Über Torsionspunkte elliptischer und hyperelliptischer Kurven nebst Anwendungen

vorgelegt von
Diplom-Mathematiker
Andreas M. Schöpp
aus Lebach

Von der Fakultät II - Mathematik und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades
Doktor der Naturwissenschaften
– Dr. rer. nat. –
genehmigte Dissertation.

Berlin 2005
D 83

Promotionsausschuss

Vorsitzender:	Prof. Dr. Fredi Tröltzsch, Technische Universität Berlin
Berichter:	Prof. Dr. Michael E. Pohst, Technische Universität Berlin
Berichter:	Prof. Dr. Franck Leprévost, Université du Luxembourg

Tag der wissenschaftlichen Aussprache: 02. Dezember 2005

Inhaltsverzeichnis

Einleitung **v**

1 Elliptische Kurven **1**
1.1 Gruppengesetz . . . 1
1.2 Isogenien . . . 5
1.2.1 Der Endomorphismenring . . . 6
1.3 Torsion elliptischer Kurven . . . 7
1.3.1 Kubert-Kurven . . . 10

2 Hyperelliptische Kurven **13**
2.1 Die Jacobische Varietät . . . 13
2.1.1 Addition in $J_{\mathcal{C}}(K)$ . . . 17
2.1.2 Berechnung von Hauptdivisoren . . . 18
2.2 Torsion hyperelliptischer Kurven . . . 25
2.2.1 Bekanntes und Vermutungen . . . 26
2.2.2 Die Polynomgleichung . . . 31
2.2.3 Kurvenfamilien . . . 34

3 Zahlentheoretische Anwendungen **47**
3.1 Zahlkörper mit Galoisgruppe D_l . . . 47
3.1.1 Allgemeine Konstruktion . . . 47
3.1.2 Konstruktion der Polynome . . . 49
3.1.3 Arithmetik für Zahlkörper vom Grad 4 . . . 57
3.1.4 Arithmetik für Zahlkörper vom Grad 5 . . . 63
3.1.5 Arithmetik für Zahlkörper vom Grad 6 . . . 79
3.2 Zahlkörper mit Galoisgruppe C_l . . . 81
3.2.1 Allgemeine Situation . . . 81
3.2.2 Indikatorfunktionen . . . 82
3.2.3 Quotientenkurven nach Vélu . . . 84
3.2.4 Punkte auf Quotientenkurven . . . 86
3.3 Zahlkörper mit Galoisgruppe $D_{l/2}$ . . . 96

3.4 Zahlkörper mit großem l-Rang . . . 101

A Quotientenkurvenberechnung nach Vélu **109**

B D_l und C_l mit $l = 9, 10, 12$ **113**
B.1 Fall $l = 9$ . . . 113
B.2 Fall $l = 10$ . . . 117
B.3 Fall $l = 12$ . . . 120

C Exakte Formeln zur Arithmetik im Grad 5 **127**
C.1 Nullstelle $\varrho^{(2)}$ . . . 128
C.2 Nullstelle $\varrho^{(4)}$ . . . 130

D Kurven: geometrisch und zahlentheoretisch **135**
D.1 Algebraische Funktionenkörper . . . 135
D.2 Algebraische Kurven . . . 138
D.2.1 Affine Varietäten . . . 138
D.2.2 Projektive Varietäten . . . 139
D.2.3 Kurven und Funktionenkörper . . . 142
D.2.4 Abbildungen zwischen Kurven . . . 144
D.2.5 Divisoren . . . 145
D.3 Modulkurven . . . 147
D.3.1 Elliptische Kurven über $\mathbb{C}$ . . . 148
D.3.2 $Y_0(N)$ und $X_0(N)$ . . . 150
D.3.3 Gleichungen von $X_0(N)$ über $\mathbb{Q}$ . . . 153
D.3.4 Weitere Modulkurven . . . 155

Symbolverzeichnis **157**

Index **161**

Literaturverzeichnis **165**

Zusammenfassung **173**

Einleitung

Elliptische Kurven sind Gegenstand zahlreicher Studien sowohl in algebraischer Geometrie als auch in Zahlentheorie seit über einhundert Jahren. Inzwischen gibt es eine umfangreiche Literatur zu diesem Thema, wobei stellvertretend auf die Bücher von Silverman [86, 87] verwiesen sei. Ursprünglich widmete man sich diesem Gebiet aus rein theoretischem Interesse, was sich aber in den letzten zwanzig Jahren grundlegend geändert hat, so dass heute elliptische Kurven vor allem mit Anwendungen verschiedenster Art in Verbindung gebracht werden:

- 1986: Public-Key-Kryptographie (Koblitz, Miller)[1]
- 1987: Fehlerkorrigierende Codes (Driencourt/Michon)[2]
- 1987: Pseudo-Zufallszahlen-Generator (Kaliski)[3]
- 1987: Primzahltest (Goldwasser/Kilian)[4]
- 1987: Faktorisierung ganzer Zahlen (Lenstra)[5]

Insbesondere die Idee der Nutzung elliptischer Kurven zu Verschlüsselungszwecken hat eine große Aufmerksamkeit seitens der Wissenschaft, der Wirtschaft und auch der Öffentlichkeit zur Folge gehabt. Die in diesem Zusammenhang verwendeten Algorithmen waren nicht neu: Diffie-Hellman-Schlüsselaustausch, El-Gamal-Verschlüsselung, Authentifizierungs- und Signaturalgorithmen basierten auf allgemeinen zyklischen Gruppen mit großer Primzahlordnung; bis dahin wurde in diesen Algorithmen meist die multiplikative Gruppe eines endlichen Körpers genutzt, ab jetzt auch die Punkte auf einer elliptischen Kurve, die eine Gruppe bilden.

Die Sicherheit der Verschlüsselung beruht dabei in beiden Fällen (endliche Körper, elliptische Kurven) auf dem mathematisch schweren Problem des diskreten Logarithmus. Die Verschlüsselung mit elliptischen Kurven (ECC) hatte im Vergleich zum grundlegend anderen genutzten Verfahren (RSA) den Vorteil deutlich kürzerer Schlüssel bei gleicher Sicherheit: 512 Bit ECC stehen 15316 Bit RSA gegenüber, so dass für die Schlüssel weniger Speicherkapazität benötigt wird, was elliptische Kurven interessant macht und für die Implementierung z. B. auf Smartcards prädestiniert. Schnell stellte man jedoch fest, dass nicht alle elliptischen Kurven gleiche Sicherheit garantieren: mittels Weil-Pairing konnte das diskrete Logarithmusproblem von der elliptischen Kurve über einem endlichen Körper $\mathbb{F}_q$ nach $\mathbb{F}_{q^k}^\times$ übertragen werden, was sogenannte supersinguläre Kurven angreifbar machte, da diese einen kleinen Erweiterungsgrad k zur Folge hatten. Insgesamt trieb das große Interesse der Wissenschaftler die Kenntnis über elliptische Kurven immens

voran, so dass entsprechende Kryptographiesysteme rentable Wirtschaftsunternehmen (siehe Certicom, Cryptovision) entstehen ließen. Darüber hinaus ist die Verschlüsselung mit elliptischen Kurven so sicher, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Nutzung entsprechender Systeme für die Public-Key-Verschlüsselung empfiehlt.[6]

Die Verschlüsselung mittels elliptischer Kurven geschieht mit einer Kurve über einem endlichen Körper $\mathbb{F}_q$. Grundlegend ist dabei die Bestimmung der Punktgruppenordnung, da diese zur Gewährleistung der Sicherheit einen großen Primfaktor besitzen muss. Man kann umgekehrt auch eine passende Primzahl wählen und dazu eine elliptische Kurve (über einem geeigneten Körper $\mathbb{F}_q$) konstruieren. Ändert man den Grundkörper von $\mathbb{F}_q$ nach $\mathbb{C}$ (klassische Geometrie) oder nach $\mathbb{Q}$ bzw. einem algebraischen Zahlkörper K (Gegenstand dieser Arbeit), so tauchen sofort andere Fragen auf, z. B. die nach Rang und Torsion einer gegebenen Kurve.

Mordell und Weil haben sich vor rund 80 Jahren dieser Fragen angenommen und die wichtige Erkenntnis formuliert, dass die Punktgruppe einer elliptischen Kurve über K endlich erzeugt ist. Die Wissenschaft ist jedoch weit entfernt, diese Fragen umfassend beantwortet zu haben: nachdem die Torsion über $\mathbb{Q}$ theoretisch (Mazur) und konstruktiv (Kubert) und über einem quadratischen Zahlkörper theoretisch (Kamienny) beschrieben wurde, ist man aktuell dabei, kubische Zahlkörper zu untersuchen (Jeon, Kim und Schweizer). Zum Rang gibt es jedoch selbst über $\mathbb{Q}$ keine allgemeine Aussage. Jedoch gibt es Algorithmen, die bei einer gegebenen Kurve Rang und Torsion (über $\mathbb{Q}$) i.A. berechnen können. Gegenstand weiterer Untersuchungen sind der Führer einer elliptischen Kurve, Punkte mit kleiner kanonischer Höhe und Punkte mit großen ganzzahligen Koeffizienten.

Hyperelliptische Kurven sind auf Grund ihrer komplexeren Struktur bei weitem nicht so ausführlich beschrieben wie elliptische Kurven. Die meisten Erkenntnisse in diesem Gebiet umfassen abstrakte Existenzaussagen, aus denen Anwendungen wie bei elliptischen Kurven und sogar Algorithmen zur Untersuchung einer einzelnen gegebenen Kurve nicht abgeleitet werden können. Zentral bei der gesamten Betrachtung ist die Divisorenklassengruppe einer Kurve, die sogenannte Jacobische Varietät. In Analogie zu elliptischen Kurven werden die Divisorenklassen häufig Punkte und die Jacobische Varietät Punktgruppe einer hyperelliptischen Kurve genannt. Verwechslungen mit den eigentlichen Punkten (Koordinatentupeln) einer solche Kurve können dabei nicht auftreten, da letztere keine Gruppe bilden.

