A gute Reduktion besitzt, für die aber $[4]P_n$ im Kern der Reduktionsabbildung ist. Da die Reduktionsabbildung injektiv auf den Torsionspunkten ist, kann $[4]P_n$ keiner sein. Mit Hilfe der Additionsformel berechnen wir die x -Koordinate von $[4]P_n$ und schreiben diese als rationale Funktion in t . Wir sehen, dass der Nenner von $t^{2^{n-1}} + 1$ und somit auch von $t + 1$ geteilt wird. Reduzieren wir den Zähler modulo $t + 1$, so ist das Ergebnis gleich eins. Die x -Koordinate von $[4]P_n$ hat somit an der zu $t + 1$ korrespondierenden Stelle v einen Pol, aber an der Diskriminante $\Delta(A_n) = t^{2^n+1}$ erkennen wir, dass A_n an v gute Reduktion besitzt.

4.3 Reduktion

An dieser Stelle untersuchen wir die Laufzeit und die Approximationsgüte des Reduktionsalgorithmus für Geschlecht-Eins-Modelle vom Grad 4. Da die Reduktion von Grad 2 Modellen einfacher ist, verzichten wir auf eine Testreihe dazu. Wie schon zuvor bezeichnen wir mit der Höhe eines Modells das Maximum über die Höhen – in unserem Fall also das Maximum über die Polynomgrade – aller Koeffizienten. Für den Test wählen wir minimierte und reduzierte Geschlecht-Eins-Modelle q_i vom Grad 4 für homogene Räume verschiedener elliptischer Kurven über $\mathbb{F}_{2^d}(t)$. Dann berechnen wir zufällige $\mathbb{F}_{2^d}[t]$ -äquivalente Modelle q'_i und wenden den Reduktionsalgorithmus auf diese nicht-reduzierten Modelle an. Dabei beschränken wir die Laufzeit jeweils nach oben, stoppen aber, wenn die Höhe des zu reduzierenden Modells kleiner gleich der unseres ursprünglichen Modells ist.

Grundkörper	$\mathbb{F}_2(t)$	$\mathbb{F}_2(t)$	$\mathbb{F}_2(t)$
red. Modell	q_1	q_2	q_3
Höhe q_i	2	2	2
Anzahl Bsp	1000	1000	1000
Höhe vor Red.	6 – 20	6 – 20	6 – 20
∅ Höhe vor Red.	13.0	12.5	12.8
Höhe nach Red.	2	2 – 10	2 – 10
∅ Höhe nach Red.	2	2.7	2.9
∅ Laufzeit in Sek.	5.9 (max. 60)	21.6 (max. 60)	24.1 (max. 60)

$$\begin{aligned}
 q_1 &= (t^2x_1^2 + (t^2 + t + 1)x_1x_3 + (t^2 + t + 1)x_1x_4 + tx_2^2 + tx_3^2 + (t^2 + t + 1)x_3x_4 + x_4^2, \\
 &\quad x_1^2 + (t^2 + t)x_1x_2 + tx_2^2 + x_2x_3) \\
 q_2 &= ((t^2 + t + 1)x_1x_3 + (t^2 + 1)x_1x_4 + x_2^2 + t^2x_2x_3 + (t^2 + 1)x_2x_4 + (t^2 + t)x_3^2 \\
 &\quad + (t^2 + 1)x_3x_4 + (t + 1)x_4^2, \\
 &\quad x_1^2 + (t + 1)x_2x_3 + tx_3^2 + x_3x_4) \\
 q_3 &= ((t^2 + 1)x_1^2 + (t^2 + 1)x_1x_2 + x_1x_4 + (t^2 + t + 1)x_2^2 + (t + 1)x_2x_4 + (t^2 + t)x_3^2 \\
 &\quad + tx_3x_4 + t^2x_4^2, \\
 &\quad t^2x_1^2 + (t^2 + 1)x_1x_2 + x_1x_4 + (t^2 + t)x_2^2 + tx_2x_4 + (t^2 + t)x_3^2 + (t + 1)x_3x_4 \\
 &\quad + (t^2 + 1)x_4^2)
 \end{aligned}$$

Grundkörper	$\mathbb{F}_{2^2}(t)$	$\mathbb{F}_{2^5}(t)$	$\mathbb{F}_{2^5}(t)$
reduziertes Modell	q_4	q_5	q_5
Höhe q_i	2	2	2
Anzahl Bsp.	1000	1000	1000
Höhe vor Red.	12 – 22	13 – 20	13 – 20
∅ Höhe vor Red.	17.3	17.2	17.2
Höhe nach Red.	2 – 13	10 – 14	10 – 14
∅ Höhe nach Red.	3.6	12.9	13.0
∅ Laufzeit in Sek.	130.1 (max. 180)	300 (max. 300)	600 (max. 600)

$$\begin{aligned}
q_4 &= ((t^2 + t + \gamma)x_1^2 + (\gamma^2 t^2 + \gamma^2 t + \gamma^2)x_1 x_2 + (\gamma^2 t^2 + \gamma^2 t + \gamma^2)x_1 x_3 + (\gamma t^2 + \gamma t)x_2^2 \\
&\quad + (\gamma t^2 + \gamma t + \gamma)x_2 x_3 + x_3^2 + (\gamma t^2 + \gamma t)x_4^2, \\
&\quad (t + \gamma^2)x_1^2 + \gamma^2 x_1 x_3 + (t^2 + t + \gamma)x_1 x_4 + (t + \gamma)x_2^2 + (\gamma t^2 + \gamma t + 1)x_2 x_3 \\
&\quad + (\gamma^2 t^2 + \gamma^2 t)x_2 x_4 + \gamma^2 x_3^2 + (\gamma t^2 + \gamma t + \gamma^2)x_3 x_4 + \gamma^2 t x_4^2) \\
q_5 &= (x_1^2 + x_3 x_4, \\
&\quad (\gamma^5 t^2 + \gamma^6 t + \gamma^{16})x_1 x_2 + \gamma^{25} x_1 x_3 + (\gamma^6 t^2 + \gamma^7 t + \gamma^{17})x_1 x_4 + x_2^2 \\
&\quad + (t^2 + \gamma^{20} t + \gamma^{30})x_4^2)
\end{aligned}$$

Bei den Modellen q_4 und q_5 bezeichnet γ jeweils einen Erzeuger der multiplikativen Gruppe von \mathbb{F}_{2^2} bzw. \mathbb{F}_{2^5} mit Minimalpolynom $\gamma^2 + \gamma + 1 = 0$ bzw. $\gamma^5 + \gamma + 1 = 0$. Die Laufzeit ist für alle Beispiele in Sekunden angegeben. Die Zahl in Klammern dahinter gibt die obere Schranke für die Laufzeit an. Für kleine Konstantenkörper berechnet der Reduktionsalgorithmus schnell und zuverlässig Modelle mit kleinen Koeffizienten. Doch schon für Konstantenkörper mit 32 Elementen ist er auch nach 10 Minuten im Mittel noch weit von einem optimalen Modell entfernt.

4.4 Große Koordinaten

Die gewöhnliche elliptische Kurve

$$A : y^2 + (t^4 + t^3 + t^2 + 1)xy + x^3 + (t^4 + t^3 + t^2) = 0$$

über $\mathbb{F}_2(t)$ hat – wie Magma berechnet – den analytischen Rang 1. Die V -Selmergruppe ist von $t/(t^3 + t + 1)$ und die F -Selmergruppe von dem Bild des nichttrivialen 2-Torsionspunkt auf $A^{(2)}(K)$ erzeugt. Somit besitzt $A(K)$ einen Punkt unendlicher Ordnung genau dann, wenn $t/(t^3 + t + 1)$ ein Urbild unter α_1 besitzt. Dieses Urbild korrespondiert zu einem Punkt auf

$$\begin{aligned}
q &= y^2 + ((t^4 + t^3 + t^2 + 1)x^2 + (t^8 + t^6 + t^4 + 1)x + (t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 \\
&\quad + t^2 + t))y + (t^6 + t^3 + t^2 + t)x^4 + (t^{12} + t^{11} + t^{10} + t^6 + t^5 + t^3 + t + 1)x^3 \\
&\quad + (t^{14} + t^{11} + t^8 + t^6 + t^5 + t^4 + t^3 + t)x^2 + (t^{16} + t^{15} + t^{14} + t^{12} + t^{10} \\
&\quad + t^9 + t^7 + t^6 + t^5 + t^2)x + (t^{18} + t^{15} + t^{14} + t^{13} + t^{12} + t^{10} + t^9 + t^6 + t^2)
\end{aligned}$$

Minimierung und Reduktion liefern uns nach wenigen Minuten das Grad 4 Modell

$$\begin{aligned}
q_1 &= t^4 x_1^2 + (t^4 + t^3 + 1)x_1 x_2 + (t + 1)x_1 x_3 + t^2 x_1 x_4 + t^3 x_2^2 + (t + 1)x_2 x_3 + (t^4 + t^3 \\
&\quad + t^2 + 1)x_2 x_4 + (t + 1)x_3 x_4 + (t^4 + t^2)x_4^2 \\
q_2 &= (t^4 + t^2 + 1)x_1^2 + (t^4 + t^3 + 1)x_1 x_2 + (t^4 + t^3 + t^2 + t)x_1 x_3 + t^2 x_1 x_4 + (t^4 + t^2) \\
&\quad x_2^2 + (t + 1)x_2 x_3 + (t^4 + t^3 + t^2 + 1)x_2 x_4 + (t^3 + t^2 + t)x_3^2 + (t + 1)x_3 x_4 + t^3 x_4^2
\end{aligned}$$

auf dem wir nach Punkten sieben. Der Siebalgorithmus findet allerdings nach mehr als 2 Stunden keinen nichttrivialen Punkt. Daher führen wir einen weiteren Abstieg

durch. Die V^2 -Selmergruppe wird von dem Wittvektor

$$\left(\frac{t}{t^3 + t + 1}, \frac{t^{11} + t^9 + t^4 + t^3 + t^2}{t^{12} + t^{11} + t^9 + t^8 + t^7 + t^3 + t^2 + 1} \right)$$

erzeugt. Der korrespondierende homogene Raum ist durch die Gleichungen

$$\begin{aligned} & (t^{18} + t^{16} + t^{15} + t^4 + t^3 + t^2 + t + 1)x_1^2 + (t^{27} + t^{26} + t^{21} + t^{20} + t^{19} + t^{17} \\ & + t^{16} + t^{14} + t^{12} + t^{11} + t^7 + 1)x_1x_3 + (t^{22} + t^{21} + t^{18} + t^{17} + t^{16} + t^{15} + t^8 \\ & + t^6 + t^5 + t^3 + t + 1)x_1x_4 + (t^{25} + t^{23} + t^{22} + t^{20} + t^{19} + t^{13} + t^9 + t^7 + t^6 \\ & + t^2 + 1)x_2^2 + (t^{31} + t^{29} + t^{27} + t^{23} + t^{19} + t^{14} + t^{13} + t^9 + t^7 + t^5 + 1)x_2x_3 \\ & + (t^{26} + t^{25} + t^{24} + t^{23} + t^{21} + t^{18} + t^{17} + t^{16} + t^{14} + t^{13} + t^{10} + t^8 + t^7 \\ & + t^4 + t^3 + 1)x_2x_4 + (t^{34} + t^{32} + t^{31} + t^{29} + t^{28} + t^{24} + t^{21} + t^{20} + t^{19} + t^{18} \\ & + t^{17} + t^{15} + t^{14} + t^{13} + t^{12} + t^{10} + t^9 + t^6 + t^3 + t^2)x_3^2 + (t^{28} + t^{27} + t^{19} \\ & + t^{18} + t^{14} + t^8 + t^7 + t^5 + t^4 + t^3 + t)x_3x_4 + (t^{24} + t^{23} + t^{20} + t^{19} + t^{18} + \\ & t^{17} + t^{14} + t^{10} + t^6 + t^3 + t)x_4^2 = 0 \\ & (t^{19} + t^{15} + t^{13} + t^{11} + t^{10} + t^9 + t^8 + t^6 + t^2 + t)x_1^2 + (t^{28} + t^{27} + t^{26} + t^{24} \\ & + t^{22} + t^{21} + t^{20} + t^{17} + t^{16} + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^7 + t^6 + t \\ & + 1)x_1x_3 + (t^{23} + t^{22} + t^{21} + t^{18} + t^{16} + t^{15} + t^{12} + t^{11} + t^{10} + t^3 + t^2 \\ & + t)x_1x_4 + (t^{26} + t^{22} + t^{21} + t^{19} + t^{18} + t^{16} + t^{15} + t^{14} + t^{11} + t^8 + t^7 + t^6 \\ & + t^5 + t^2 + 1)x_2^2 + (t^{32} + t^{29} + t^{27} + t^{26} + t^{25} + t^{23} + t^{21} + t^{20} + t^{18} + t^{15} \\ & + t^{13} + t^{11} + t^9 + t^7 + t^6 + t^4 + 1)x_2x_3 + (t^{27} + t^{26} + t^{24} + t^{22} + t^{21} + t^{20} \\ & + t^{19} + t^{18} + t^{16} + t^{14} + t^{13} + t^9 + t^5 + t^4 + t + 1)x_2x_4 + (t^{35} + t^{31} + t^{30} \\ & + t^{28} + t^{27} + t^{24} + t^{23} + t^{18} + t^{16} + t^{15} + t^{13} + t^{10} + t^9 + t^8 + t^6 + t^5 + t^4 \\ & + t^3 + t + 1)x_3^2 + (t^{29} + t^{28} + t^{27} + t^{25} + t^{21} + t^{20} + t^{14} + t^8 + t^4 + 1)x_3x_4 + \\ & (t^{25} + t^{24} + t^{23} + t^{20} + t^{18} + t^{17} + t^{15} + t^{14} + t^9 + t^8 + t^7 + t^5 + t^2 + t)x_4^2 = 0 \end{aligned}$$