Basierend auf der Jacobischen Varietät einer hyperelliptischen Kurve wurden

auch hier Anwendungen vorgeschlagen:

- 1989: Public-Key-Kryptographie (Koblitz)[7]
- 1991: Fehlerkorrigierende Codes (Le Brigand)[8]
- 1992: Primzahltest (Adleman und Huang)[9]
- 1993: Faktorisierung ganzer Zahlen (Lenstra, Pila und Pomerance)[10]

Eine potentielle kryptographische Nutzung hyperelliptischer Kurven hatte wie bei elliptischen Kurven eine rege Forschung zur Folge, die wesentliche Vorteile bei z. B. Geschlecht 2 im Vergleich zu Geschlecht 1 (elliptische Kurven) sah:[11] die Punktgruppe (Jacobische Varietät) über $\mathbb{F}_q$ hat etwa q^2 Elemente im Gegensatz zu q Elementen (bei $g = 1$), und die komplexe Arithmetik in der Jacobischen Varietät ermöglichte eine höhere Sicherheit bei gleicher Schlüssellänge. Andererseits stellte sich schnell heraus, dass die Verschlüsselung mit Kurven ab Geschlecht $g = 4$ wieder an Sicherheit einbüßte und die Konstruktion geeigneter Kurven (schon bei $g = 2$) viel aufwändiger ist. Ist eine hyperelliptische Kurve nicht über $\mathbb{F}_q$ sondern über $\mathbb{Q}$ oder über einem Zahlkörper K gegeben, gilt auch hier die Aussage, dass die Punktgruppe endlich erzeugt ist. Wieder beschäftigt sich die Theorie mit der Torsionsuntergruppe und dem Rang der Kurve; hier kommt jedoch auf Grund der Unterscheidung von Kurve und Jacobischer Varietät (bei elliptischen Kurven stimmen beide überein) noch die Frage nach Punkten auf der Kurve selbst hinzu. Faltings hat bewiesen, dass es nur endlich viele K-rationale Punkte auf einer Kurve gibt. Wie Torsionsuntergruppe und Rang aussehen können, ist hingegen unbekannt, aber es gibt einen Algorithmus zur Bestimmung der Torsionsgruppe bei einer gegebenen Kurve vom Geschlecht $g = 2$.

Ausgangspunkt dieser Arbeit ist die Suche nach hyperelliptischen Kurven vom Geschlecht $g = 2$ über $\mathbb{Q}$ mit einem Punkt der Ordnung $l = 11$, da dies der erste Fall möglicher Torsion ist, der bei einer elliptischen Kurve über $\mathbb{Q}$ nicht auftritt. Es wurde konkret nach einer Familie entsprechender Kurven $(g = 2, l = 11)$ gesucht, die $X_0(23)$: $y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$ bzw. $y^2 = (x^3 - x + 1)(x^3 + 4x^2 + 7x + 5)$ enthalten, da eine solche Kurvenschar bisher nicht bekannt ist. Hilfsmittel bei dieser Suche war eine Polynomgleichung, in der die Grade der Polynome durch das Geschlecht g und die Torsion l festgelegt sind. Es gelang, neue unendliche Familien hyperelliptischer Kurven mit bestimmter Torsion $(l = 5, 7, 10)$ zu konstruieren, in denen sich gewisse Modulkurven $X_0(N)$ $(N = 29, 31, 41)$ wiederfinden. Eine Familie, in der sich die Kurve $X_0(23)$ wiederfindet, konnte auf Grund computertechnischer Beschränkungen nicht gefunden werden, denn die Auswertung der Polynomgleichung wird bei steigender Torsion deutlich aufwändiger.

Ausgehend von den konstruierten Familien hyperelliptischer Kurven wurden umfangreiche Rechnungen angestellt, um imaginärquadratische Zahlkörper mit großem 5- bzw. 7-Rang zu finden. Dies führte zu 49 bzw. 67 unveröffentlichten Zahlkörpern mit 5-Rang 3 bzw. 7-Rang 2.

Während der Beschäftigung mit der Torsion hyperelliptischer und elliptischer Kurven rückte eine Idee von Odile Lecacheux ins Zentrum der Untersuchung: mit Hilfe eines l-Torsionspunktes einer parametrisierten Familie von elliptischen Kurven ($3 \leq l \leq 10, l = 12$) wurden parametrisierte Zahlkörper vom Grad l über $\mathbb{Q}$ konstruiert, deren Galoisgruppe die Diedergruppe D_l mit $2l$ Elementen ist.[12] Die erzeugenden Polynome dieser Körper sind kürzer als entsprechende bisher bekannte, in einer Datenbank der Universität Kassel veröffentlichte Polynome.[13] Bei der Konstruktion wurde auch die generische Polynomfamilie von Brumer gefunden, die unabhängig von ihm auch von Darmon beschrieben worden ist.[14]

Naheliegenderweise schloss sich die Frage nach Unterfamilien mit zyklischer Galoisgruppe an, die detailliert bearbeitet wurde. Dabei konnten Familien für $l = 3, 4, 5, 6$ gefunden werden; u.a. die Familie *einfachster kubischer Körper* von Shanks und *einfachster quartischer Körper* von Gras.[15] In einem letzten Schritt wurde die Arithmetik der gefundenen D_l-Familien mit besonderer Beachtung der Einheitengruppe untersucht: für $l = 5$ konnten parametrisierte Fundamentaleinheiten bei Signatur $(1, 2)$ angegeben werden, was bisher für komplexe Einbettungen in der Literatur keine Entsprechung hat.

Diese Arbeit hat zu drei Artikeln geführt, die im Folgenden LPS1 [48], LPS2 [49] und LPS3 [50] genannt werden.

Die Gliederung dieser Arbeit besteht aus drei Kapiteln und einem vierteiligen Anhang: Im ersten Kapitel werden einige Aussagen zu elliptischen Kurven ausgeführt und insbesondere die Formeln zum Gruppengesetz und die Gleichungen parametrisierter elliptischer Kurven, wie Kubert sie konstruiert hat, angegeben. Beides wird im dritten Kapitel ausführlich genutzt.

In Kapitel 2 werden hyperelliptische Kurven erläutert. Dabei wird insbesondere auf die Punktgruppe eingegangen. Zentral ist hierbei die Berechnung von Hauptdivisoren hyperelliptischer Kurven mit zwei Punkten im Unendlichen. Anschließend wird der aktuelle Wissensstand der Forschung bzgl. der Torsion hyperelliptischer Kurven über $\mathbb{Q}$ vorgestellt, und mit Hilfe einer Polynomgleichung werden Kurvenfamilien mit Torsion $l = 5, 7, 10$ konstruiert, die die Modulkurven $X_0(29), X_0(31)$ und $X_0(41)$ enthalten.

Das dritte Kapitel befasst sich anfangs mit der Konstruktion von Zahlkörperfamilien, deren Galoisgruppe die Diedergruppe D_l ist. Die Konstruktion basiert auf einem Torsionspunkt der Ordnung l einer parametrisierten Familie elliptischer Kurven. Für die Fälle $l = 4, 5$ werden bei Signatur $(2, 1)$ und $(1, 2)$ Systeme von parametrisierten Fundamentaleinheiten bestimmt. Im Fall $l = 5$ mit einer reellen Einbettung werden zum Beweis der Fundamentalität der Einheiten Abschätzungen der komplexen Nullstellen des erzeugenden Polynoms benötigt, die mit Hilfe eines Satzes von Obreschkoff gewonnen werden. Für die Fälle $l = 3, 4, 5, 6$ werden Unterfamilien der Zahlkörperfamilien bestimmt, deren Galoisgruppe jeweils die zyklische Gruppe C_l ist. Dazu werden Indikatorfunktionen untersucht, was – wie sich herausstellt – äquivalent dazu ist, parametrisierte Punkte auf gewissen elliptischen Kurven (Quotientenkurven) zu finden. Diese Untersuchung wird auch für die $D_{l/2}$ durchgeführt. Den Abschluss des Kapitels bildet die Untersuchung der konstruierten Familien hyperelliptischer Kurven mit einem Torsionspunkt der Ordnung $l = 5, 7$ im Hinblick auf imaginärquadratische Zahlkörper mit großem l-Rang. Gefunden wurden dabei unveröffentlichte Zahlkörper mit 5-Rang 3 und 7-Rang 2.

Im vierteiligen Anhang der Arbeit werden in den Teilen A, B und C umfangreiche Formeln für die erwähnten Betrachtungen angegeben: die Ideen und Methoden der Berechnungen sind dabei schon an den entsprechenden Stellen in der Arbeit zu finden, während die Ausdrücke dort auf das Wesentliche reduziert sind. Hier sind sie zur Exaktheit und Nachvollziehbarkeit ausführlich aufgeschrieben. Im vierten Teil D des Anhangs werden die in Kapitel 1 und 2 auftretenden Begriffe so erklärt, dass auch mit geringem zahlentheoretischen Wissen ein Zugang zu dieser Arbeit möglich wird; dabei wird versucht, die unterschiedlichen Betrachtungsweisen von Kurven (geometrisch: Varietäten $\leftrightarrow$ zahlentheoretisch: Funktionenkörper) zusammenzuführen.

Ausblick: Eine Weiterführung der Konstruktion hyperelliptischer Kurven mit vorgegebener Torsion erscheint möglich, insbesondere die Bestimmung einer Familie, die $X_0(23)$ enthält. Für weitere Familien (mit großer Torsion) scheint es sinnvoll, die Herangehensweise zu modifizieren, wie es in Satz 2.2.17 (Pell-Gleichung) anklingt: Ergebnisse aus ähnlichen Fragestellungen sind auszunutzen, die in anderen Zusammenhängen erzielt wurden. Im Rahmen dieser Arbeit wurde die Literatur zum Thema *Einheitenberechnung in quadratischen Zahlkörpern* untersucht[16]; weitere Untersuchungen erscheinen sinnvoll.

Im Zusammenhang mit der Konstruktion von Zahlkörperfamilien mit Galoisgruppe D_l ist die Fortführung der Methode auf größere Körpergrade leicht

möglich, wenn z. B. parametrisierte Kurvengleichungen über einem quadratischen Zahlkörper ausgenutzt werden (vgl. Kamienny). Dabei könnten neue Familien für $l = 11, 13, 14, 15, 16, 18$ gefunden werden. Da aber schon die Polynome für $l = 10$ und $l = 12$ recht unübersichtlich sind, liefert die Weiterführung dieser Konstruktion voraussichtlich umfangreiche Ausdrücke.