gegeben. Reduktion liefert uns nach wenigen Minuten das $\mathbb{F}_2[t]$ -äquivalente Modell

$$\begin{aligned} q'_1 &= (t^6 + t^4 + t)x_1x_2 + (t^4 + t^3)x_1x_3 + (t^3 + t^2 + t + 1)x_1x_4 + (t^6 + t^4 + t^3 + t^2)x_2^2 \\ & + (t^6 + t^4 + t)x_2x_3 + (t^4 + t^2)x_3^2 + (t^5 + t^4 + t^3 + 1)x_3x_4 + (t^5 + t^4)x_4^2 \\ q'_2 &= (t^5 + t^3)x_1^2 + (t^5 + t^3 + t^2)x_1x_3 + (t^6 + t^5 + t^3 + 1)x_1x_4 + (t^5 + t)x_2^2 + (t^5 + t^4 \\ & + 1)x_2x_3 + (t^6 + t^3 + t^2 + t)x_2x_4 + (t^4 + t^3 + t^2 + 1)x_3^2 + (t^6 + t^5 + t^3 + t^2)x_4^2 \end{aligned}$$

Auf diesem finden wir mit unserem Sieb nach weniger als 20 Sekunden den nichttrivialen Punkt

$$(t^6 + t, t^6 + t^5 + t^4 + t^3, t^9 + t^8 + t^7 + t^6 + t^5, t^8 + t^4)$$

und dieser liefert uns den Punkt

$$\left(\frac{t^{13} + t^{10} + t^8 + t^6 + t^5 + t^3 + t^2}{t^{16} + t^{14} + t^{12} + t^{10} + t^6 + t^4 + 1}, \frac{t^{26} + t^{25} + t^{22} + t^{19} + t^{17} + t^{16} + t^{15} + t^{13} + t^{11} + t^6 + t^4 + t}{t^{24} + t^{23} + t^{19} + t^{18} + t^{17} + t^{16} + t^{14} + t^6 + t^5 + t^4 + t^3 + t^2 + 1} \right)$$

unendlicher Ordnung auf A . Er hat die kanonische Höhe $37/2$. Dieses Beispiel illustriert die Vereinfachung, die sich durch Reduktion und Minimierung erreichen lässt. Des Weiteren zeigt es Grenzen für die Höhe von Punkten, die durch einen V - oder F -Abstieg gefunden werden können und veranschaulicht die Notwendigkeit höherer Abstiege.

Die Kurve A ist das Resultat einer Suche nach elliptischen Kurven mit kleinen Koeffizienten, die keine Mordell-Weil-Basis aus Punkten kleiner Höhe besitzen. Meist besitzen elliptische Kurven mit ähnlich kleinen Koeffizienten deutlich kleinere Erzeuger.

4.5 Sieben

In einer Testreihe untersuchen wir die Wahl der Stelle, die die Gitter definiert. Im Allgemeinen gilt für eine feste Höhengrenze: je größer der Grad der Stelle, desto mehr Gitter müssen untersucht werden und desto schneller geht die Untersuchung eines einzelnen Gitters. Ist die elliptische Kurve über $\mathbb{F}_q(t)$ definiert und wählen wir eine Stelle vom Grad d , dann hat die reduzierte Kurve in etwa q^d viele Punkte, d.h. wir müssen q^d viele Gitter untersuchen. Jedes Gitter hat eine Diskriminante vom Grad $5d$ und den Rang 4. Ist h eine Höhengrenze und ist der Grad jedes Gittervektors kleiner gleich h , dann müssen pro Gitter q^{4h-5d} Gittervektoren untersucht werden. Das folgt direkt aus den möglichen Koeffizienten einer Linearkombination für einen Gittervektor unter der Schranke h . Für die Konstruktion eines Gitters müssen einige Rechnungen durchgeführt werden. Schätzen wir die dafür benötigte Zeit durch eine Konstante C_1 ab und die Zeit zum Testen eines Gittervektors durch C_2 bekommen wir für die Gesamtlaufzeit

$$C_1 q^d + q^d C_2 q^{4h-5d}.$$

Im Allgemeinen wird C_1 deutlich größer als C_2 sein. Diese Abschätzung der Laufzeit hat einige Schwächen. Zum einen ist die Abschätzung der Anzahl der zu untersuchenden Vektoren zu klein, wenn die Grade von einem oder mehreren der reduzierten Basisvektoren größer gleich h sind. Das ist häufig der Fall, wenn h und d in etwa gleich groß sind. Zum anderen wird, wenn wir mit Gröbnerbasen oder Resultanten arbeiten, nicht jeder Gittervektor einzeln untersucht. Wir müssen also $C_2 q^{4h-5d}$ durch einen anderen von q, h und d abhängigen, schwer zu bestimmenden Wert ersetzen. In [Rob07] wird vorgeschlagen, den Grad der Stelle minimal zu wählen unter der Nebenbedingung, dass für alle Punkte unterhalb der Höhengrenze mindestens ein Koeffizient bei der Darstellung als Gitterpunkt bezüglich einer reduzierten Gitterbasis gleich null ist, also in etwa $d = \frac{4}{5}h$. Für kleine Konstantenkörper erweist sich diese Wahl auch bei uns als gut. Wir haben 100 Beispiele über \mathbb{F}_2 berechnet und nach Punkten mit naiver Höhe kleiner gleich 15 gesucht. Zur Konstruktion der Gitter haben wir eine Stelle vom Grad 7, eine vom Grad 12 und eine vom Grad 14 verwendet. Dabei ist $12 = \frac{4}{5} \cdot 15$ der von Roberts vorgeschlagene Grad. Die resultierenden Laufzeiten lagen je nach Beispiel und verwendeter Methode zwischen 4 und 7 Minuten. Für jede Stelle war die auf Resultanten basierende Methode am schnellsten und die Differenz der Laufzeiten betrug im Allgemeinen weniger als 30 Sekunden. Bei der Verwendung, der auf der Lösung von Gleichungssystemen über \mathbb{F}_2 basierenden Methode waren die Differenzen der Laufzeiten im Schnitt größer, doch betrug sie auch hier meist weniger als eine Minute. Verwenden wir hingegen eine deutlich kleinere Stelle, zum Beispiel vom Grad 4, so dauert die Berechnung meist mehr als eine Stunde. Eine weitere Testreihe über

\mathbb{F}_{2^3} zeigt ähnliche Ergebnisse. Für größere Konstantenkörper ändert sich die Situation. Schon über $\mathbb{F}_{2^{10}}$ benötigt das Berechnen aller Gitter für eine Stelle vom Grad 2 mehr als 5 Stunden (es sind über eine Millionen Gitter) während das Sieben nach Punkten der Höhe kleiner gleich 4 mit einer Stelle vom Grad 1 weniger als 15 Minuten benötigt.

Nun untersuchen wir die in Abschnitt 2.4.5 vorgestellten unterschiedliche Methoden, um nach Gitterpunkten zu suchen, die auf dem Schnitt zweier über dem globalen Funktionenkörper K definierten Quadriken liegen, genauer. Diese basieren entweder auf der Lösung eines Gleichungssystems über dem endlichen Konstantenkörper k von K – durch Gröbnerbasenberechnung oder durch vollständige Enumeration – oder auf der Berechnung von Resultanten und der Faktorisierung von Polynomen über K . An dieser Stelle vergleichen wir die Methoden anhand einiger Beispiele. Dazu sei $K = \mathbb{F}_{2^d}(t)$. Wir erzeugen zufällig elliptische Kurven und berechnen Modelle vom Grad 4 für ihre homogenen Räume. Auf diesen Kurven sieben wir dann nach Punkten. Für Kurven über $\mathbb{F}_2(t)$ und bei relativ kleinem Suchbereich unterscheidet sich die Laufzeit aller drei Methoden nur geringfügig. Liegt diese zwischen wenigen Sekunden und circa 3 Minuten (je nach Suchbereich), so ist bei den gerechneten Beispielen die Differenz der Laufzeit zwischen der Verwendung von Gröbnerbasen und der vollständigen Enumeration meist kleiner als 1% der Gesamtlaufzeit, mit mal der einen mal der anderen Methode im Vorteil. Die auf Resultanten basierende Methode ist immer etwas schneller als die anderen beiden. Die Differenz beträgt zwischen 2% und 10% der Gesamtlaufzeit. Dieses Verhalten lässt sich auch für größere Suchbereiche mit Laufzeiten zwischen 10 Minuten und einer Stunde feststellen.

Mit wachsender Größe des Konstantenkörpers wird die Resultantenmethode im Vergleich zu den anderen beiden langsamer. Während über $\mathbb{F}_{2^5}(t)$ bei Laufzeiten zwischen 30 Sekunden und 30 Minuten alle Methoden in etwa gleich schnell sind, mit mal der einen und mal der anderen im Vorteil, so ist schon über $\mathbb{F}_{2^7}(t)$ die Resultantenmethode bei allen Beispielen am langsamsten. Doch auch hier beträgt die Differenz nur einen Bruchteil der Gesamtlaufzeit. Für $\mathbb{F}_{2^{10}}(t)$ sind die Unterschiede gravierend. Beispiele, bei denen die auf Gröbnerbasen basierende Methode wenige Minuten benötigt, können von den anderen beiden Methoden auch in mehreren Stunden nicht gelöst werden.

Die Resultantenmethode hat den Vorteil, dass sie auch Punkte finden kann, deren Höhe größer als die vorgegebene Schranke ist. Grund dafür ist, dass die Koeffizienten, die durch das Faktorisieren bestimmt werden, nicht beschränkt sind. In der Praxis tritt diese Situation für sehr kleine Suchbereiche häufig auf. Und auch bei größeren ist es nicht schwierig, homogene Räume zu finden, bei denen die Resultantenmethode Punkte findet, die anderen beiden aber erfolglos bleiben. Für Kurven über $\mathbb{F}_2(t)$ und Laufzeiten zwischen 20 Sekunden und 20 Minuten war das bei uns für 6 von 100 Beispielen der Fall.