Die gefundenen Zahlkörperfamilien besitzen vom Galois-Standpunkt aus interessante Verzweigungsdaten[17], so dass eine entsprechende Untersuchung der Familien in Ergänzung der hier durchgeführten arithmetischen Berechnungen sich zu lohnen scheint.

---

[1] Koblitz, Neal: Elliptic curve cryptosystems, in: *Math. Comput* 48, 1987, 203–209.
Miller, Victor S.: Use of elliptic curves in cryptography, in: Williams, Hugh C. (Hrsg.): *Advances in cryptology - CRYPTO V, 1985*, (Lect. Notes Comput. Sci. 218), Springer 1986, 417–426.

[2] Driencourt, Yves; Michon, Jean Francis: Elliptic codes over fields of characteristic 2, in: *J. Pure Appl. Algebra* 45, 1987, 15–39.

[3] Kaliski, Burton S.jun.: A pseudo-random bit generator based on elliptic logarithms, in: Odlyzko, Andrew M. (Hrsg.): *Advances in cryptology - CRYPTO VI, 1986*, (Lect. Notes Comput. Sci. 263), Springer 1987, 84–103.

[4] Goldwasser, Shafi; Kilian, Joe: Almost all primes can be quickly certified, in: *18. Annual ACM Symposium on Theory of Computing 1986*, (Journal of computer and system sciences 38.1), Acad. Press 1989, 316–329.

[5] Lenstra, Hendrik W.jun.: Factoring integers with elliptic curves, in: *Ann. Math. Ser. II*, 126, 1987, 649–673.

[6] http://www.bsi.de/projekte/edat62/

[7] Koblitz, Neal: Hyperelliptic cryptosystems, in: *J. Cryptology* 1.3, 1989, 139–150.

[8] Le Brigand, Dominique: Decoding of codes on hyperelliptic curves, in: Cohen, Gérard (Hrsg.): *EUROCODE '90*, (Lect. Notes Comput. Sci. 514), Springer 1991, 126–134.

[9] Adleman, Leonard M.; Huang, Ming-Deh A.: *Primality testing and Abelian varieties over finite fields*, (Lecture Notes in Mathematics 1512), Springer 1992.

[10] Lenstra, Hendrik W.jun.; Pila, Jonathan; Pomerance, Carl: A hyperelliptic smoothness test. I, in: *Philos. Trans. R. Soc. Lond., Ser. A* 345.1676, 1993, 397–408.

[11] Siehe Literaturverzeichnis: Spallek.

[12] Die Polynome sind unter folgender Web-Adresse zu finden:
http://www.math.tu-berlin.de/~kant/publications/papers/polynomes.txt

[13] Die Datenbank der Universität Kassel findet sich auf der Homepage:
http://www.mathematik.uni-kassel.de/~klueners/minimum/minimum.html

[14] Brumers Familie wurde von D. Martinais und L. Schneps zitiert; siehe Literaturverzeichnis: Martinais.
Darmon, Henri: Une famille de polynômes liées à $X_0(5)$, *unveröffentlichte Notizen*, 1993.

[15] Siehe Literaturverzeichnis: Shanks bzw. Gras.

[16] Nordhoff, Heinz-Uwe: *Explizite Darstellungen von Einheiten und ihre Anwendung auf Mehrklassigkeitsfragen bei reell-quadratischen Zahlkörpern*, Inaugural-Dissertation, Köln 1974, Satz 2.2, Seite 28 liefert 2 Kurven vom Geschlecht 2 mit einer Divisorenklasse der Ordnung 5: $(x^3 + 4x^2 + 5x + 3)(x^3 + x - 1)$ und $(x^3 + 4x^2 + 3x - 3)(x^3 - x + 1)$.

[17] Private Kommunikation am 09.08.2004 mit Jürgen Klüners.

Ich danke Herrn Prof. Dr. Michael E. Pohst ganz herzlich für die Aufnahme in seine Arbeitsgruppe, für die Möglichkeit, zu jedem Zeitpunkt mit Fragen zu ihm zu kommen, und für die vielen Erfahrungen, die ich durch ihn und durch die Mitarbeit in seiner Arbeitsgruppe machen durfte.

Ich danke Prof. Dr. Franck Leprévost besonders herzlich für die Überlassung des Themas dieser Arbeit, die große Geduld, die er mit mir und meinen Fragen hatte, und die viele Zeit, die er mir schenkte, egal ob er in Berlin, Grenoble oder Luxembourg war.

Ich danke den Mitgliedern der KANT-Gruppe der TU Berlin und insbesondere Dr. Robert Fraatz, José Mendez und Dr. Sebastian Pauli für die Hinweise bei der Erstellung dieser Arbeit.

Kapitel 1

Elliptische Kurven

Ein Hauptpunkt in der Theorie algebraischer Kurven und damit sowohl elliptischer als auch hyperelliptischer Kurven ist die in Abschnitt D.2 erläuterte Jacobische Varietät einer Kurve, die im Gegensatz zu beliebigen Varietäten eine algebraische Gruppe ist. Bei der Untersuchung dieser Gruppe stellen sich u.a. Fragen nach der Gruppenstruktur, nach -erzeugern und -arithmetik. In allen diesen Punkten sind elliptische Kurven (und deren Jacobische Varietäten) auf Grund der geringeren Komplexität besser erforscht als hyperelliptische Kurven.

Die Ausführungen in diesem Kapitel zu elliptischen Kurven (diese werden mit E bzw. E/K bezeichnet) dienen der Erläuterung der in dieser Arbeit benötigten Begriffe. Dabei wird auf Themenkomplexe, die die vorliegende Arbeit nicht berührt, im Hinblick auf bessere Übersicht nicht weiter eingegangen. Eine detaillierte Einführung in das Thema findet sich z. B. in Silverman [86].

1.1 Gruppengesetz

Elliptische Kurven E sind algebraische Kurven vom Geschlecht 1, die einen ausgezeichneten Punkt $\mathcal{O}$ besitzen.[1] Der Zugang zur Jacobischen Varietät J_E einer solchen Kurve ist besonders einfach, denn es existiert folgende Isomorphie.

[1] Wird von einer elliptischen Kurve E gesprochen, so ist diese immer als über $\bar{K}$ definiert zu verstehen, wobei $\bar{K}$ der algebraische Abschluss eines algebraischen Zahlkörpers K ist.

Satz 1.1.1 (Silverman, [86], III.3.4). *Ist E eine elliptische Kurve, so besteht folgender Isomorphismus:*

$$E \simeq J_E, \quad P \mapsto [P - \mathcal{O}].$$

Dieser Satz erhellt den einfachen Zugang zur Jacobischen Varietät einer elliptischen Kurve: Man braucht keine Divisoren vom Grad 0 und deren Nebenklassen bzgl. der Hauptdivisoren zu untersuchen, sondern untersucht die Punkte der Kurve selbst. Somit stellen sich zunächst die Fragen, wie Punkte auf einer elliptischen Kurve berechnet werden können und wie sich das Gruppengesetz der formalen Gruppe der Divisoren auf die Punkte überträgt.

Die Grundlage zur ersten Frage beinhaltet der folgende Satz:

Satz 1.1.2 (Hindry/Silverman [27], A.4.4). *Sei E/K eine über einem perfekten Körper K definierte elliptische Kurve mit einem K-rationalen Punkt $P \in E(K)$. Dann ist E isomorph zu einer über K definierten glatten Kurve der (homogenen) Form*

$$E \quad : \quad y^2\,z + a_1\,x\,y\,z + a_3\,y\,z^2 = x^3 + a_2\,x^2\,z + a_4\,x\,z^2 + a_6\,z^3,$$

mit $a_i \in K$ für $i = 1, 2, 3, 4, 6$, wobei P durch die existierende Isomorphie auf den Punkt $\mathcal{O} = (0 : 1 : 0)$ abgebildet wird.

Auch die Umkehrung des Satzes gilt (siehe Silverman [86], III.3.1): Ist E/K eine glatte Kurve in obiger Form mit $a_i \in K$, so ist E/K eine elliptische Kurve mit ausgezeichnetem Punkt $\mathcal{O} = (0 : 1 : 0)$.[2] Die oben angegebene Gleichung einer elliptischen Kurve heißt (lange) **Weierstraßgleichung**. Ist die Charakteristik von K ungleich $2, 3$ (z. B. bei einem algebraischen Zahlkörper K), so kann E/K sogar auf eine (kurze) Weierstraßform $y^2\,z = x^3 + a\,x\,z^2 + b\,z^3$ mit $a, b \in K$ transformiert werden.

Die Berechnung von Punkten auf einer elliptischen Kurve besitzt mit diesen Gleichungen einen Ausgangspunkt. Generell handelt es sich dabei um kein einfaches Problem, welches jedoch im Zusammenhang mit dieser Arbeit nicht weiter ausgeführt zu werden braucht. Details dazu finden sich z. B. in Silverman [86], Kapitel IX und X.

[2] Die Umkehrung des Satzes kann wie folgt erweitert werden: Ist $\mathrm{char}(K) \neq 2$, ist $f \in K[x]$ ein Polynom vom Grad 4 ohne doppelte Nullstellen und besitzt $E : y^2 = f(x)$ einen K-rationalen Punkt, so ist E/K eine über K definierte elliptische Kurve.

Unerlässlich für spätere Ausführungen ist die Beantwortung der Frage, wie sich das Gruppengesetz der formalen Gruppe der Divisoren auf die Punkte der Kurve überträgt.

Satz 1.1.3 (Silverman [86], III.2.1 + III.3.4). *Durch folgende geometrische Methode wird ein Gruppengesetz $\oplus$ auf den Punkten einer elliptischen Kurve E definiert:*

Seien $P, Q \in E$ und sei $\mathcal{V}$ die Linie, die P und Q verbindet.[3] *Sei R der dritte Punkt im Schnitt von $\mathcal{V}$ und E und sei $\mathcal{V}'$ die Linie, die R mit $\mathcal{O}$ verbindet (d.h. $\mathcal{V}'$ verläuft parallel zur y-Achse). Dann ist $P \oplus Q$ der dritte Punkt im Schnitt von $\mathcal{V}'$ und E. Damit ist $(E, \oplus)$ eine abelsche Gruppe mit neutralem Element $\mathcal{O}$.*

Dieses geometrische Gruppengesetz entspricht mittels der Abbildung $P \mapsto [P - \mathcal{O}]$ genau der formalen Addition in der Jacobischen Varietät J_E.