4.6 Berechnung ganzer Punkte

Die Kurve A über $\mathbb{F}_2(t)$ gegeben durch die Weierstraß-Gleichung

$$y^2 + xy = x^3 + (t^{12} + t^{10} + t^8 + t^5 + t^4 + t^3 + t^2 + t + 1)$$

besitzt viele ganze Punkte. Wir berechnen sie mit Hilfe der verschiedenen Methoden und vergleichen die benötigte Zeit. Die V - und F -Selmergruppe lassen sich in weniger

als einer Sekunde berechnen. Eine Suche nach kleinen Punkten liefert uns Urbilder für die Abstiegs-Abbildungen und so können wir in kurzer Zeit eine Mordell-Weil-Basis bestehend aus den drei Punkten

$$(t^2 + t + 1, t^6 + t^5 + t^3 + t + 1), (t^3 + t^2 + t, t^6 + t^5 + t^3 + t + 1),$$

$$\left(\frac{t^3 + 1}{t^4}, \frac{t^{12} + t^{11} + t^{10} + t^5 + t^4 + t^3 + t^2 + t + 1}{t^6} \right)$$

berechnen. Mit der unter Abschnitt 3.2.1 beschriebenen Technik berechnen wir, dass die Grade der x -Koordinaten ganzer Punkte kleiner gleich 12 sind. Magma benötigt weniger als 4 Sekunden, um zu testen, für welche der 2^{13} möglichen x -Koordinaten eine y -Koordinate existiert. Auf diese Weise finden wir 20 ganze Punkte. Die V -Selmergruppe besitzt 4 Elemente. Jeder ganze Punkt auf A kommt von einem ganzen Punkt auf einem der vier homogenen Räume C_i der Form $y^2 + P_i(z)y + Q_i(z) = 0$. Der Grad der z -Koordinate der gesuchten ganzen Punkte auf den C_i ist kleiner gleich 6. Statt 2^{13} Elemente zu untersuchen, können wir uns mit dieser Technik auf die Untersuchung von $4 \cdot 2^7 = 2^9$ Elemente beschränken. Magma findet auf diese Weise in weniger als einer Sekunde die 20 ganzen Punkte auf A . Alternativ können wir einen Ansatz für x und y machen und das Gleichungssystemen der Koordinaten lösen. Das Gleichungssystem besteht aus 37 Gleichungen (der Grad von x^3 ist 36) in 32 Variablen (Grad von x plus Grad von y plus 2). Magma kann es durch einen auf die Berechnung von Gröbnerbasen über \mathbb{F}_2 spezialisierten Algorithmus in weniger als einer Sekunde lösen und wir bekommen wieder dieselben 20 ganzen Punkte. Aus der Schranke für die naive Höhe eines ganzen Punktes berechnen wir, dass die Koeffizienten von Darstellungen ganzer Punkte bezüglich unserer Mordell-Weil-Basis betraglich kleiner gleich 8 sind. Das liefert uns $9 \cdot 17 \cdot 17 - 1 = 2600$ zu untersuchende Punkte. Das Durchprobieren aller dieser berechnet uns ebenfalls in weniger als 4 Sekunden die gesuchten 20 ganzen Punkte. Betrachten wir die Struktur der modulo der endlichen Stellen vom Grad 1 reduzierten Kurve, dann können wir die Anzahl der Koeffizienten weiter einschränken. Statt der 2600 Punkte müssen wir dann nur 1446 Punkte untersuchen. Vergleiche [Ker09].

Zum Vergleich berechnen wir die ganzen Punkte auf $y^2 + xy = x^3 + (t^3 + t + 1)$ über $\mathbb{F}_{23}(t)$. Der Rang dieser Kurve ist nur 1 und wir finden nach wenigen Sekunden einen Erzeuger $P = (t, t + 1)$. Eine obere Schranke für den Grad der x -Koordinate ist 4. Das Testen aller möglichen x -Koordinaten benötigt circa 8 Sekunden, das Lösen des Gleichungssystems circa 55 Sekunden. Eine Schranke für den Koeffizient eines ganzen Punktes dargestellt bezüglich der Mordell-Weil-Basis ist 2, in weniger als einer Sekunde können beide Punkte getestet werden. Jede der Methoden findet nur die ganzen Punkte P und $-P$.

4.7 Vergleich mit Magma

Ein Algorithmus zur Berechnung der V - und F -Selmergruppe gewöhnlicher elliptischer Kurven über rationalen Funktionenkörpern existiert bereits in Magma. Er basiert auf derselben theoretischen Grundlage wie unser Algorithmus. Zum Vergleich haben wir beide auf verschiedene zufällig erzeugte Beispiele mit unterschiedlichen Konstantenkörpern und unterschiedlichen Schranken für die Grade der Koeffizienten

angewendet. Als Resultat bekommen wir die folgenden durchschnittlichen Laufzeiten. Die Varianz in den einzelnen Testreihen ist mitunter sehr groß. Neben einem Vergleich mit der Laufzeit der existierenden Implementation sollen die Abhängigkeit dieser von der Größe der Koeffizienten und dem Konstantenkörper veranschaulicht werden.

Grundkörper	max. Grad a_i	Anzahl Bsp.	Ø Laufzeit	Ø Laufzeit Magma
$\mathbb{F}_2(t)$	4	100	0.5 s	1.9 s
$\mathbb{F}_2(t)$	7	100	0.7 s	17.8 s
$\mathbb{F}_2(t)$	14	100	245.4 s	-
$\mathbb{F}_{2^2}(t)$	3	100	0.5 s	10.3 s
$\mathbb{F}_{2^2}(t)$	5	100	6.9 s	331.75 s
$\mathbb{F}_{2^2}(t)$	7	100	277.9 s	2636.7 s
$\mathbb{F}_{2^3}(t)$	3	100	2.9 s	172.1 s
$\mathbb{F}_{2^3}(t)$	5	100	1578.0 s	-
$\mathbb{F}_{2^4}(t)$	3	100	75.5 s	1545.1 s

In Magma ist ein Algorithmus implementiert, der für elliptische Kurven über $\mathbb{F}_{2^m}(t)$ mit Koeffizienten $a_i \in \mathbb{F}_{2^m}[t]$ und $\deg a_i \leq i$ eine Mordell-Weil-Basis berechnet. Ist der Konstantenkörper gleich \mathbb{F}_2 , dann benötigt die Rechnung je nach Größe der Koeffizienten, Rang und Höhe der Erzeuger der elliptischen Kurve zwischen circa einer Sekunde und zwei Minuten. Es ist relativ schwierig die Laufzeit dieses Algorithmus mit der unseres zu vergleichen. Viele der Kurven besitzen Punkte mit kleinen Koordinaten, so dass unser Algorithmus ebenfalls sehr schnell ist, falls die Schranke für den Rang, die uns die Selmergruppen liefern, mit dem tatsächlichen Rang übereinstimmt. Ist das nicht der Fall, so kann unser Algorithmus das Problem nicht exakt lösen (zumindest nicht ohne zusätzliche Rechnungen durchzuführen). Zum Vergleich folgt ein zufällig gewähltes Beispiel vom Rang 2. Für die durch $y^2 + txy + x^3 + (t^2 + 1)x^2 + t^3 + t^2 + 1$ definierte gewöhnliche elliptische Kurve über $\mathbb{F}_2(t)$ genügen die Grade der Koeffizienten der Ungleichung $\deg(a_i) \leq i$. Magma berechnet in circa 2 Minuten eine Mordell-Weil-Basis. Unser Algorithmus benötigt weniger als eine Sekunde zur Berechnen der V - und F -Selmergruppe. In jeweils circa 5 Sekunden können minimierte und reduzierte Modelle für die beiden relevanten homogenen Räume berechnet werden und in weiteren 5 Sekunden finden wir jeweils einen Punkt auf ihnen. Anschließend benötigen wir eine weitere Sekunde, um zu zeigen, dass die beiden gefundenen Punkte bereits eine Modell-Weil-Basis bilden. Die Laufzeit der Magmafunktion wächst – wie auch die unserer Implementation – stark mit wachsender Größe des Konstantenkörpers, doch es scheint, als hätte hier Magma bei vielen Beispielen einen Vorteil. Ebenso ist Magma bei Kurven mit einem sehr großen Erzeuger schneller.

Kapitel 5

Schluss

5.1 Weitere Methoden zur Berechnung von Mordell-Weil-Basen

Abgesehen von der in dieser Arbeit behandelten Methode zur Berechnung der Mordell-Weil-Basis einer elliptischen Kurve gibt es in der Literatur noch weitere Ansätze. Hier ein kurzer – möglicherweise unvollständiger – Überblick. Elliptische Kurven über einem Funktionenkörper K können auch mit Flächen über dem Konstantenkörper von K in Verbindung gebracht werden. Siehe Kapitel III in [Sil94]. Diesen Flächen lässt sich eine abelsche Gruppe, die Néron-Severi-Gruppe, zuordnen. Nach einem Theorem von Severi und Néron ist sie endlich erzeugt und das Theorem von Shioda-Tate stellt eine Verbindung zwischen ihrem Rang und dem Rang der elliptischen Kurve über K her, siehe [Sil94], [Ulm09], [Shi99]. In diesen Quellen wird allerdings vorausgesetzt, dass der Konstantenkörper von K algebraisch abgeschlossen ist. Eine kurze Behandlung der Situation für endliche Konstantenkörper findet sich in [Ulm13]. Die Berechnung des Rangs der Néron-Severi-Gruppe der korrespondierenden elliptischen Fläche stellt somit eine alternative Möglichkeit dar, um Aussagen über den Rang einer elliptischen Kurve zu treffen. Siehe dazu auch die Bemerkungen in [Ulm04] nach Theorem 4.2.1 für Vorschläge zur Konstruktion von Punkten mit dieser Methode.

Die Birch-Swinnerton-Dyer-Vermutung (BSD) ist für elliptische Kurven über globalen Funktionenkörpern in vielen Fällen bewiesen. Für solche elliptische Kurven lässt sich der Rang mit analytischen Methoden bestimmen. In [Ulm09] findet sich ein Überblick über verschiedene Resultate zur Konstruktion von unendlichen Familien elliptischer Kurven, für die BSD gilt und deren Rang gegen Unendlich strebt. Die Magma Implementation zur Berechnung des analytischen Rangs ist in der Praxis für Kurven mit kleinen Koeffizienten sehr schnell. Sie bietet uns eine Möglichkeit, den Rang bestimmter elliptischer Kurven zu ermitteln. Selbst für Kurven, für die BSD nicht verifiziert ist, bekommen wir auf diese Weise eine obere Schranke für den Rang. Allerdings hilft uns die Kenntnis der L -Reihe im Allgemeinen nicht bei der Suche nach konkreten Punkten. Da sich mit der Abstiegs-Methode Punkte mit weit größerer Höhe finden lassen, als es mit einer direkten Suche möglich wäre, bleiben die Überlegungen dieser Arbeit relevant, selbst wenn BSD vollständig bewiesen ist.

Für elliptische Kurven vom Rang eins gibt es eine analytische Methode zur Berechnung eines Erzeugers. Einen Überblick über die Resultate und die sich daraus

ergebenden Möglichkeiten, findet sich in [Ulm04].

5.2 Richtungen für zukünftige Arbeiten

Bei einem 4- (oder 8-Abstieg) für eine elliptische Kurve A über einem Zahlkörper, wie in [Wom03] oder [Sta05] beschrieben, unterscheidet sich das Vorgehen von dem in dieser Arbeit behandelten Vorgehen bei einem V^2 - und F^2 -Abstieg. Anstatt A direkt mit einer 4-Abstiegs-Abbildung zu untersuchen, wird erst ein 2-Abstieg durchgeführt und anschließend nehmen die homogenen Räume C der 2-Selmergruppe die Rolle von A ein und dienen als Ausgangspunkt für weitere Abstiege. Dieses Vorgehen hat einige Vorteile. Zum einen können ganz gezielt bestimmte homogene Räume untersucht werden und alle, auf denen bereits ein rationaler Punkt gefunden wurde, verursachen keine weitere Arbeit. Zum anderen sind keine Rechnungen in dem Erweiterungskörper, über dem A volle 4-Torsion besitzt, notwendig. Es genügt, wenn A volle 2-Torsion besitzt. Es stellt sich daher die Frage, wie ein vergleichbares Vorgehen in Charakteristik 2 zu bewerkstelligen ist. Dazu könnten wir versuchen, die Operation von A auf einem ihrer homogenen Räume C zu benutzen, um eine Gruppenstruktur auf C zu definieren. Mit Hilfe dieser müsste ein Analogon zur Verschiebung und zum Frobenius definiert und dieses zur Konstruktion expliziter Abstiegs-Abbildungen verwendet werden.