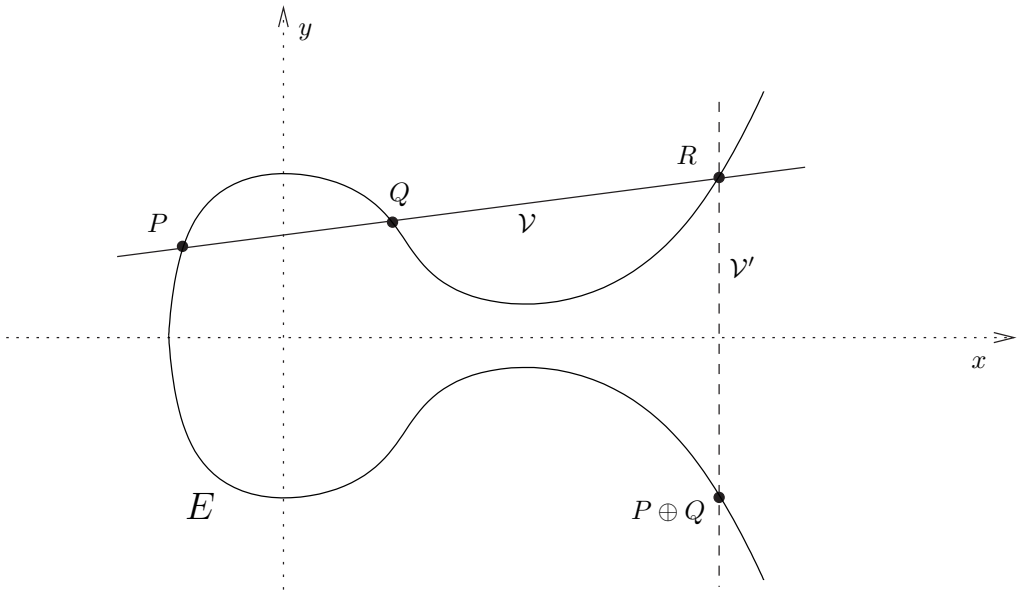

Abbildung 1.1: Geometrisches Additionsgesetz auf einer elliptischen Kurve E über $\mathbb{R}$

Eine algorithmische Version des Gruppengesetzes auf einer elliptischen Kurve lautet wie folgt:

[3] Ist $P = Q$, so sei $\mathcal{V}$ die Tangente an diesen Punkt.

Korollar 1.1.4 (Silverman [86], III.2.3). *Sei*

$$E \quad : \quad y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$$

eine elliptische Kurve (in affiner Form) und seien $P_1 = (x_1, y_1)$ *und* $P_2 = (x_2, y_2)$ *zwei endliche Punkte von* E*. Dann gelten folgende Formeln zur Punktaddition* $P_1 \oplus P_2$*:*

(*i*) $-P_1 = (x_1, -y_1 - a_1\,x_1 - a_3)$.

(*ii*) *Falls* $x_1 = x_2$ *und* $y_1 + y_2 + a_1\,x_2 + a_3 = 0$*, dann* $P_1 \oplus P_2 = \mathcal{O}$.

(*iii*) *Ansonsten:*

falls $x_1 \neq x_2$ *, setze* $\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = \frac{y_1\,x_2 - y_2\,x_1}{x_2 - x_1}$,

falls $x_1 = x_2$ *, setze* $\lambda = \frac{3\,x_1^2 + 2\,a_2\,x_1 + a_4 - a_1\,y_1}{2\,y_1 + a_1\,x_1 + a_3}, \nu = \frac{-x_1^3 + a_4\,x_1 + 2\,a_6 - a_3\,y_1}{2\,y_1 + a_1\,x_1 + a_3}$,

dann $P_1 \oplus P_2 = (\lambda^2 + a_1\,\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)\,x_3 - \nu - a_3)$.

Die Formeln in Korollar 1.1.4 lassen sich natürlich vereinfachen, sobald die betrachtete elliptische Kurve E in kurzer Weierstraßform gegeben ist. Im Verlauf der Arbeit werden sie jedoch für Kurven in langer Weierstraßform benötigt.

Nachdem nun ausgeführt wurde, dass eine über einem Zahlkörper K definierte elliptische Kurve E/K sowohl durch eine lange, als auch durch eine kurze Gleichung gegeben sein kann, stellt sich die Frage nach der Klassifizierung entsprechend isomorpher Kurven. Diese geschieht mit Hilfe der j-Invarianten einer Kurve E:

Definition 1.1.5. *Sei* E *in langer Weierstraßform gegeben. Definiere*

$$\begin{aligned}
b_2 &:= a_1^2 + 4\,a_2, \\
b_4 &:= 2\,a_4 + a_1\,a_3, \\
b_6 &:= a_3^2 + 4\,a_6, \\
b_8 &:= a_1^2\,a_6 + 4\,a_2\,a_6 - a_1\,a_3\,a_4 + a_2\,a_3^2 - a_4^2, \\
\Delta(E) &:= -b_2^2\,b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2\,b_4\,b_6, \\
j(E) &:= \frac{(b_2^2 - 24\,b_4)^3}{\Delta}.
\end{aligned}$$

Dann heißt $\Delta(E)$ *die* **Diskriminante** *und* $j(E)$ *die* j**-Invariante** *von* E.

Damit läßt sich folgender Satz bzgl. der Isomorphie elliptischer Kurven formulieren.

Satz 1.1.6 (Silverman [86], III.1.4). *Zwei elliptische Kurven sind genau dann (über $\bar{K}$) isomorph, wenn sie dieselbe j-Invariante besitzen. Außerdem existiert zu jeder Zahl $j_0 \in \bar{K}$ eine über $K(j_0)$ definierte Kurve, deren j-Invariante gerade j_0 ist.*[4]

1.2 Isogenien

In diesem Abschnitt werden Abbildungen zwischen verschiedenen elliptischen Kurven betrachtet; dabei ist grundlegend, dass die neutralen Elemente $\mathcal{O}$ aufeinander abgebildet werden.

Seien für diesen Abschnitt die elliptischen Kurven immer über einem algebraischen Zahlkörper K bzw. dessen Abschluss $\bar{K}$ definiert.

Definition 1.2.1. *Seien E_1 und E_2 zwei elliptische Kurven. Eine* **Isogenie** *zwischen E_1 und E_2 ist ein Morphismus von algebraischen Kurven*

$$\phi \ : \ E_1 \to E_2,$$

der $\phi(\mathcal{O}) = \mathcal{O}$ erfüllt. E_1 und E_2 heißen **isogen** *zueinander, falls es eine nicht-triviale Isogenie ϕ zwischen ihnen gibt, also falls $\phi(E_1) \neq \{\mathcal{O}\}$ ist.*

Nach Satz D.2.13 erfüllt eine Isogenie ϕ zwischen E_1 und E_2 entweder $\phi(E_1) = \{\mathcal{O}\}$ oder $\phi(E_1) = E_2$. Außerdem gilt $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$ für beliebige Punkte $P, Q \in E_1$. (Siehe Silverman [86], III.4.8.)

Beispiel 1.2.2. Für jedes $m \in \mathbb{Z}$ ist die Multiplikation mit m eine Isogenie einer elliptischen Kurve E: $[m] \ : \ E \to E$. Sie ist kanonisch für $m > 0$ als $[m](P) = P \oplus \ldots \oplus P$ (m-mal) zu verstehen. Ist $m < 0$, so bedeutet $[m](P) := [-m](-P)$, ist $m = 0$, so ist $[0](P) = \mathcal{O}$. Ist dabei E über K definiert, so ist $[m]$ ebenfalls über K definiert, und $[m]$ ist genau dann eine nicht-triviale Isogenie, falls $m \neq 0$ gilt.

Satz 1.2.3 (Silverman [86], III.4.9 + III.4.12). *Sei $\phi \ : \ E_1 \to E_2$ eine nicht-triviale Isogenie. Dann ist*

$$\ker \phi := \phi^{-1}(\mathcal{O})$$

[4] Gleichungen solcher Kurven finden sich in Silverman [86], Beweis zu III.1.4.

eine endliche Untergruppe von E_1. Ist Γ eine beliebige endliche Untergruppe von E_1, so gibt es eine eindeutige elliptische Kurve E^* und eine Isogenie $\phi : E_1 \to E^*$, so dass $\ker \phi = \Gamma$ gilt. Häufig wird E^* mit E_1/Γ bezeichnet.

Die Existenz einer solchen Kurve $E^* \simeq E_1/\Gamma$ ist nicht in jedem Fall konstruktiv nachvollziehbar. Ist die Kurve E_1 jedoch über K definiert und bleibt Γ unter der Operation der Automorphismen von $Gal(\bar{K}/K)$ invariant im Sinne von $P \in \Gamma \Rightarrow P^\sigma = (\sigma(x_P), \sigma(y_P)) \in \Gamma$ für alle $\sigma \in Gal(\bar{K}/K)$, dann ist eine Konstruktion von E^* und ϕ möglich und beide sind dann über K definiert. (Siehe Silverman [86], III.4.13.2. und auch Abschnitt 3.2.3.)

1.2.1 Der Endomorphismenring

Die Menge der Isogenien zwischen zwei elliptischen Kurven E_1 und E_2 (genannt $\mathrm{Hom}(E_1, E_2)$) ist eine additive Gruppe; falls $E_1 = E_2 =: E$ gilt, so können Isogenien hintereinandergeschaltet werden. Somit wird aus $\mathrm{Hom}(E, E)$ ein Ring mit Addition und Multiplikation (Hintereinanderausführung), der Endomorphismenring $\mathrm{End}(E)$ von E. Dieser Ring ist eine wichtige Invariante einer elliptischen Kurve. Es handelt sich dabei um einen (im Allgemeinen nicht kommutativen) Ring der Charakteristik 0, der keine Nullteiler besitzt. (Siehe Silverman [86], III.4.) Falls die Kurve E über dem Körper K definiert ist, so werden nur solche Isogenien von E betrachtet, die ebenfalls über K definiert sind: $\mathrm{End}_K(E)$.

Bemerkung 1.2.4 (Silverman [86], III.4.3+VI.6.1.b). *Ist K ein Körper der Charakteristik 0 und E eine über K definierte elliptische Kurve, so gilt meist $End_K(E) \cong \mathbb{Z}$. Gilt dies nicht, ist also der Endomorphismenring von E echt größer als $\mathbb{Z}$, so sagt man, dass E* **komplexe Multiplikation** *besitzt. Ist dies der Fall, so ist $End_K(E)$ eine Ordnung in einem imaginär-quadratischen Zahlkörper.*

Zur Formulierung einer weiteren Bemerkung zum Endomorphismenring einer elliptischen Kurve E und mit Bezug auf Abschnitt D.3.1 wird hier folgende Aussage erwähnt.

Satz 1.2.5 (Silverman [86], VI.4.1). *Seien Λ_1, Λ_2 zwei Gitter in $\mathbb{C}$ und E_1, E_2 die zugehörigen elliptischen Kurven. Dann ist die Abbildung*

$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\} \;\to\; \{\phi \mid \phi \text{ ist Isogenie zwischen } E_1 \text{ und } E_2\}$$

eine Bijektion.

Bemerkung 1.2.6. *Sei $K/\mathbb{Q}$ ein imaginär-quadratischer Zahlkörper mit Maximalordnung O_K, und sei $Cl(O_K)$ die Idealklassengruppe von K. Ist Λ ein Ideal von O_K (bei festgehaltener Einbettung von K in $\mathbb{C}$), so ist $\Lambda \subset \mathbb{C}$ ein Gitter in $\mathbb{C}$. Für die korrespondierende elliptische Kurve gilt mit Satz 1.2.5, dass $End(\mathbb{C}/\Lambda) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} = O_K$ ist. Darüber hinaus gibt es nach Satz D.3.3 eine Bijektion zwischen den Idealklassen von $Cl(O_K)$ und den Isomorphieklassen elliptischer Kurven $E/\mathbb{C}$ mit $End(E) \cong O_K$. (Siehe auch Silverman [86], C.11.1.)*

1.3 Torsion elliptischer Kurven

Die in Beispiel 1.2.2 erwähnte Isogenie $[m]$ existiert für jedes $m \in \mathbb{Z}$ auf jeder elliptischen Kurve E/K und ist somit der erste Ansatzpunkt zur Untersuchung der Struktur der Punktgruppe von E/K.

Sei im Folgenden K ein algebraischer Zahlkörper.

Definition 1.3.1. *Sei E eine elliptische Kurve und $m \in \mathbb{Z}\backslash\{0\}$. Die m-***Torsionsuntergruppe** *von E ist die Menge*

$$E[m] := \{P \in E \mid [m]\, P = \mathcal{O}\}.$$

Die **Torsionsuntergruppe** *von E ist die Menge aller Punkte mit endlicher Ordnung, also*

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

$E(K)_{tors}$ bezeichnet die Torsionspunkte von E/K.

Ist $E/\bar{K}$ eine über $\bar{K}$ definierte elliptische Kurve, so ist die Struktur von $E[m]$ bekannt: $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. (Siehe Silverman [86], III.6.4.) Ist jedoch E/K gegeben, so ist die Situation komplizierter. Zuerst einmal existiert eine wichtige (allgemeine) Aussage von Mordell-Weil:

Satz 1.3.2 (Hindry/Silverman [27], C.0.1). *Sei V/K eine über einem algebraischen Zahlkörper K definierte abelsche Varietät. Dann ist die Gruppe $V(K)$ der K-rationalen Punkte von V endlich erzeugt.*

Somit existieren also zu einer elliptischen Kurve E/K Punkte $P_1, \cdots, P_r$ mit

$$E(K) = E(K)_{tors} \times \mathbb{Z}P_1 \times \cdots \times \mathbb{Z}P_r.$$

Die Zahl r wird dabei der **Rang** der Kurve E/K genannt und $E(K)$ heißt die **Mordell-Weil-Gruppe** von E/K. Da $E(K)_{tors}$ eine endliche abelsche Gruppe ist, kann

$$E(K)_{tors} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$$

geschrieben werden.

Zur Struktur der Torsionsgruppe und zum Rang ist bei beliebigem K nicht viel bekannt. Über den rationalen Zahlen vermutet man, dass der Rang beliebig groß sein kann. (Siehe Silverman [86], Conjecture VIII.10.1.) Mestre hat 1982 ([59]) eine Kurve mit $r \geq 12$ und 1992 ([61]) eine Kurve mit $r \geq 15$ veröffentlicht. Nach Mestres Ideen hat Fermigier [13] 1992 eine elliptische Kurve mit $r \geq 19$ und Nagao und Kouya [66] haben 1994 eine mit $r \geq 21$ konstruiert. 1997 veröffentlichte Fermigier [15] eine Kurve mit $r \geq 22$.

Zur Struktur der Torsionsgruppe einer elliptischen Kurve $E/\mathbb{Q}$ hat Mazur [55] 1977 das folgende Ergebnis bewiesen.

Satz 1.3.3 (Silverman [86], VIII.7.5). *Sei $E/\mathbb{Q}$ eine elliptische Kurve. Dann gilt für die Torsionsuntergruppe:*

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/m\mathbb{Z} \quad \textit{oder} \quad E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$$

für $1 \leq m \leq 10$ oder $m = 12$ bzw. für $1 \leq n \leq 4$.

Zur Gestalt eines Torsionspunktes P einer elliptischen Kurve $E/\mathbb{Q}$, die in kurzer (affiner) Weierstraßform mit Koeffizienten aus $\mathbb{Z}$ gegeben ist, haben Lutz [51] und Nagell [69] unabhängig voneinander bewiesen, dass P Koordinaten in $\mathbb{Z}$ besitzen muss. (Siehe Silverman [86], VIII.7.2., und für eine allgemeinere Form VIII.7.1.)

Für quadratische Zahlkörper K hat Kamienny [31] 1992 gezeigt, dass die Torsionsuntergruppe einer elliptischen Kurve E/K nur eine der folgenden Gruppenstrukturen haben kann.

Satz 1.3.4 (Hindry/Silverman [27], F.4.1.1.(ii)). *Sei K ein algebraischer Zahlkörper vom Grad 2 und sei E/K eine elliptische Kurve. Dann können folgende Gruppen als Torsionsuntergruppen auftreten:*

$$\mathbb{Z}/m\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

für $1 \leq m \leq 16$ oder $m = 18$ bzw. für $1 \leq n \leq 6$.

Für beliebige Zahlkörper gibt es noch keine solchen spezifischen Aussagen, aber Merel [57] hat 1996 folgenden Schrankensatz bewiesen.

Satz 1.3.5 (Hindry/Silverman [27], F.4.1.1.(iii)). *Sei K ein algebraischer Zahlkörper mit $[K : \mathbb{Q}] \leq d$. Dann gibt es eine Konstante $B(d)$, so dass für die Torsionsuntergruppe einer beliebigen elliptischen Kurve E/K die Abschätzung $\#E(K)_{tors} \leq B(d)$ gilt. Insbesondere gibt es zu jedem d nur endlich viele mögliche Gruppenstrukturen für $E(K)_{tors}$.*

Eine explizitere Form des Satzes mit konkreter Angabe der Schranken $B(d)$ findet sich bei Parent [75].

Für $d \geq 3$ gibt es noch keine umfassende Aussage über die Gruppen, die als Torsionsuntergruppen auftreten. Es lassen sich jedoch folgende Aussagen bzgl. der auftretenden Primzahlordnungen formulieren (siehe z. B. Parent [76] oder Edixhoven [10]):[5] Sei $d \in \mathbb{N}$ und sei $S(d)$ die Menge aller Primzahlen p, für die es eine Körpererweiterung $[K : \mathbb{Q}] = d$ und eine elliptische Kurve E/K gibt, so dass E/K einen Punkt der Ordnung p besitzt. Dann ist die Menge $S(d)$ endlich (vgl. Merel) und es gilt $S(1) = \{2, 3, 5, 7\}$ (vgl. Mazur) bzw. $S(2) = \{2, 3, 5, 7, 11, 13\}$ (vgl. Kamienny). Für $d = 3$ gilt $p \in S(3) \Rightarrow p \leq 37$ oder $p = 43$. Für $d > 3$ gilt $p \in S(d) \Rightarrow p \leq (1 + 3^{d/2})^2$.

Über diese Aussagen zu möglichen Primzahlordnungen hinaus ist es Jeon, Kim und Schweizer [30] im Jahr 2004 gelungen, folgenden Satz zu möglichen Gruppenstrukturen über einem kubischen Zahlkörper zu beweisen.

Satz 1.3.6 (Jeon/Kim/Schweizer [30], 3.4.). *Sei K ein beliebiger kubischer Zahlkörper und E/K eine über K definierte elliptische Kurve. Die Gruppenstrukturen, die unendlich häufig als $E(K)_{tors}$ auftreten, sind genau die folgenden:*

$$\mathbb{Z}/m\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$$

für $1 \leq m \leq 16$ oder $m = 18, 20$ bzw. für $1 \leq n \leq 7$.

Damit ist noch nicht bewiesen, dass nicht noch weitere Gruppenstrukturen auftreten können; die Vermutung, dass dies alle sind, liegt jedoch nahe.

Weitere Arbeiten beschäftigen sich mit elliptischen Kurven über bestimmten Zahlkörpern (z. B. Kreisteilungskörpern, siehe Dem'yanenko [9], oder abelschen 2-Erweiterungen, siehe z. B. Fujita [18]) oder der Konstruktion ellipti-

[5] Laut Edixhoven [10] hat J. Oesterlé die letzte Aussage 1994 bewiesen. Die Originalarbeit konnte jedoch nicht ermittelt werden.

scher Kurven mit großem Rang und nicht-trivialer Torsion (siehe z. B. Lecacheux [37], Kulesz [36], Fermigier [14], Nagao [67]).