Der in dieser Arbeit vorgestellte Reduktionsalgorithmus für Geschlecht-Eins-Modelle arbeitet für Modelle über einem rationalen Funktionenkörper mit kleinem Konstantenkörper zuverlässig. Doch für größere Konstantenkörper ist er langsam und speicherintensiv. Es wäre interessant zu sehen, ob sich das Berechnen von Geschlecht-Eins-Modellen mit kleinen Koeffizienten auf das Finden kurzer Basen eines geeigneten Gitters reduzieren lässt. Dieses Problem wäre nämlich über Funktionenkörpern effizient lösbar. Da etwas vergleichbares zumindest über \mathbb{Q} möglich ist – siehe [CFS10] – besteht hier Hoffnung.

Eine weitere offene Frage, mit der sich zukünftige Arbeiten befassen können, ist in wie weit die vorgestellten Methoden modifiziert werden müssen um F^i - und V^i -Abstiegs-Abbildungen für $i \geq 2$ auch im supersingulären Fall zu konstruieren.

Kapitel 6

Anhang

6.1 Gruppenschema

In diesem Abschnitt des Anhangs geben wir einen sehr kurzen Überblick über Gruppenschemata. Als Quellen für die Definitionen und Aussagen dienten dabei hauptsächlich [Sil94], [Mum70], [KM85], [Wat79] sowie Kapitel 3 von [Sha86]. Ausführliche Informationen über die verwendeten Begriffe der Schematheorie finden sich zum Beispiele bei [Har77]. Viele Begriffe könnten noch deutlich allgemeiner definiert werden als wir es an dieser Stelle tun.

Definition 6.1.1. Sei S ein noethersches Schema. Ein Gruppenschema über S oder auch S -Gruppenschema ist ein S -Schema $\pi : G \rightarrow S$ zusammen mit S -Morphismen

$$\sigma_0 : S \rightarrow G, \quad i : G \rightarrow G, \quad \mu : G \times G \rightarrow G,$$

so dass die folgenden Diagramme kommutieren:

$$\begin{array}{ccc}
 & & G \times_S G \\
 & \nearrow \sigma_0 \times \text{id} & \downarrow \mu \\
 S \times_S G & \xrightarrow{p_2} & G
 \end{array}
 \qquad
 \begin{array}{ccc}
 & & G \times_S G \\
 & \nearrow \text{id} \times \sigma_0 & \downarrow \mu \\
 G \times_S S & \xrightarrow{p_1} & G
 \end{array}$$

$$\begin{array}{ccc}
 G \times_S G & \xrightarrow{\text{id} \times i} & G \times_S G \\
 \uparrow \text{diag} & & \downarrow \mu \\
 G & \xrightarrow{\pi} S \xrightarrow{\sigma_0} & G
 \end{array}
 \qquad
 \begin{array}{ccc}
 G \times_S G & \xrightarrow{i \times \text{id}} & G \times_S G \\
 \uparrow \text{diag} & & \downarrow \mu \\
 G & \xrightarrow{\pi} S \xrightarrow{\sigma_0} & G
 \end{array}$$

wobei $\text{diag} : G \rightarrow G \times_S G$ die Diagonaleinbettung ist.

$$\begin{array}{ccc}
 G \times_S G \times_S G & \xrightarrow{\mu \times \text{id}} & G \times_S G \\
 \text{id} \times \mu \downarrow & & \downarrow \mu \\
 G \times_S G & \xrightarrow{\mu} & G
 \end{array}$$

Kommutiert zusätzlich das Diagramm

$$\begin{array}{ccc} G \times_S G & \xrightarrow{\mu} & G \\ \text{twist} \downarrow & \nearrow \mu & \\ G \times_S G & & \end{array}$$

so nennen wir das Gruppenschema kommutativ. Hierbei ist $\text{twist} : G \times_S G \rightarrow G \times_S G$ die Vertauschung der Koordinaten. Ist G affin, so reden wir auch von einem affinen Gruppenschema.

Wir können zeigen, dass G genau dann ein S -Gruppenschema ist, wenn μ für alle S -Schemata T eine Gruppenstruktur auf $G(T)$ induziert. Im Folgenden beschränken wir uns auf affine S . Wir bezeichnen den Ring, dessen Spektrum S ist, wieder mit S und fordern, dass S noethersch und kommutativ mit 1 ist. Für viele Zwecke wird S sogar ein Körper sein. Für uns sind die folgenden Beispiele von besonderem Interesse.

1. Die additive Gruppe \mathbb{G}_a gegeben dadurch, dass jedes S -Schema T auf die additive Gruppe seiner globalen Schnitte abgebildet wird.
2. Die multiplikative Gruppe \mathbb{G}_m . Hier ist $\mathbb{G}_m(T)$ die multiplikative Gruppe der invertierbaren globalen Schnitte von T .
3. Die Gruppe der Wittvektoren W oder abgeschnittenen Wittvektoren W_m . Hierbei handelt es sich um eine Verallgemeinerung von \mathbb{G}_a gegeben durch $W(T)$ ist die additive Gruppe der Wittvektoren über den globalen Schnitten von T . Es gilt $\mathbb{G}_a \cong W_1$.
4. Jede elliptische Kurve A über S ist ein Beispiel für ein S -Gruppenschema. Das wird in [KM85, Thm 2.1.2] bewiesen.

Diese Gruppenschemata sind alle kommutativ und abgesehen von den elliptischen Kurven auch affin. Im Folgenden seien – wenn nichts anderes gesagt wird – alle Gruppenschemata kommutativ.

Definition 6.1.2. Wir nennen ein affines Gruppenschema $G = \text{Spec } A$ endlich und flach über S , wenn A ein lokal freier S -Modul von endlichem Typ ist.

Beispiele für endliche, flache Gruppenschemata, die für uns wichtig sind, sind die folgenden. Dabei ist T ein S -Schema.

1. Endliche konstante Gruppenschemata.
2. Die m -ten Einheitswurzeln μ_m gegeben durch $\mu_m(T) = \{a \in \mathbb{G}_m(T) \mid a^m = 1\}$.
3. Der Kern der Abbildung $\wp : W_m \rightarrow W_m, w \mapsto F(w) - w$ für S ein Körper der Charakteristik $p > 0$. Hierbei ist F der Morphismus, der auf $W_m(T)$ durch $(w_0, \dots, w_{m-1}) \mapsto (w_0^p, \dots, w_{m-1}^p)$ gegeben ist.
4. Das Schema \mathfrak{a}_p für Charakteristik S gleich p . Hierbei ist $\mathfrak{a}_p(T)$ der Kern der Abbildung $F : \mathbb{G}_a(T) \rightarrow \mathbb{G}_a(T), a \mapsto a^p$.
5. Der Kern einer Isogenie $\psi : A \rightarrow B$ zweier elliptischer Kurven über einem Körper K .

Definition 6.1.3. Sei $G = \text{Spec } A$ ein affines Gruppenschema über S . Die S -Morphismen

$$\sigma_0 : S \rightarrow G, \quad i : G \rightarrow G, \quad \mu : G \times G \rightarrow G,$$

korrespondieren zu S -Algebrenhomomorphismen

$$\varepsilon : A \rightarrow S, \quad \iota : A \rightarrow A, \quad \Delta : A \rightarrow A \otimes A$$

genannt Koeinheit, Koinverse und Komultiplikation. Analog zur Definition 6.1.1 lassen sie entsprechende Diagramme kommutieren. Wir bezeichnen A zusammen mit den Abbildungen ε, ι und Δ als die Hopfalgebra von G .

Es besteht eine Korrespondenz zwischen affinen Gruppenschemata und Hopfalgebren. Wir wollen das ausnutzen, um zum Beispiel die Isomorphie zweier Gruppenschemata zu beweisen, indem wir zeigen, dass ihre Hopfalgebren isomorph sind. Daher hier einige Beispiele.

1. Die Hopfalgebra des endlichen konstanten S -Gruppenschemas einer endlichen Gruppe Γ ist die Algebra S^Γ zusammen mit den Morphismen ε, ι und Δ gegeben durch $\varepsilon(v) = v_0, \iota(v)_\gamma = v_{-\gamma}$ und $\Delta(v)_{\gamma \otimes \gamma'} = v_{\gamma + \gamma'}$.
2. Das Gruppenschema der m -ten Einheitswurzeln über S hat $S[x]/(x^m - 1)$ zusammen mit $\varepsilon(x) = 1, \iota(x) = x^{m-1}$ und $\Delta(x) = x \otimes x$ als Hopfalgebra.
3. Für Charakteristik $S = p > 0$ ist $S[x]/(x^p)$ zusammen mit $\varepsilon(x) = 0, \iota(x) = -x$ und $\Delta(x) = 1 \otimes x + x \otimes 1$ die Hopfalgebra von \mathfrak{a}_p .

Definition 6.1.4. Für ein endliches, flaches Gruppenschema $G = \text{Spec } A$ sei A^D durch $A^D := \text{Hom}_S(A, S)$ definiert. Das Identifizieren von S^D mit S sowie $(A \otimes A)^D$ mit $A^D \otimes A^D$ und das Dualisieren der Ringmultiplikation $m : A \otimes A \rightarrow A$ und S -Algebrastruktur $u : S \rightarrow A$ von A zu $m^D : A^D \rightarrow A^D \otimes A^D$ und $u^D : A^D \rightarrow S$ macht aus A^D eine Hopfalgebra über S . Ihre S -Algebrastruktur ergibt sich dabei durch das Dualisieren der Koeinheit, Koinversen und Komultiplikation von A . Das zu A^D gehörige S -Gruppenschema nennen wir das Cartier-Duale von G und bezeichnen es mit G^D . Es gilt $(G^D)^D \cong G$.

Einfache Rechnungen zeigen, dass $\mathfrak{a}_p^D \cong \mathfrak{a}_p$ gilt. Des Weiteren sind das Cartier-Duale des endlichen, konstanten Gruppenschemas der zyklischen Gruppe mit m Elementen und die m -ten Einheitswurzeln isomorph. Für eine Isogenie $\psi : A \rightarrow B$ zweier elliptischer Kurven A und B über einem Körper K mit dualer Isogenie $\psi^\vee : B \rightarrow A$ gilt $\ker \psi \cong (\ker \psi^\vee)^D$. Diese Aussage findet sich zum Beispiel in [Mil08, I.9] mit Verweis auf [Oor66].

Definition 6.1.5. Für S -Gruppenschemata G_1, G_2 und G_3 wird ein Morphismus $G_1 \times G_2 \rightarrow G_3$ eine Paarung genannt, wenn für alle S -Schemata T die induzierte Abbildung $G_1(T) \times G_2(T) \rightarrow G_3(T)$ eine Paarung von Gruppen ist. Wir interessieren uns hier nur für Paarungen mit $G_3 = \mathbb{G}_m$. Ist $G_1 = G = \text{Spec } A$ ein affines, endliches, flaches Gruppenschema und $G_2 = G^D$ sein Cartier-Duales, dann existiert immer eine Paarung nach \mathbb{G}_m . Sie korrespondiert zu einem S -Algebrenhomomorphismus

$$S[x, x^{-1}] \rightarrow A \otimes A^D$$

Bemerkung 6.1.6. Die explizite Konstruktion solch einer Paarung wenn G der Kern einer Isogenie ist, wird in [KM85, 2.8] beschrieben. Wir bezeichnen sie auch als (verallgemeinerte) Weil-Paarung.

Wenn wir exakte Sequenzen kommutativer Gruppenschemata betrachten, dann behandeln wir diese als Garben von abelschen Gruppen für den flachen Situs. Nach [Mil80, II.1.7] oder [Sha63] ist das legitim. Daher verwenden wir dann auch die entsprechende Definition für Surjektivität. Beispielsweise ist für eine Isogenie $\psi : A \rightarrow B$ elliptischer Kurven über einem Körper K die Sequenz

$$0 \rightarrow \ker \psi \rightarrow A \rightarrow B \rightarrow 0 \quad (6.1.1)$$

von Garben exakt, obwohl die Sequenz

$$0 \rightarrow \ker \psi(K) \rightarrow A(K) \rightarrow B(K) \rightarrow 0$$

abelscher Gruppen im Allgemeinen nicht exakt ist. Siehe dazu auch [Mil80, II.2.15].

6.2 Kohomologie

Für eine separable Isogenie $\psi : A \rightarrow B$ zweier elliptischer Kurven A und B über einem Körper K ist

$$0 \rightarrow \ker \psi(K^{\text{sep}}) \rightarrow A(K^{\text{sep}}) \xrightarrow{\psi} B(K^{\text{sep}}) \rightarrow 0$$

eine kurze exakte Sequenz von G_K -Modulen. Sie induziert daher eine lange exakte Sequenz in Galoiskohomologie. Diese ist für $\psi = [n]$ ein wichtiges Hilfsmittel für den Beweis des schwachen Satzes von Mordell-Weil. Wir wollen solche induzierten Kohomologiesequenzen auch für inseparable Isogenien, wie zum Beispiel den Frobenius $F : A \rightarrow A^{(2)}$, verwenden. Dabei genügt die gewöhnliche Galoiskohomologie nicht mehr. Zum einen ist die Sequenz

$$0 \rightarrow \ker F(K^{\text{sep}}) \rightarrow A(K^{\text{sep}}) \xrightarrow{F} A^{(2)}(K^{\text{sep}}) \rightarrow 0$$

nicht exakt, da F auf $A(K^{\text{sep}})$ nicht surjektiv ist, zum anderen ist $\ker F(K')$ für alle Erweiterungskörper K' von K trivial, aber $\ker F$ als Gruppenschema nicht. Im vorherigen Abschnitt haben wir bereits gesehen, dass uns eine beliebige Isogenie eine exakte Sequenz liefert, wenn wir die elliptischen Kurven und den Kern als Garben abelscher Gruppen für den flachen Situs auffassen, siehe Sequenz 6.1.1. Wir müssen daher von einer allgemeineren Kohomologietheorie, die mit flachen Überdeckungen verträglich ist, Gebrauch machen. An dieser Stelle geben wir einen sehr kurzen Überblick über die von uns verwendeten Objekte und Aussagen. Für umfangreichere Informationen sei auf [Mil80], [Mil06], [Har77] und [Sha63] sowie die dort angegebenen Quellen verwiesen. Der von uns betrachteten Kohomologie liegt eine Grothendieck-Topologie zugrunde. Diese besteht bei uns aus der Kategorie der affinen, endlichen Schemata über einem Körper K zusammen mit der Überdeckung durch treue, flache Morphismen. Für eine Garbe G von abelschen Gruppen auf der Kategorie der endlichen, affinen K -Schemata – wobei wir uns auf solche Garben abelscher Gruppen, die von einem kommutativen K -Gruppenschema induziert sind, beschränken – können wir unter Benutzung abgeleiteter Funktoren Kohomologiegruppen definieren. Die i -te Kohomologiegruppe bezeichnen wir mit $H^i(K, G)$. Zur expliziten Berechnung solch

einer $H^i(K, G)$ bietet es sich oft an, mit Čech Kohomologie zu arbeiten. Diese wird im Detail in [Mil80, III.2], [Har77, III.4] und [Sha63, Abschnitt 2] beschrieben. Sie hat den Vorteil, dass wir die Elemente der Kohomologiegruppen – ähnlich wie bei der Galoiskohomologie – über Koketten, Kozykel und Koränder darstellen können. Elemente aus $H^i(K, G)$ besitzen auf diese Weise Repräsentanten in $G(\bar{K} \otimes \dots \otimes \bar{K})$, wobei das Tensorprodukt $i+1$ Faktoren beinhaltet. Wir sind hauptsächlich an den Kohomologiegruppen $H^i(K, G)$ für $i = 0, 1$ und G ein Gruppenschema interessiert. Dass die Čech Kohomologie in diesen Situationen mit der zuvor definierten Kohomologie $H^i(K, G)$ übereinstimmt, findet sich in [Mil80, III.2.10, III.4.5] und [Sha63, Thm. 1]. Wir nennen eine endliches flaches K -Gruppenschema G *étale*, wenn seine Hopfalgebra isomorph zu einem Produkt von separablen Körpererweiterungen von K ist. Das ist zum Beispiel für den Kern einer separablen Isogenie, für endliche konstante Gruppenschema, sowie die Einheitswurzeln μ_n und $\ker \varphi$ der Fall. Für solche Gruppenschemata stimmt die Čech Kohomologie mit der Galoiskohomologie überein, vergleiche [Mil06, Bemerkung III.6.12(b)] und [Sha72, S.208]. Da letztere gelegentlich einfacher zu berechnen ist, wechseln wir je nach Situation zwischen den beiden. Ausführliche Informationen über Galoiskohomologie finden sich in [Ser97]. Wollen wir hervorheben, dass wir mit Galoiskohomologie arbeiten, dann schreiben wir auch $H^i(G_K, G)$ oder $H^i(G_K, G(K^{\text{sep}}))$ für die entsprechenden Kohomologiegruppen.

In verschiedenen Situationen kann gezeigt werden, dass bestimmte Kohomologiegruppen trivial sind. Für uns sind dabei besonders die mit Satz Hilbert 90 bezeichneten Resultate relevant. Sie besagen, dass $H^1(K, G) = 0$ für $G = \mathbb{G}_m$ oder $G = W_m$ gilt.

Ist $0 \rightarrow G_1 \xrightarrow{\Psi_1} G_2 \xrightarrow{\Psi_2} G_3 \rightarrow 0$ eine kurze exakte Sequenz von Garben abelscher Gruppen auf der oben beschriebenen Kategorie, so induziert sie eine exakte Sequenz

$$0 \rightarrow G_1(K) \rightarrow G_2(K) \rightarrow G_3(K) \xrightarrow{\delta} H^1(K, G_1) \rightarrow H^1(K, G_2) \rightarrow H^1(K, G_3)$$

in Kohomologie (vergleiche [Mil80, III.4.5]). Hier verwenden wir die bekannte Gleichheit $H^0(K, G_i) = G_i(K)$. Siehe [Mil80, III.2]. Die Abbildung δ wird Verbindungshomomorphismus genannt und lässt sich über Čech Kozykel explizit beschreiben. Die anderen Abbildungen resultieren aus den durch die Morphismen der Garben Ψ_i induzierten Abbildungen der Koketten. Für $H^1(K, G_2) = 0$ liefert uns δ einen Isomorphismus $H^0(K, G_3)/\Psi_2(H^0(K, G_2)) \cong H^1(K, G_1)$. Im Hinblick auf Satz Hilbert 90 wollen wir das auf die exakten Sequenzen

$$\begin{aligned} 0 \rightarrow \mu_n \rightarrow \mathbb{G}_m &\xrightarrow{n} \mathbb{G}_m \rightarrow 0 \\ 0 \rightarrow \mathbb{Z}/p^m\mathbb{Z} \rightarrow W_m &\xrightarrow{p} W_m \rightarrow 0 \\ 0 \rightarrow \mathfrak{a}_p \rightarrow \mathbb{G}_a &\xrightarrow{F} \mathbb{G}_a \rightarrow 0 \end{aligned}$$

anwenden. Erstere wird auch Kummer-, zweite Artin-Schreier-Sequenz genannt.

Eine Paarung $G_1 \times G_2 \rightarrow G_3$ von K -Gruppenschemata wie zuvor beschrieben induziert eine Cup-Produkt-Paarung

$$H^r(K, G_1) \times H^s(K, G_2) \rightarrow H^{r+s}(K, G_3).$$

Sie lässt sich unter Verwendung von Čech-Kozykeln explizit auswerten, siehe [Sha63]. Wir interessieren uns dabei besonders für den Fall $r + s = 2$. Für $G_3 = \mathbb{G}_m$ und K einen lokalen Körper bildet die Cup-Produkt-Paarung dann nach $H^2(K, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$ ab. Siehe [Sha63, S.421].

6.3 Rechnungen und Beweise

In diesem Abschnitt geben wir einige Rechnungen und Beweise, die wir aus Gründen der Lesbarkeit im Hauptteil der Arbeit ausgelassen haben, an.

6.3.1 Rechnung zur V^m -Abstiegs-Abbildung

In Beweis von Lemma 1.3.4 behaupten wir, dass die Gleichheit

$$\Psi(Q - \sigma(Q)) = w - \sigma w$$

aus einer expliziten Rechnung folgt. An dieser Stelle geben wir sie nun an. Es sei der Punkt $P = (x_0, y_0) \in A(K)$ beliebig mit einem Urbild $Q = (x_2, y_2)$ unter V^2 und σ ein Erzeuger der Galoisgruppe von $K(Q)/K$. Habe $K(Q)$ den Grad 4 über K . Der Isomorphismus Ψ sei durch

$$\Psi : \ker V^2(K) \rightarrow W_2(\mathbb{F}_2), (a_1^2 a_6, a_1^6 s^4 a_6 + a_6^2) \mapsto (1, 1)$$

festgelegt. Formen wir die rationalen Funktionen, die V^2 beschreiben, um, so sehen wir, dass x_2 eine Nullstelle des Polynoms

$$(T^2 + a_1^4 a_6^2)^2 + a_1^2 a_6 (a_1^4 T)^2 + x_0 a_1^2 (T^2 + a_1^4 a_6^2) a_1^4 T$$

in $K[T]$ ist. Formales Faktorisieren zeigt uns, dass σ durch

$$\begin{aligned} x_2 \mapsto & \left(\frac{x_0 x_1}{a_6} + \frac{a_1^2 x_0^2}{a_6} + 1 \right) x_2 + \left(\frac{a_1^3 y_0}{x_0} + a_1^2 x_0 + a_1^4 s + a_1^4 \right) x_1 \\ & + a_1^5 y_0 + \frac{a_1^4 x_0^3 + (a_1^6 s + a_1^6) x_0^2 + a_1^4 a_6}{x_0} \end{aligned}$$

gegeben ist. Dann gilt

$$y_2 = \left(\frac{x_1(x_0 + a_1^2)}{x_0} + \frac{a_1^3 y_0}{x_0} + a_1^2 x_0 + a_1^4 s^4 + a_1^4 s + a_1^4 \right) x_2 + a_1^2 a_6 x_1 + a_1^4 a_6 x_0 + a_6^2$$

und

$$\begin{aligned} \sigma(y_2) = & \left(\left(\frac{a_1^3 y_0}{a_6} + \frac{(a_1^4 s^4 + a_1^4 s) x_0}{a_6} + 1 + \frac{a_1^2}{x_0} \right) x_1 + \frac{a_1^5 x_0 y_0}{a_6} + \frac{a_1^3 y_0}{x_0} + \frac{(a_1^6 s^4 + a_1^6 s) x_0^2}{a_6} \right. \\ & \left. + a_1^2 x_0 + a_1^4 s^4 + a_1^4 s + a_1^4 \right) x_2 + \left(\frac{(a_1^5 x_0 + a_1^7 s^4) y_0}{x_0} + (a_1^6 s^4 + a_1^6 s + a_1^6) x_0 \right. \\ & \left. + a_1^8 s^5 + a_1^8 s^4 + a_1^2 a_6 + \frac{a_1^4 a_6}{x_0} \right) x_1 + \frac{(a_1^7 x_0^2 + a_1^9 s^4 x_0 + a_1^5 a_6) y_0}{x_0} \\ & \left. + (a_1^8 s^4 + a_1^8 s + a_1^8) x_0^2 + (a_1^{10} s^5 + a_1^{10} s^4 + a_1^4 a_6) x_0 + a_1^6 s a_6 + a_6^2 + \frac{a_1^8 s^4 a_6}{x_0} \right. \end{aligned}$$

Das heißt, wir können die Koordinaten von Q und $\sigma(Q)$ als Elemente aus $K(x_2)$ schreiben. Für die linke Seite der obigen Gleichung erhalten wir

$$Q - \sigma(Q) = (x_2, y_2) - (\sigma(x_2), \sigma(y_2)) = (a_1^2 a_6, a_1^6 s^4 a_6 + a_6^2) \in \ker V^2(K)$$

In der gesamten Rechnung bezeichnet x_1 die x -Koordinate des Punkts $V(Q)$. Wir können die Komponenten eines Urbilds w von $\alpha_2(P)$ in x_2 ausdrücken und erhalten

$$w = \left(\frac{x_1}{a_1^2 x_0}, \frac{(x_1 + a_1^2 x_0)x_2}{a_1^6 a_6} + \frac{x_1(a_1 y_0 + x_0^2 + a_1^2 x_0(s+1))}{a_1^4 x_0^2} + \frac{y_0}{a_1 x_0} + \frac{x_0}{a_1^2} + s + \frac{a_6}{a_1^2 x_0^2} \right).$$

Anwenden von σ liefert

$$\sigma(w) = \left(\frac{x_1}{a_1^2 x_0} + 1, \frac{(x_1 + a_1^2 x_0)x_2}{a_1^6 a_6} + \left(\frac{y_0}{a_1^3 x_0^2} + \frac{1}{a_1^4} + \frac{s}{a_1^2 x_0} \right) x_1 + \frac{y_0}{a_1 x_0} + \frac{x_0}{a_1^2} + s + \frac{a_6}{a_1^2 x_0^2} \right).$$

Die Berechnung von

$$w - \sigma(w) = (1, 1)$$

beendet den Beweis. Für die Fälle $[K(Q) : K] = 2$ und $[K(Q) : K] = 1$ gehen wir analog vor.