1.3.1 Kubert-Kurven

Mazur hat in seinem Satz 1.3.3 gezeigt, dass es über $\mathbb{Q}$ definierte elliptische Kurven $E/\mathbb{Q}$ gibt, die einen Punkt der Ordnung $l \in \{3, 4, 5, 6, 7, 8, 9, 10, 12\}$ besitzen. Kubert [35] hat für diese Zahlen l generische Gleichungen elliptischer Kurven konstruiert, die einen rationalen Torsionspunkt der Ordnung l besitzen. Die folgenden Tabellen enthalten diese generische Gleichungen in der Form, wie sie in Abschnitt 3.1 benutzt werden. Die Kurven sind alle auf eine solche Gestalt gebracht, dass der Punkt $A = (0, 0)$ ein Punkt der gewünschten Ordnung l ist.

Im Fall $l = 3$ gibt es zwei freie Parameter $a_1, a_3 \in \mathbb{Q}$ und die Kurven haben folgende Form:

$$E_3 \quad : \quad y^2 + a_1\,xy + a_3\,y \;=\; x^3$$

In den anderen acht Fällen sind die Kurven jeweils Spezialfälle der folgenden einheitlichen Form mit Parameterwahl wie unten angegeben.

	$E_l \quad : \quad y^2 + (1-c)\,xy - b\,y \;=\; x^3 - b\,x^2$
$l = 4$	$c = 0$
$l = 5$	$b = c$
$l = 6$	$b = c(c+1)$
$l = 7$	$c = d(d-1)$ $b = dc = d^2(d-1)$
$l = 8$	$b = (2d-1)(d-1)$ $c = \frac{b}{d} = \frac{(2d-1)(d-1)}{d}$
$l = 9$	$c = d^2(d-1)$ $b = c(d(d-1)+1) = d^2(d-1)(d^2-d+1)$

	$E_l \quad := \quad y^2 + (1-c)\,xy - b\,y \;=\; x^3 - b\,x^2$
$l = 10$	$c = d(\frac{d^2}{d-(d-1)^2} - 1) = -\frac{d(2d^2-3d+1)}{d^2-3d+1}$ $b = c\frac{d^2}{d-(d-1)^2} = \frac{d^3(2d^2-3d+1)}{(d^2-3d+1)^2}$
$l = 12$	$c = \frac{3d-3d^2-1}{-(d-1)^2}\frac{d(1-2d)}{d-1} = -\frac{d(2d-1)(3d^2-3d+1)}{(d-1)^3}$ $b = c\frac{-2d^2+2d-1}{d-1} = \frac{d(2d-1)(3d^2-2d+1)(2d^2-2d+1)}{(d-1)^4}$

Da die Nenner in den obigen Gleichungen in den Fällen $l = 8, 10$ und 12 bei den späteren Berechnungen zu Problemen führen würden, werden durch Transformationen der genannten Kurvenfamilien nennerfreie Gleichungen erzeugt.

$l = 8$:

Durch die Transformation $x \mapsto \frac{x}{d^2}, \quad y \mapsto \frac{y}{d^3}$ erhält man die nennerfreie Gleichung in der Form

$$\boxed{E_8 \quad : \quad y^2 + (d-b)\,xy - d^3 b\,y \;=\; x^3 - d^2 b}$$

wobei, wie oben, $b = (2d-1)(d-1)$ ist. Offensichtlich wird der 8-Torsionspunkt $A = (0,0)$ auf sich selbst abgebildet.

$l = 10$:

Eine analoge Transformation $x \mapsto -\frac{x}{d^2-3d+1}, \quad y \mapsto -\frac{y}{d^2-3d+1}$ ergibt:

$$\boxed{E_{10} \quad : \quad y^2 + (\alpha-\beta)\,xy - \alpha\beta d^2\,y \;=\; x^3 - d^2\beta}$$

wobei $\alpha = -(d^2 - 3d + 1)$ und $\beta = d(d-1)(2d-1)$ ist. Auch hier wird der 10-Torsionspunkt $A = (0,0)$ auf sich selbst abgebildet.

$l = 12$:

Hier führt die analoge Transformation $x \mapsto -\frac{x}{(d-1)^6}, \quad y \mapsto -\frac{y}{(d-1)^9}$ zu:

$$\boxed{E_{12} : \; y^2 + (\alpha^3+\beta)\,xy - \alpha^5\beta(2d^2-2d+1)\,y \;=\; x^3 - \alpha^2\beta(2d^2-2d+1)\,x^2}$$

wobei $\alpha = (d-1)$ und $\beta = d(2d-1)(3d^2-3d+1)$ ist. Auch hier wird der 12-Torsionspunkt $A = (0,0)$ auf sich selbst abgebildet.

Kapitel 2

Hyperelliptische Kurven

Hyperelliptische Kurven sind Kurven vom Geschlecht $g \geq 2$, die eine zweifache Überlagerung der projektiven Linie $\mathbb{P}^1(\mathbb{C})$ darstellen.[1] Während eine Kurve vom Geschlecht 2 immer hyperelliptisch ist, sind Kurven von höherem Geschlecht dies im Allgemeinen nicht.[2] Wie Hindry und Silverman in [27], A.4.5, Seite 83 (siehe auch Hartshorne [25] IV.5.5.4+IV.5.5.5) erwähnen,[3] kann die Menge aller Isomorphieklassen von Kurven mit $g \geq 2$ durch eine Varietät der Dimension $3g-3$ parametrisiert werden, wobei die Teilmenge der Isomorphieklassen hyperelliptischer Kurven einer Untervarietät der Dimension $2g-1$ entspricht. Ist $g = 2$, so fallen diese beiden Varietäten zusammen.

2.1 Die Jacobische Varietät

Zentraler Punkt bei der Untersuchung einer hyperelliptischen Kurve $\mathcal{C}$ ist die Jacobische Varietät $J_{\mathcal{C}}$, die jedoch nicht isomorph zur Kurve selbst ist.

[1] Vergleiche Definition D.2.9 und auch die sich dort anschließende Fußnote 6.

[2] Ein Beispiel ist die nicht-hyperelliptische Kurve $y^4 - x^3 - 1 = 0$ vom Geschlecht 3.

[3] Hindry und Silverman beziehen sich auf Mumford [64], Lecture IV. Dieser zeigt mit Hilfe eines Satzes von Torelli, dass der Modulraum $\mathfrak{M}_g$ aller Isomorphieklassen von Kurven vom Geschlecht g die Dimension $3g-3$ besitzt. Übersichtlicher lässt sich dieselbe Aussage bei van der Waerden [92], Satz 7 finden. Eine Erläuterung zu den Isomorphieklassen hyperelliptischer Kurven vom Geschlecht g geben Griffiths und Harris in [24]: Eine entsprechende Kurve besitzt $2g+2$ Weierstraßpunkte (siehe Fußnote 7 in diesem Kapitel) und ist isomorph zu einer Kurve, bei der die Punkte $(0,0), (1,0)$ und $\mathcal{O}$ Weierstraßpunkte sind. Übrig bleiben $2g-1$ zu wählende Punkte, um die Kurve zu bestimmen.

In Analogie zu Satz 1.1.1 gibt es aber folgende Einbettung.

Lemma 2.1.1 (Baker [1], Seite 1). *Seien K ein Zahlkörper und $\mathcal{C}/K$ eine über K definierte algebraische Kurve vom Geschlecht $g \geq 1$ mit einem K-rationalen Punkt Q. Dann ist die über K definierte Abbildung*

$$i_Q : \mathcal{C}(K) \to J_{\mathcal{C}}(K), \quad P \mapsto [P - Q]$$

injektiv. Diese Abbildung heißt **Albanese-Einbettung**.

Untersucht man diese Einbettung näher, so ergeben sich unmittelbar zwei Fragen im Hinblick auf die Jacobische Varietät $J_{\mathcal{C}}(K)$ und deren Torsionspunkte:

- Wieviele Punkte liegen im Bild von $\mathcal{C}(K)$ in $J_{\mathcal{C}}(K)$?[4]
- Wieviele Punkte davon können Torsionspunkte sein?

Die Antwort lautet jeweils „nur endlich viele“, sofern $g \geq 2$ ist, was als Vermutungen von Mordell einerseits und Manin bzw. Mumford andererseits formuliert worden war. Mit der Beantwortung der ersten Frage, war die zweite trivial. Faltings und Raynaud haben sich jedoch unabhängig voneinander mit der Albanese-Einbettung und diesen Fragen beschäftigt und die Vermutungen (über K bzw. $\bar{K}$) 1983 bewiesen; Faltings [12] die erste und Raynaud [82] die zweite:

Mordell-Vermutung 2.1.2 (Hindry/Silverman [27], E.0.1). *Sei K ein Zahlkörper und $\mathcal{C}/K$ eine Kurve vom Geschlecht $g \geq 2$. Dann ist $\mathcal{C}(K)$ endlich.*

Manin-Mumford-Vermutung 2.1.3 (Hindry/Silverman [27], F.1.1.1). *Sei K ein Zahlkörper und sei $\mathcal{C}/K$ eine Kurve vom Geschlecht $g \geq 2$. Die Menge $T := \{ P \in \mathcal{C}(\bar{K}) \mid i_Q(P) \in J(\bar{K})_{tors} \}$ ist endlich.*

(Für $g = 1$ ist die Situation natürlich verschieden: Die Abbildung i_Q ist ein Isomorphismus (siehe Satz 1.1.1) und T ist unendlich (siehe Abschnitt 1.3).)

Diese Aussagen umfassen sämtliche Kurven von höherem Geschlecht, nicht nur hyperelliptische Kurven. Letztere können auf eine besondere Art dargestellt werden, wie der folgende Satz ausführt. (Siehe dazu auch Stichtenoth [90], VI.2.3.)

[4] Erinnerung: Punkte von $\mathcal{C}(K)$ sind Koordinatentupel, sie bilden keine Gruppe. Unter einem Punkt von $J_{\mathcal{C}}(K)$ ist eine Divisorenklasse zu verstehen; diese bilden eine Gruppe.