6.3.2 Rechnung zur Hopfalgebra von $\ker F$ und $\ker V$

Bei der Konstruktion der F - und V -Abstiegs-Abbildung für eine supersinguläre elliptische Kurve A in Abschnitt 1.3.4.2 fassen wir $\ker F$ und $\ker V$ als endliche flache Gruppenschemata auf. In einigen Schritten arbeiten wir mit ihren Hopfalgebren. An dieser Stelle geben wir die Rechnungen an, die wir zuvor weggelassen haben. Sei im Folgenden also A durch die Gleichung $y^2 + a_3 y + x^3 + a_4 x + a_6 = 0$ über einem Körper K der Charakteristik 2 gegeben und bezeichne $F : A \rightarrow A^{(2)}$ den Frobenius.

Lemma 6.3.1. *Die Hopfalgebra von $\ker F$ ist isomorph zur Hopfalgebra von \mathfrak{a}_2 .*

Beweis. Wir zeigen zunächst die Isomorphie der Algebren. Wie in 6.3.3 gezeigt, liegt $\ker F$ in dem affinen Teil von A , der durch die Weierstraß-Gleichung in x - z -Koordinaten gegeben ist. In diesen Koordinaten ist $(0, 0)$ der Nullpunkt und der Frobenius durch

$$(x, z) \mapsto (x^2, z^2)$$

definiert. Daher ist der Koordinatenring von $\ker F$ isomorph zu

$$K[x, z]/(z^2 + a_3 z + x^3 + a_4 x z^2 + a_6 z^3, x^2, z^2)$$

Die drei Relationen $z^2 + a_3 z + x^3 + a_4 x z^2 + a_6 z^3 = 0$, $x^2 = 0$, $z^2 = 0$ implizieren $z = 0$. Folglich ist der Koordinatenring von $\ker F$ isomorph zu $K[x]/(x^2)$ unter der Isomorphie

$$x \mapsto x, z \mapsto 0.$$

Wir zeigen nun, dass diese Isomorphie mit der Koeinheit, der Koinversen und der Komultiplikation verträglich ist. Diese sind für \mathfrak{a}_2 durch $\varepsilon(x) = 0$, $\iota(x) = x$ und $\Delta(x) = 1 \otimes x + x \otimes 1$ gegeben. Da die Elemente von $\ker F(S)$ für alle affinen K -Schemata S selbstinvers sind und aufgrund der Koordinaten des Nullpunkts, ist unser Isomorphismus mit Koeinheit und Koinversen verträglich. Für die Verträglichkeit mit der Komultiplikation verwenden wir die bei [LR87] auf Seite 110 unter $(Z^{(2)})$ angegebene Formel, um zu zeigen, dass die x -Koordinate der Summe zweier Punkte aus $\ker F(S)$ gleich der Summe der x -Koordinaten ist. \square

Bemerkung 6.3.2. *Mit einer analogen Rechnung finden wir einen Isomorphismus zwischen den Hopfalgebren von $\ker V$ und \mathfrak{a}_2 .*

Der Isomorphismus $\ker F \rightarrow \mathfrak{a}_2$ induziert auch einen Isomorphismus der ersten Kohomologiegruppen $H^1(K, \ker F) \rightarrow H^1(K, \mathfrak{a}_2)$. Wir verwenden ihn bei der Konstruktion einer F -Abstiegs-Abbildung.

Lemma 6.3.3. *Die Abbildung*

$$\beta_1 : A^{(2)}(K) \rightarrow K/K^2, (x, y) \mapsto 1/a_3^2 x.$$

ist die gesuchte F -Abstiegs-Abbildung.

Beweis. Wir wissen bereits, dass eine Isomorphie $K/K^2 \cong H^1(K, \mathfrak{a}_2)$ unter der Abbildung $a \mapsto 1 \otimes b + b \otimes 1$ mit $b^2 = a$ besteht. Weiterhin wissen wir, dass die Randabbildung $\delta_F : A^{(2)}(K) \rightarrow H^1(K, \ker F)$ durch $\delta_F(P) = (1 \otimes x_Q, 1 \otimes y_Q) - (x_Q \otimes 1, y_Q \otimes 1)$ für ein $Q = (x_Q, y_Q) \in A(\bar{K})$ mit $F(Q) = P$ bestimmt ist. Verketteten wir nun diese Homomorphismen mit der zuvor konstruierten Isomorphie von $H^1(K, \ker F)$ nach $H^1(K, \mathfrak{a}_2)$, so erhalten wir β_1 mit den gewünschten Eigenschaften. Es verbleibt zu zeigen, dass β_1 durch die angegebene rationale Funktion beschrieben ist. Dazu verwenden wir das Gruppengesetz in der in [LR87, Theorem 2.2] beschriebenen Form, um das Bild von $\delta_F(P)$ als Kozykel in $\ker F(\bar{K} \otimes \bar{K})$ in x - z -Koordinaten zu beschreiben. Von dem resultierenden Element nehmen wir die x -Koordinate, die in $\bar{K} \otimes \bar{K}$ liegt, und schreiben sie in der Form $1 \otimes b + b \otimes 1$. Wir erhalten

$$1 \otimes b + b \otimes 1 = 1 \otimes (1/a_3 x_Q) + (1/a_3 x_Q) \otimes 1$$

Dann ist $b^2 = 1/a_3^2 x_Q^2 = 1/a_3^2 x_P$ das Bild von $P = (x_P, y_P)$ unter β_1 . \square

Bemerkung 6.3.4. *Auf dieselbe Weise bekommen wir eine explizite Beschreibung der V -Abstiegs-Abbildung α_1 . Die Rechnungen verlaufen analog.*

6.3.3 Auswertung der Weil-Paarung

Wie schon in Abschnitt 6.1 angegeben, sind für eine Isogenie $\psi : A \rightarrow B$ zweier elliptischer Kurven über einem Körper K der Kern von ψ und der Kern von ψ^\vee endliche flache Gruppenschemata und $\ker \psi^\vee$ ist isomorph zum Cartier-Dual $(\ker \psi)^D$ des Kerns von ψ . Cartier-Dualität induziert eine Paarung von $\ker \psi \times \ker \psi^\vee$ in das multiplikative Gruppenschema \mathbb{G}_m . Wir wollen an dieser Stelle angeben, wie sich die Paarung – im Folgenden als Weil-Paarung bezeichnet – für $\psi = F$ den Frobenius zwischen den supersingulären elliptischen Kurven A und $A^{(2)}$ auswerten lässt. Das liefert uns die fehlenden Details für den Beweis von Aussage 1.3.10. Die an dieser Stelle angegebene Konstruktion hält sich eng an die Vorlagen [KM85, 2.8] und [Oda69, Abschnitt 1]. Bis zu dem Punkt, an dem wir konkrete Rechnungen angeben, bleiben die Überlegungen korrekt, wenn wir statt F eine beliebige Isogenie verwenden. Sei $S = \text{Spec } R$ ein affines Schema mit R eine endliche K -Algebra. Für unsere Zwecke genügen solche Schemata S , im Allgemeinen kommt man mit deutlich schwächeren Anforderungen an S aus. Durch einen Basiswechsel fassen wir A und $A^{(2)}$ als elliptische Kurven über S auf und schreiben A/S bzw. $A^{(2)}/S$, wenn wir das hervorheben wollen. Die Nullpunkte bezeichnen wir jeweils mit \mathcal{O} bzw. \mathcal{O}' . Da die elliptischen Kurven eigentlich und glatt über K sind, sind sie es nach [Har77, II.4.8] und [Har77, III.10.1] auch nach dem Basiswechsel. Seien nun $P \in \ker F$ und $P' \in \ker F^\vee$ beliebige aber feste S -rationale Punkte. Nach der Konstruktion der dualen Isogenie – siehe [Oor66, I.5] – gilt: Der Punkt P' liegt im Kern von F^\vee genau dann, wenn das Bild des Cartier-Divisor $(P' - \mathcal{O}')$ in der

relativen Picardgruppe $\text{Pic}(A^{(2)}/S)$ im Kern von $F^* : \text{Pic}(A^{(2)}/S) \rightarrow \text{Pic}(A/S)$ liegt. Hierbei verwenden wir, dass wir Punkte in $A^{(2)}/S(S)$ nach [KM85, 1.2.7] als effektive Cartier-Divisoren auffassen können. Wir verwenden runde Klammern um Divisoren zu kennzeichnen. Nach [Oda69, S.66] kommutiert das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Pic}(S) & \longrightarrow & \text{Pic}(A) & \longrightarrow & \text{Pic}(A/S) \longrightarrow 0 \\ & & \uparrow \text{id} & & \uparrow F^* & & \uparrow F^* \\ 0 & \longrightarrow & \text{Pic}(S) & \longrightarrow & \text{Pic}(A^{(2)}) & \longrightarrow & \text{Pic}(A^{(2)}/S) \longrightarrow 0 \end{array}$$

Hierbei bezeichnet $\text{Pic}(A)$ die Picardgruppe von A als Kurve über S und $\text{Pic}(A/S)$ die relative Picardgruppe bezüglich S . Mit F^* bezeichnen wir die von F induzierte Abbildung sowohl auf den absoluten, als auch auf den relativen Picardgruppen. Wir sehen direkt, dass $\text{Pic}(A^{(2)}/S) \simeq \text{Pic}(A^{(2)})/\text{Pic}(S)$ gilt. Wir können $(P' - \mathcal{O}')$ also als ein Element von $\text{Pic}(A^{(2)})$ auffassen, das nur modulo $\text{Pic}(S)$ eindeutig bestimmt ist. Das Element $(P' - \mathcal{O}')$ liegt im Kern von F^* auf $\text{Pic}(A^{(2)}/S)$, durch geeignete Modifikation modulo $\text{Pic}(S)$ liegt es auch aufgefasst als Element von $\text{Pic}(A^{(2)})$ im Kern von F^* . Daher können wir annehmen, dass die zu $F^*(P' - \mathcal{O}') \in \text{Pic}(A)$ korrespondierende Idealgarbe $I(F^*(P' - \mathcal{O}'))$ von einem globalen Schnitt g des absoluten Quotientenrings von A/S erzeugt wird. Folgen wir nun [Oda69, S.67], so sehen wir, dass die Translation mit P einen Automorphismus τ_P des absoluten Quotientenrings liefert. Die Kette von Isomorphismen auf Seite 67 bei [Oda69] besagt, dass $(g \circ \tau_P)/g = (\tau_P^* g)/g$ einen $\mathcal{O}_{A/S}$ -Isomorphismus von $\mathcal{O}_{A/S}$ darstellt. Dieser entspricht der Multiplikation mit einem globalen Schnitt von $\mathcal{O}_{A/S}^\times$ und das ist nach Oda ein globaler Schnitt von \mathcal{O}_S^\times , also ein Element aus R^\times .