Satz 2.1.4 (Poonen [79], §2). *Ist K ein algebraischer Zahlkörper, so ist eine hyperelliptische Kurve $\mathcal{C}/K$ isomorph zu einer Kurve der Gestalt $y^2 = f(x)$, wobei $f(x) \in K[x]$ keine mehrfachen Nullstellen besitzt und den Grad $2g+1$ oder $2g+2$ hat, je nachdem ob eine Nullstelle von $f(x)$ in K liegt oder nicht; g ist dabei das Geschlecht der Kurve $\mathcal{C}/K$.*

Es gilt auch die Umkehrung des Satzes: Ist $\mathcal{C} : y^2 = f(x)$ mit $f(x) \in K[x]$ für einen Zahlkörper K gegeben und besitzt $f(x)$ keine mehrfachen Nullstellen, so ist $\mathcal{C}/K$ eine hyperelliptische Kurve, falls $deg(f) \geq 5$ gilt. Ist der Grad von $f(x)$ dabei $2\,g+1$ oder $2\,g+2$, so ist g das Geschlecht der Kurve. (Siehe Silverman [86], II.2.5.1.) Nach Beispiel D.2.5 besitzt die Kurve $\mathcal{C}/K$ keine (endlichen) singulären Punkte. Ist der Grad von $f(x)$ gerade, so besitzt $\mathcal{C}/K$ zwei Punkte im Unendlichen (manchmal als singulärer Punkt im Unendlichen bezeichnet). Diese sind genau dann K-rational, falls der führende Koeffizient von $f(x)$ ein Quadrat in K ist. Weitere Details zu hyperelliptischen Kurven in dieser Form finden sich in Abschnitt 2.1.2.

Isomorphieklassen hyperelliptischer Kurven sind für $g = 2$ durch die Igusa-Invarianten (siehe [29]) bestimmbar. Dabei handelt es sich um drei (absolute) Invarianten, die – analog zur j-Invarianten bei elliptischen Kurven – aus den Koeffizienten einer Gleichung der Kurve berechnet werden. Für $g \geq 3$ gibt es kein vollständiges Invariantensystem hyperelliptischer Kurven. Es gibt jedoch absolute Invarianten, mit denen zumindest die Nicht-Isomorphie zweier Kurven oder von Kurvenfamilien gezeigt werden kann. (Siehe z. B. die Ausführungen von Leprévost in [41, 44, 46] und [47].)

Es kann also jede hyperelliptische Kurve, ebenso wie auch jede elliptische Kurve (vgl. Satz 1.1.2), durch eine isomorphe Kurve der Form $y^2 = f(x)$ dargestellt werden. Entsprechend gibt es eine unmittelbare Analogie der zugehörigen Mordell-Weil-Gruppen, die für elliptische Kurven schon in Satz 1.3.2 formuliert wurde.

Satz 2.1.5 (Hindry/Silverman [27], C.0.1). *Sei V/K eine abelsche Varietät der Dimension g über einem Zahlkörper K. Dann ist die Mordell-Weil-Gruppe von V/K eine endlich erzeugte Gruppe:*

$$V(K) \simeq V(K)_{tors} \times \mathbb{Z}^{rank(V(K))}.$$

Dabei ist zu beachten, dass für eine hyperelliptische Kurve $\mathcal{C}/K$ die Kurve selbst keine abelsche Varietät ist, sondern erst ihre Jacobische Varietät $J_{\mathcal{C}}(K)$. Wird im Folgenden von der **Punktgruppe einer hyperelliptischen**

Kurve $\mathcal{C}/K$ gesprochen, so ist darunter immer $J_{\mathcal{C}}(K)$ zu verstehen. Die Varietät $J_{\mathcal{C}}(K)$ besitzt die **Dimension** g (siehe Hindry/Silverman [27], A.8.1.1), was eine Zerlegung in Untervarietäten zur Folge haben kann; in diesem Fall nennt man $J_{\mathcal{C}}(K)$ **reduzibel**, im anderen Fall **einfach**, sofern es keine Zerlegung über K und **absolut einfach**, sofern es keine über $\bar{K}$ gibt. Zerfällt eine abelsche Varietät vollständig in Untervarietäten der Dimension 1 (also in elliptische Kurven), so spricht man von **vollständig zerlegt**.

Lemma 2.1.6 (Hindry/Silverman [27], A.5.1.8). *Jede abelsche Varietät V ist isogen zu einem Produkt der Form*

$$V_1^{n_1} \times \ldots \times V_s^{n_s},$$

wobei die V_i einfache, paarweise nicht-isogene abelsche Varietäten sind.

Somit kann z. B. die Jacobische Varietät einer hyperelliptischen Kurve vom Geschlecht $g = 2$ entweder einfach sein oder in ein Produkt (möglicherweise isogener) elliptischer Kurven zerfallen.

Satz 2.1.7 (Cassels/Flynn [4], 14.1.1). *Sei $\mathcal{C}$ eine Kurve vom Geschlecht $g = 2$. Dann sind die folgenden Aussagen äquivalent:*

$\mathcal{C}$ ist isomorph zu einer Kurve

(i) $y^2 = c_3\,x^6 + c_2\,x^4 + c_1\,x^2 + c_0$ *mit* $c_i \in \bar{K}$,

(ii) $y^2 = g_1(x)\,g_2(x)\,g_3(x)$, *wobei die quadratischen Polynome* $g_i(x) \in \bar{K}[x]$ *linear abhängig sind,*

(iii) $y^2 = x\,(x-1)\,(x-a)\,(x-b)\,(x-ab)$ *für* $a, b \in \bar{K}$.

Tritt einer der Fälle ein (und damit alle), so ist $J_{\mathcal{C}}$ reduzibel.

Cassels/Flynn ([4], 14.3) führen aus, wie man aus zwei elliptischen Kurven eine hyperelliptische vom Geschlecht $g = 2$ konstruieren kann, deren Jacobische Varietät isogen zum Produkt der beiden Kurven ist. Eine Technik zur Untersuchung der Einfachheit einer Jacobischen Varietät einer Kurve vom Geschlecht 2 wird ebenfalls angedeutet; für weitere Details zu letzterem siehe Stoll [91] und insbesondere Leprévost [45].

2.1.1 Addition in $J_{\mathcal{C}}(K)$

Sei nun $\mathcal{C}/K$ eine über einem algebraischen Zahlkörper K definierte Kurve mit Gleichung $y^2 = f(x)$ und $deg(f) = 2\,g + 1$, und sei $J_{\mathcal{C}}(K)$ die Jacobische Varietät der über K definierten Divisoren. Eine konstruktive Version der Addition in $J_{\mathcal{C}}(K)$ findet sich bei Cantor [5], an der sich die folgenden Ausführungen orientieren.

Sei $\mathcal{O}$ der Punkt im Unendlichen von $\mathcal{C}/K$. Seien mit $m_i \in \mathbb{Z}$

$$D_1 = \sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} m_i\, P_i - (\sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} m_i)\, \mathcal{O}, \qquad D_2 = \sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} n_i\, P_i - (\sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} n_i)\, \mathcal{O}$$

zwei über K definierte Divisoren von $\mathcal{C}(K)$ vom Grad 0. Dann ist

$$D_1 + D_2 = \sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} (m_i + n_i)\, P_i - (\sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} m_i + n_i)\, \mathcal{O},$$

und der **größte gemeinsame Teiler** ist definiert als

$$\mathrm{ggT}(D_1, D_2) = \sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} \min(m_i, n_i)\, P_i - \left(\sum_{P_i \in \mathcal{C}\setminus\{\mathcal{O}\}} \min(m_i, n_i) \right) \mathcal{O}.$$

Mit einem Punkt $P = (x_P, y_P)$ (mit $y_P \neq 0$) liegt auch der Punkt $\tilde{P} = (x_P, -y_P)$ auf $\mathcal{C}(K)$. Der Divisor der Funktion $x - x_P \in K(\mathcal{C})$ lautet dann $div(x - x_P) = P + \tilde{P} - 2\,\mathcal{O}$. Ist $R = (x_R, 0)$ ein Punkt auf $\mathcal{C}(K)$, so ist der Divisor von $x - x_R$ gerade $div(x - x_R) = 2\,R - 2\,\mathcal{O}$. Damit ist also im ersten Fall $P + \tilde{P} - 2\,\mathcal{O} \equiv 0$ bzw. $-\tilde{P} \equiv P - 2\,\mathcal{O}$. Im zweiten Fall erhält man $R \equiv 2\,\mathcal{O} - R$. Somit kann zu einem beliebigen Divisor D ein äquivalenter Divisor $\hat{D}$ gefunden werden, der entweder P oder $\tilde{P}$ und zusätzlich R mit höchstens $\mathrm{ord}_R(\hat{D}) = 0$ oder $= 1$ enthält. Ein solcher Divisor $\hat{D}$ heißt **semi-reduzierter Divisor**. Jeder solche Divisor $\hat{D} = \sum P_i - r\,\mathcal{O}$ (dabei kann $P_i = P_j$ sein), der außerdem noch $r \leq g$ erfüllt, heißt **reduzierter Divisor**.

Satz 2.1.8 (Menezes [56], §6.). *Zu jedem Divisor D gibt es einen eindeutigen reduzierten Divisor $\hat{D}$ mit $D \equiv \hat{D}$.*

Jeder semi-reduzierte Divisor D lässt sich eindeutig durch Polynome $a(x)$ und $b(x)$ in der Form $D = ggT\,(div\,(a(x)), div\,(b(x) - y)) =: div\,(a, b)$ darstellen.

In dieser Darstellung eines semi-reduzierten Divisors $D = \sum m_i\, P_i - r\mathcal{O}$ mit $P_i = (x_i, y_i)$ ist $a := a(x) = \prod (x - x_i)^{m_i}$, und $b := b(x)$ ist das eindeutige

Polynom von Grad $< deg(a)$, das $b(x_i) = y_i$ für $1 \leq i \leq r$ mit passender Vielfachheit erfüllt.[5] Dabei ist D genau dann reduziert, wenn $deg(a) \leq g$ gilt. Auch die Umkehrung gilt (siehe Spallek [89], 2.2): ist a normiert und b ein Polynom mit $deg(b) < deg(a) \leq g$ und $a \mid (b^2 - f)$, so entspricht das Paar $(a, b) \in K[x] \times K[x]$ genau einem reduzierten Divisor D. Somit existieren folgende Isomorphismen:

$$\begin{aligned} J_{\mathcal{C}} &\simeq \bigcup_{r=0}^{g} \left\{ \sum_{i=1}^{r} P_i - r\,\mathcal{O} \mid P_i \neq \mathcal{O}, P_i \neq \tilde{P}_j \text{ für } i \neq j \right\} \\ &\simeq \bigcup_{r=0}^{g} \left\{ (a, b) \mid a \text{ normiert}, \, deg(a) = r, \, deg(b) < r, a \mid (b^2 - f) \right\}. \end{aligned}$$

Eine analoge Aussage gilt auch für $J_{\mathcal{C}}(K)$, die entsprechenden über K definierten Divisorenklassen und Polynome $a(x), b(x) \in K[x]$. (Siehe Spallek [89], 2.2 und auch Gaudry [20], 3.1 + 3.5.)