Wir wollen nun g in unserer Situation bestimmen. Dazu überdecken wir $A^{(2)}$ durch die affinen Teile

$$U'_0 = \text{Spec } B'_0 \text{ und } U'_\infty = \text{Spec } B'_\infty$$

mit

$$B'_0 = R[x, z]/(z + a_3^2 z^2 + x^3 + a_4^2 x z^2 + a_6^2 z^3)$$

und

$$B'_\infty = R[1/x, z/x]/(z/x^3 + a_3^2 z^2/x^3 + 1 + a_4^2 (z/x)^2 + a_6^2 (z/x)^3).$$

Um zu zeigen, dass U'_0 und U'_∞ eine Überdeckung von $A^{(2)}/S$ bilden, betrachten wir die Situation zunächst für $A^{(2)}/K$ mit affinen Teilen

$$V'_0 = \text{Spec } C'_0 \text{ und } V'_\infty = \text{Spec } C'_\infty$$

mit

$$C'_0 = K[x, z]/(z + a_3^2 z^2 + x^3 + a_4^2 x z^2 + a_6^2 z^3)$$

und

$$C'_\infty = K[1/x, z/x]/(z/x^3 + a_3^2 z^2/x^3 + 1 + a_4^2 (z/x)^2 + a_6^2 (z/x)^3).$$

Wir betrachten Abbildungen

$$v'_0 : V'_0(\bar{K}) \rightarrow A^{(2)}(\bar{K}), (x, z) \mapsto (x : 1 : z)$$

und

$$v'_\infty : V'_\infty(\bar{K}) \rightarrow A^{(2)}(\bar{K}), (r, s) \mapsto \begin{cases} (1/r : 1 : s/r) & \text{für } r \neq 0 \\ (1 : 0 : s) & \text{sonst.} \end{cases}$$

Es ist offensichtlich, dass alle \bar{K} -rationalen Punkte von V'_0 durch v'_0 auf \bar{K} -rationale Punkte auf $A^{(2)}$, beschrieben durch projektive Koordinaten, abgebildet werden. Für v'_∞ unterscheiden wir zwei Fälle. Ist $(r, s) \in V'_\infty(\bar{K})$ mit $r \neq 0$, dann impliziert

$$sr^2 + a_3s^2r + 1 + a_4s^2 + a_6s^3 = 0$$

die Gleichheit

$$(s/r)(1/r) + a_3(s/r)^2 + (1/r)^3 + a_4(s/r)^2(1/r) + a_6(s/r)^3 = 0$$

und $(1/r : 1 : s/r)$ ist somit ein Punkt auf $A^{(2)}$. Für $r = 0$ gilt die Gleichheit

$$1 + a_4s^2 + a_6s^3 = 0.$$

Dann ist aber auch $(1 : 0 : s)$ ein Punkt auf $A^{(2)}$. Sei nun umgekehrt ein beliebiger Punkt Q auf $A^{(2)}$ gegeben. Wir beschreiben ihn durch projektive Koordinaten $(x_Q : y_Q : z_Q)$ und abhängig davon ob $y_Q = 0$ ist, finden wir ein Urbild auf V'_∞ oder V'_0 . Für R eine endliche K -Algebra ist $S \rightarrow \text{Spec } K$ ein treuer flacher Morphismus. Durch einen Basiswechsel mit S werden V'_∞ und V'_0 zu U'_∞ und U'_0 . Da V'_∞ und V'_0 eine Überdeckung von $A^{(2)}/K$ ist, liefert U'_∞ und U'_0 eine Überdeckung von $A^{(2)}/S$. Siehe [Mil80, Bemerkung II.1.1 (3)]. Alternativ können wir auch den obigen Beweis anpassen. Die Fallunterscheidungen darüber, ob ein Element gleich null ist oder nicht, werden zu Fallunterscheidungen ob ein Element ein Nullteiler ist oder nicht. Die Punkte auf $A^{(2)}/S(S)$, deren x -Koordinate ein Nullteiler ist, besitzen kein Urbild in U'_∞ . Zusammen mit der folgenden Beschreibung der Punkte im Kern von F^\vee sehen wir, dass die Überdeckung so gewählt ist, dass $\ker F^\vee$ in U'_0 liegt. Der Schnitt von $\ker F^\vee$ und U'_∞ ist trivial. Daher gilt

$$I(P')(U'_\infty) = I(\mathcal{O}')(U'_\infty) = B'_{\text{infty}fty}.$$

Der Punkt \mathcal{O}' kann auf U'_0 mit den affinen x - z -Koordinaten $\mathcal{O}' = (0, 0)$ geschrieben werden. Ebenso lässt sich P' auf U'_0 durch $P' = (a, b)$ mit a und b in R schreiben. Da er im Kern der Verschiebung liegt und sich diese, weil A supersingulär ist, in die Verknüpfung des Frobenius mit einem Isomorphismus aufspalten lässt, gilt $a^2 = 0$ und $b^2 = 0$. Einsetzen in die definierende Gleichung für U'_0 liefert uns $b = 0$. Somit ist das Ideal $I(\mathcal{O}')(U'_0)$ von x und z und das Ideal $I(P')(U'_0)$ von $x + a$ und z erzeugt. Nun überdecken wir A durch die affinen Teile

$$U_0 = \text{Spec } B_0 \text{ und } U_\infty = \text{Spec } B_\infty$$

mit

$$B_0 = R[x, z]/(z + a_3z^2 + x^3 + a_4xz^2 + a_6z^3)$$

und

$$B_\infty = R[1/x, z/x]/(z/x^3 + a_3z^2/x^3 + 1 + a_4(z/x)^2 + a_6(z/x)^3).$$

Wir können Ideale auf U'_0 und U'_∞ mit F^* zurückziehen, indem wir die Erzeuger mit F verknüpfen. Dafür verwenden wir, dass nach [KM85, S.6] Zurückziehen mit der Idealbildung kommutiert. Auf diese Weise erhalten wir auf U_∞ wieder jeweils das von 1 erzeugte Ideal. Für $I(F^*(P'))(U_0)$ bekommen wir Erzeuger $x^2 + a$ und z^2 , für $I(F^*(\mathcal{O}'))(U_0)$ die Erzeuger x^2 und z^2 . Eine kurze Rechnung zeigt uns, dass das inverse Ideal von $I(F^*(\mathcal{O}'))(U_0)$ ein $k[x]$ -Erzeugendensystem $1, z, \frac{a_6z^2 + (a_4x + a_3)z + 1}{x^2}$ besitzt.

Multiplizieren der Erzeuger zeigt uns, dass $I(F^*(P' - \mathcal{O}'))(U_\infty)$ das Einheitsideal ist, und liefert uns ein Erzeugendensystem für $I(F^*(P' - \mathcal{O}'))(U_0)$. Zwischen diesen Erzeugern bestehen Relationen. Entfernen wir alle überflüssigen, so erhalten wir das $k[x]$ -Erzeugendensystem z , z^2 und $1 + a(a_6(z/x)^2 + a_4(z/x) + a_3(z/x^2) + 1/x^2)$. Das Element $g := 1 + a(a_6(z/x)^2 + a_4(z/x) + a_3(z/x^2) + 1/x^2)$ liegt auch in $I(F^*(P' - \mathcal{O}'))(U_\infty)$. Wir behaupten, es erzeugt $I(F^*(\mathcal{O}'))(U_0)$ und $I(F^*(\mathcal{O}'))(U_\infty)$. Dazu sehen wir $g^2 = 1$, somit erzeugt g das Einheitsideal auf U_∞ . Weiterhin gilt

$$g^{-1}z = gz = \frac{zx^2 + a(a_6z^3 + a_4xz^2 + a_3z^2 + z)}{x^2} = \frac{zx^2 + ax^3}{x^2} = z + ax.$$

Also handelt es sich auch bei den Erzeugern von $I(F^*(\mathcal{O}'))(U_0)$ um $k[x, z]$ -Vielfache von g und somit ist g der gesuchte globale Schnitt. Sei nun $P \in \ker F(S)$. Nach obigen Überlegungen ist P in x - z -Koordinaten von der Form $P = (c, 0)$ mit $c \in R$, $c^2 = 0$. Sei $X = (x, z)$ ein weiterer Punkt in x - z -Koordinaten. Dann gilt

$$X + P = (a_6cz^2 + c + x, a_4cz^2 + cx^2 + z)$$

wie eine Rechnung mit den rationalen Funktionen, die das Gruppengesetz in x - z -Koordinaten beschreiben, zeigt. Wir berechnen damit $g(X + P)/g(X)$. Unter Verwendung von $a^2 = c^2 = 0$ erhalten wir

$$g(X + P)/g(X) = a_3ac + 1.$$

Das Ergebnis ist, wie schon bei [Oda69] angegeben, unabhängig von der Wahl von X und liegt in $\mu_2(S) \subset \mathbb{G}_m(S)$. Zusammengefasst haben wir die folgende Aussage bewiesen.

Lemma 6.3.5. *Sei S ein endliches affines K -Schema und seien $P \in \ker F(S)$ und $P' \in \ker V(S)$ für F und V der Frobenius und die Verschiebung der supersingulären elliptischen Kurven A und $A^{(2)}$ über dem Körper K . Ist A durch die projektive Weierstraß-Gleichung*

$$A : y^2z + a_3yz^2 + x^3 + a_4xz^2 + a_6z^3$$

und sind $P = (x, z)$ und $P' = (x', z')$ in x - z -Koordinaten gegeben, so nimmt die Weil-Paarung ausgewertet an P und P' den Wert $1 + a_3xx'$ an.

Bemerkung 6.3.6. *Die Aussage gilt für einen beliebigen Körper K . Für unsere Zwecke sind dabei globale Körper und ihre lokalen Vervollständigungen von besonderem Interesse.*

Curriculum Vitae

Gerriet Möhlmann

E-Mail: moehlman@math.tu-berlin.de

Geburtsdatum: 10.8.1982

Familienstatus: ledig

Staatsangehörigkeit: deutsch

Wissenschaftlicher Werdegang

seit 2009 Wissenschaftlicher Mitarbeiter an der Technischen Universität Berlin

2003 – 2008 Diplom in Mathematik an der Technischen Universität Berlin

April 2008 Diplomarbeit über Einbettungen globaler Funktionenkörper (Betreuer Florian Heß)

Akademische Aktivitäten

März 2011 Forschungsaufenthalt an der Universität von Debrecen

Mai 2010 Sage Days über Funktionenkörper

Februar 2009 Forschungsaufenthalt in der MAGMA Gruppe in Sydney

Literaturverzeichnis

- [Ban04] BANDINI, A.: *Three-descent and the Birch and Swinnerton-Dyer conjecture*. Rocky Mountain J. Math., 34:13–27, 2004.
- [BCP97] BOSMA, W., J. CANNON und C. PLAYOUST: *The Magma algebra system I: The user language*. J. Symbolic Comp., 24, 3/4:235–265, 1997.
- [BK77] BRUMER, A. und K. KRAMER: *The rank of elliptic curves*. Duke Mathematical Journal, 44(4):715–743, 1977.
- [Bro97] BROUMAS, A.: *Effective p -descent*. Compositio Mathematica, 107(2):125–141, 1997.
- [BSD63] BIRCH, B. J. und H. P. F. SWINNERTON-DYER: *Notes on elliptic curves. I*. J. Reine angew. Math., 212:7–25, 1963.
- [BSD65] BIRCH, B. J. und H. P. F. SWINNERTON-DYER: *Notes on elliptic curves. II*. J. Reine angew. Math., 218:79–108, 1965.
- [CFO⁺] CREMONA, J. E., T. A. FISHER, C. O’NEIL, D. SIMON und M. STOLL: *Explicit n -descent on elliptic curves. III. Algorithms*. Submitted, Preprint available under <http://arxiv.org/pdf/1107.3516.pdf>.
- [CFO⁺08] CREMONA, J. E., T. A. FISHER, C. O’NEIL, D. SIMON und M. STOLL: *Explicit n -descent on elliptic curves. I. Algebra*. J. Reine Angew. Math., 615:121–155, 2008.
- [CFO⁺09] CREMONA, J. E., T. A. FISHER, C. O’NEIL, D. SIMON und M. STOLL: *Explicit n -descent on elliptic curves. II. Geometry*. J. Reine Angew. Math., 632:63–84, 2009.
- [CFS10] CREMONA, J. E., T. A. FISHER und M. STOLL: *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*. Algebra Number Theory, 4(6):763–820, 2010.
- [CP09] COHEN, H. und F. PAZUKI: *Elementary 3-descent by 3-isogeny*. Acta Arith., 140:369–404, 2009.
- [CR03] CREMONA, J. E. und D. RUSIN: *Efficient solution of rational conics*. Math. Comp., 72(243):1417–1441 (electronic), 2003.
- [Cre] CREMONA, J. E.: *mwrnk Program*. Available under <http://homepages.warwick.ac.uk/staff/J.E.Cremona/mwrnk/>.

- [Cre97] CREMONA, J. E.: *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 2. Auflage, 1997.
- [Cre06] CREMONA, JOHN: *The elliptic curve database for conductors to 130000*. In: *Algorithmic number theory*, Band 4076 der Reihe *Lecture Notes in Comput. Sci.*, Seiten 11–29. Springer, Berlin, 2006.
- [Cre10] CREUTZ, B.: *Explicit Second p -Descent on Elliptic Curves*. PhD Thesis, Jacobs University Bremen, 2010.
- [DS98] DJABRI, Z. und N. P. SMART: *A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve*. In: J. BUHLER (Herausgeber): *Proceedings of the Third Symposium on Algorithmic Number Theory, ANTS-III*, LNCS 1423, Seiten 502–513, Portland, Oregon, 1998. Springer-Verlag, Berlin-Heidelberg-New York.
- [Elk00] ELKIES, N. D.: *Rational Points Near Curves and Small Nonzero $|x^3 - y^2|$ via Lattice Reduction*. In: W. BOSMA (Herausgeber): *Proceedings of the Fourth Symposium on Algorithmic Number Theory, ANTS-IV*, LNCS 1838, Seiten 33–64, Leiden, Netherlands, 2000. Springer-Verlag, Berlin-Heidelberg-New York.
- [FGP13] FIEKER, C., I. GAAL und M. POHST: *On computing integral points of a Mordell curve over rational function fields in characteristic > 3* . *J. Number Th.*, 131:738–750, 2013.
- [Fie97] FIEKER, C.: *Über relative Normgleichungen in algebraischen Zahlkörpern*. PhD Thesis, Technische Universität Berlin, 1997.
- [Fis00] FISHER, T.: *On 5 and 7 descent for elliptic curves over \mathbb{Q}* . PhD Thesis, University of Cambridge, 2000.
- [Fis08] FISHER, T.: *The invariants of a genus one curve*. *Proc. Lond. Math. Soc.*, 97:753–782, 2008.
- [FV93] FESENKO, I. B. und S. V. VOSTOKOV: *Local Fields and Their Extensions*. American Mathematical Society, New York, 1993.
- [GPZ94] GEBEL, J., A. PETHŐ und H. ZIMMER: *Computing integral points on elliptic curves*. *Acta Arith.*, 68(2):171–192, 1994.
- [Gre69] GREENBERG, M. J.: *Lectures on Forms in many Variables*. Benjamin, New York, 1969.
- [Har77] HARTSHORNE, R.: *Algebraic Geometry*. Springer-Verlag, Berlin-Heidelberg-New York, 1977.
- [Haz09] HAZEWINKEL, M.: *Handbook of Algebra VI*. North-Holland, Amsterdam, 2009.
- [Hes99] HESS, F.: *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. PhD Thesis, Technische Universität Berlin, 1999.
- [Hes02] HESS, F.: *Computing Riemann-Roch spaces in algebraic function fields and related topics*. *J. Symbolic Comp.*, 33(4):425–445, 2002.

- [Ker09] KERN, D.: *S-ganze Punkte auf elliptischen Kurven*. Diplomarbeit, Technische Universität Berlin, 2009.
- [KM85] KATZ, N. M. und B. MAZUR: *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, Princeton, 1985.
- [Koh96] KOHEL, D. R.: *Endomorphism rings of elliptic curves over finite fields*. PhD Thesis, University of California, Berkeley, 1996.
- [Kra77] KRAMER, K.: *Two-descent for elliptic curves in characteristic two*. Trans. Amer. Math. Soc., 232:279–295, 1977.
- [Lan78] LANG, S.: *Elliptic Curves Diophantine Analysis*. Springer-Verlag, Berlin-Heidelberg-New York, 1978.
- [Lan83] LANG, S.: *Fundamentals of Diophantine Geometry*. Springer-Verlag, Berlin-Heidelberg-New York, 1983.
- [Lan02] LANG, S.: *Algebra*. 3rd edition, GTM 211. Springer-Verlag, Berlin-Heidelberg-New York, 2002.
- [LN59] LANG, S. und A. NÉRON: *Rational points of abelian varieties over function fields*. Amer. J. Math., 81:95–118, 1959.
- [Lor90] LORENZ, F.: *Einführung in die Algebra Teil 2*. B.I. Wissenschaftsverlag, Mannheim/Wien/Zürich, 1990.
- [LR87] LANGE, H. und W. RUPPERT: *Addition Laws on Elliptic Curves in Arbitrary Characteristics*. J. Algebra, 107:106–116, 1987.
- [Mil80] MILNE, J.S.: *Etale Cohomology*. Princeton University Press, Princeton, 1980.
- [Mil06] MILNE, J.S.: *Arithmetic Duality Theorems*. BookSurge, LLC, zweite Auflage, 2006.
- [Mil08] MILNE, JAMES S.: *Abelian Varieties (v2.00)*, 2008. Available at www.jmilne.org/math/.
- [Mil13] MILNE, J.S.: *Class Field Theory (v4.02)*, 2013. Available at www.jmilne.org/math/.
- [MSS96] MERRIMAN, J., N. P. SMART und S. SIKSEK: *Explicit 4-descents on an elliptic curve*. Acta Arithmetica, 77(4):385–404, 1996.
- [Mum70] MUMFORD, D.: *Abelian Varieties*. Oxford University Press, Oxford, 1970.
- [Oda69] ODA, T.: *The first de Rham cohomology group and Dieudonné modules*. Annales Scientifiques de l'É.N.S., 2:63–135, 1969.
- [Oor66] OORT, F.: *Commutative group schemes*. Springer-Verlag, Berlin-Heidelberg-New York, 1966.
- [OT70] OORT, F. und J. TATE: *Group Schemes of prime order*. Ann. Sci. Ec. Norm. Super., 3:1–21, 1970.

- [PS97] POONEN, B. und E. F. SCHAEFER: *Explicit descent for Jacobians of cyclic covers of the projective line*. J. Reine angew. Math., 488:141–188, 1997.
- [PZ97] POHST, M. E. und H. ZASSENHAUS: *Algorithmic Algebraic Number Theory*. Cambridge University Press, Cambridge, 1st paperback Auflage, 1997.
- [Rob07] ROBERTS, D.: *Explicit Descent On Elliptic Curves Over Function Fields*. PhD Thesis, University of Nottingham, 2007.
- [Sad09] SADEK, M.: *Models of genus one curves*. PhD Thesis, Fitzwilliam College, Cambridge, 2009.
- [Sal06] SALVADOR, G. D. VILLA: *Topics in the Theory of Algebraic Function Fields*. Birkhäuser Verlag, Basel, 2006.
- [Sch96] SCHÖRNIG, M.: *Untersuchung konstruktiver Probleme in globalen Funktionenkörpern*. PhD Thesis, Technische Universität Berlin, 1996.
- [Ser79] SERRE, J. P.: *Local Fields*. Springer-Verlag, Berlin-Heidelberg-New York, 1979.
- [Ser97] SERRE, J. P.: *Galois cohomology*. Springer-Verlag, Berlin-Heidelberg-New York, 1997.
- [Sha63] SHATZ, S.: *Cohomology of Artinian Group Schemes Over Local Fields*. Annals of Mathematics, 79(3):411–449, 1963.
- [Sha67] SHATZ, S.: *The cohomology of certain elliptic curves over local and quasi-local fields*. Illinois J. Math., 11(2):234–241, 1967.
- [Sha72] SHATZ, S.: *Profinite Groups, Arithmetic, and Geometry*. Princeton University Press, Princeton, 1972.
- [Sha86] SHATZ, S.: *Group Schemes, Formal Groups and p -Divisible Groups*. In: J. H. SILVERMAN, G. CORNELL & (Herausgeber): *Arithmetic Geometry*, Seiten 29–78, Storrs, Connecticut, 1986. Springer-Verlag, Berlin-Heidelberg-New York.
- [Shi99] SHIODA, T.: *Mordell-Weil lattices for higher genus fibration*, 1999. New Trends in algebraic geometry.
- [Sik95] SIKSEK, S.: *Descent on curves of genus 1*. PhD Thesis, University of Exeter, 1995.
- [Sil86] SILVERMAN, J. H.: *The Arithmetic of Elliptic Curves*. Springer-Verlag, Berlin-Heidelberg-New York, 1986.
- [Sil90] SILVERMAN, J. H.: *The difference between the Weil height and the canonical height on elliptic curves*. Math. Comp., 55:723–743, 1990.
- [Sil94] SILVERMAN, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, Berlin-Heidelberg-New York, 1994.
- [Sim98] SIMON, D.: *Equations dans les corps de nombres et discriminants minimaux*. PhD Thesis, Université Bordeaux, 1998.

- [Sim02] SIMON, D.: *Computing the Rank of Elliptic Curves over Number Fields*. LMS J. Comput. Math., 5:7–17, 2002.
- [Soo13] SOOMRO, M. A.: *Algebraic curves over finite fields*. PhD Thesis, Rijksuniversiteit Groningen, 2013.
- [SS97] SIKSEK, S. und N. P. SMART: *On the complexity of computing the 2-Selmer group of an elliptic curve*. Glasgow Math. J., 39:251–258, 1997.
- [SS04] SCHAEFER, E. F. und M. STOLL: *How to do a p -descent on an elliptic curve*. Trans. Amer. Math. Soc., 356:1209–1231, 2004.
- [Sta05] STAMMINGER, S.: *Explicit 8-descent on elliptic curves*. PhD Thesis, International University Bremen, 2005.
- [Sti93] STICHTENOTH, H.: *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin-Heidelberg-New York, 1993.
- [Tat52] TATE, J.: *Genus Change in inseparable Extensions of Function Fields*. American Mathematical Society, 3(3):400–406, 1952.
- [Tho05] THOMAS, L.: *Ramification groups in Artin-Schreier-Witt extensions*. J. Theor. Nombres Bordx., 17:689–720, 2005.
- [Ulm91] ULMER, D.: *p -descent in characteristic p* . Duke Math. Journal, 62:237–265, 1991.
- [Ulm02] ULMER, D.: *Elliptic curves with large rank over function fields*. Annals of Mathematics, 155:295–315, 2002.
- [Ulm04] ULMER, D.: *Elliptic Curves and Analogies Between Number Fields and Function Fields*. In: *Heegner Points and Rankin L-Series*, Seiten 285–315, 2004.
- [Ulm09] ULMER, D.: *Elliptic curves over function fields*. Notes on a lecture course at the Park City Math Institute. Available under <http://people.math.gatech.edu/~ulmer/research/papers/2011.pdf>, 2009.
- [Ulm13] ULMER, D.: *On Mordell-Weil groups of Jacobians over function fields*. Journal of the Institute of Mathematics of Jussieu, 12:1–29, 2013.
- [vHC06] HOEIJ, M. VAN und J. E. CREMONA: *Solving conics over function fields*. J. Théor. Nombres Bordeaux, 18(3):595–606, 2006.
- [Vil] VILLEGAS, F. R. Available at <http://www.ma.utexas.edu/cnt/cnt-frames.html>.
- [Vol90] VOLOCH, J. F.: *Explicit p -descent for elliptic curves in characteristic p* . Compositio Math., 74:247–258, 1990.
- [vS91] SCHMETTOW, J. GRAF v.: *Beiträge zur Klassengruppenberechnung*. PhD Thesis, Heinrich-Heine Universität Düsseldorf, 1991.

- [Wat79] WATERHOUSE, W.: *Introduction to Affine Group Schemes*. Springer-Verlag, Berlin-Heidelberg-New York, 1979.
- [Wil97] WILDANGER, K.: *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve*. PhD Thesis, Technische Universität Berlin, 1997.
- [Wom03] WOMACK, T.: *Explicit Descent on Elliptic Curves*. PhD Thesis, University of Nottingham, 2003.