Sollen Divisoren D_1, D_2 addiert werden, so werden zuerst die zugehörigen semi-reduzierten Divisoren $\hat{D}_1, \hat{D}_2$ und deren Darstellung mittels $a_1(x), b_1(x)$ und $a_2(x), b_2(x)$ ermittelt. Die Addition $D_1 + D_2$ verlagert sich dann auf das Rechnen mit den Polynomen $a_i(x), b_i(x)$ und $f(x)$. In dem von Cantor [5] vorgestellten Algorithmus wird in einem ersten Schritt ein zu $D_1 + D_2$ äquivalenter semi-reduzierter Divisor berechnet, der in einem zweiten Schritt reduziert wird.

2.1.2 Berechnung von Hauptdivisoren

Der im vorangegangenen Abschnitt präsentierte Additionsalgorithmus von Cantor [5] wird im Folgenden nicht explizit benötigt. Benötigt werden jedoch Kenntnisse zur Berechnung von Hauptdivisoren, insbesondere auf Kurven $\mathcal{C}/K$ der Gleichung $y^2 = f(x)$, wobei $f(x)$ normiert vom Grad $2\,g + 2$ ist. Die dabei vorhandene Schwierigkeit ist die Existenz von zwei Punkten im Unendlichen, $\mathcal{O}^+$ und $\mathcal{O}^-$: Ein Divisor besitzt im Allgemeinen eine Form $D = \sum m_i\, P_i - n\,\mathcal{O}^+ - r\,\mathcal{O}^-$ mit $\sum m_i = n + r$. Ist nun $g(x, y) \in K[x, y]$ ein Polynom, so kann dennoch z. B. $\mathcal{O}^-$ eine *Nullstelle* von $g(x, y)$ sein.

Zuerst einmal stellt sich die Frage, wie die beiden Punkte $\mathcal{O}^+$ und $\mathcal{O}^-$ exakt

[5] Passende Vielfachheit bedeutet: ist die Ordnung $\text{ord}_{P_i}(D) = k > 1$, so muss $b(x) - y_i$ durch $(x - x_i)^k$ teilbar sein, was gleichbedeutend damit ist, dass a das Polynom $b(x)^2 - f(x)$ teilt.

zu beschreiben sind. Wie in Abschnitt D.2.2 ausgeführt wurde, erhält man die Punkte im Unendlichen durch Homogenisierung der Gleichung $\mathcal{C} : y^2 = f(x)$ und Betrachtung der Punkte in $\mathbb{P}^2$. Diese Konstruktion führt jedoch nur zu einem singulären Punkt $(0 : 1 : 0)$ von $\mathcal{C}$; man erreicht nicht die beiden gewünschten Punkte $\mathcal{O}^+, \mathcal{O}^-$. Variiert man dieses Verfahren durch Gewichtung des projektiven Raumes (siehe z. B. Reid [83], 1.1+1.2),

$$\mathbb{P}(1, \alpha, 1): \quad (x, y, z) \sim (\lambda\, x, \lambda^\alpha\, y, \lambda\, z) \quad \text{mit } \lambda \in \bar{K}^\times,$$

so erhält man mit $\alpha = g + 1$ für $f(x) = x^{2g+2} + c_{2g+1}\, x^{2g+1} + \cdots + c_1\, x + c_0$ die folgende Kurvengleichung mit homogener rechter Seite

$$y^2 = x^{2g+2} + c_{2g+1}\, x^{2g+1}\, z + \cdots + c_1\, x\, z^{2g+1} + c_0\, z^{2g+2},$$

auf der die Punkte $(1 : 1 : 0)$ und $(1 : -1 : 0)$ liegen: dies sind gerade die beiden (nicht-singulären) Punkte im Unendlichen $\mathcal{O}^+$ und $\mathcal{O}^-$. Während im Fall einer hyperelliptischen Kurve $y^2 = f(x)$ mit $deg\, f(x) = 2g + 1$ der Punkt im Unendlichen $\mathcal{O}$ als (∞, ∞) verstanden werden kann, erhält man bei $deg\, f = 2g + 2$ die Unterscheidung $\mathcal{O}^+ = (\pm\infty, \pm\infty)$ und $\mathcal{O}^- = (\pm\infty, \mp\infty)$.

Sei nun der Einfachheit halber $g = 2$ und $f(x) = \prod_{i=1}^{6}(x - \alpha_i) \in \bar{K}[x]$. Seien $g(x), h(x) \in \bar{K}[x]$ Polynome vom Grad 3 bzw. ≤ 5, so dass

$$f(x) = g^2(x) - h(x) = \left(g(x) - \frac{h(x)}{2\, g(x)}\right)^2 - \left(\frac{h(x)}{2\, g(x)}\right)^2$$

ist. Dann gilt die Entsprechung im Unendlichen (also für $\lim_{x \to \pm\infty}$)

$$y^2 = f(x) \sim \left(g(x) - \frac{h(x)}{2\, g(x)}\right)^2,$$

da im Grenzprozess der zweite Summand wegen des geringeren Gesamtgrades vernachlässigt werden kann. Somit gilt also für y in Bezug auf die Punkte im Unendlichen $\mathcal{O}^+, \mathcal{O}^-$ gerade

$$y \sim \pm\left(g(x) - \frac{h(x)}{2\, g(x)}\right),$$

wobei dann $\mathcal{O}^+$ einem Gesamtvorzeichen $+$ (in Abhängigkeit vom Vorzeichen von $g(x)$) und $\mathcal{O}^-$ einem Gesamtvorzeichen $-$ entspricht.

Mit dieser Vorüberlegung werden nun zu fünf Funktionen $\varphi \in \bar{K}[\mathcal{C}]$ die Hauptdivisoren $div(\varphi) = (\varphi) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(\varphi)\, P$ bestimmt. Dabei werden

die Nullstellen und die Polstellen getrennt untersucht; ersteres bedeutet $\varphi = 0$ und zweiteres $\varphi = \infty$. (Da bei der Berechnung von Divisoren multiplikative Konstanten unerheblich sind, wird zur Vereinfachung der Darstellung im Folgenden immer von normierten Polynomen ausgegangen.) Anschließend werden diese Überlegungen in einem sechsten Schritt auf Funktionen $\varphi \in \bar{K}(\mathcal{C})$ übertragen.

1) $\varphi = x$:

$$\begin{array}{lll}
\left\{ \begin{array}{rcl} x & = & 0 \\ y^2 & = & f(x) \end{array} \right. & \Rightarrow & \left\{ \begin{array}{rcl} x & = & 0 \\ y^2 & = & \prod_{i=1}^{6}(-\alpha_i) =: a_0 \end{array} \right. \\
 & \Rightarrow & P_1 = (0, \sqrt{a_0}), P_2 = (0, -\sqrt{a_0}) \text{ sind jeweils} \\
 & & \text{einfache Nullstellen.} \\
\left\{ \begin{array}{rcl} x & = & \infty \\ y^2 & = & f(x) \end{array} \right. & \Rightarrow & \left\{ \begin{array}{rcl} x & = & \infty \\ y^2 & = & \infty \end{array} \right. \\
 & \Rightarrow & \mathcal{O}^+, \mathcal{O}^- \text{ sind jeweils einfache Polstellen.} \\
\text{Somit:} & & (\varphi) = (x) = P_1 + P_2 - \mathcal{O}^+ - \mathcal{O}^-.
\end{array}$$

2) $\varphi = y$:

$$\begin{array}{lll}
\left\{ \begin{array}{rcl} y & = & 0 \\ y^2 & = & f(x) \end{array} \right. & \Rightarrow & \left\{ \begin{array}{rcl} y & = & 0 \\ 0 & = & \prod_{i=1}^{6}(x - \alpha_i) \end{array} \right. \\
 & \Rightarrow & \text{Für } 1 \leq i \leq 6 \text{ sind } P_i = (\alpha_i, 0) \text{ einfache Nullstellen.} \\
\left\{ \begin{array}{rcl} y & = & \infty \\ y^2 & = & f(x) \end{array} \right. & \Rightarrow & \left\{ \begin{array}{rcl} y & = & \infty \\ y & = & \pm\sqrt{f(x)} = \pm\left(g(x) - \frac{h(x)}{2g(x)}\right) \end{array} \right. \\
 & \Rightarrow & \mathcal{O}^+, \mathcal{O}^- \text{ je dreifache Polstelle, da } deg\, g(x) = 3. \\
\text{Somit:} & & (\varphi) = (y) = \sum_{i=1}^{6} P_i - 3\,(\mathcal{O}^+ + \mathcal{O}^-).
\end{array}$$

3) $\varphi = r(x) \in \bar{K}[x]$:

$$\left\{\begin{array}{rcl} r(x) & = & 0 \\ y^2 & = & f(x) \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} r(x) & = & \prod_{i=1}^{deg_r}(x-\beta_i) = 0 \\ y^2 & = & f(x) \end{array}\right.$$

$$\Rightarrow \quad P_i^{\pm} = (\beta_i, \pm\sqrt{f(\beta_i)}) \text{ je einfache Nullstelle. } (1 \le i \le deg_r).$$

$$\left\{\begin{array}{rcl} r(x) & = & \infty \\ y^2 & = & f(x) \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} x & = & \infty \\ y^2 & = & f(x) \end{array}\right.$$

$$\Rightarrow \quad \mathcal{O}^+, \mathcal{O}^- \text{ je } deg_r\text{-fache Polstelle.}$$

$$\text{Somit:} \qquad (\varphi) = (r(x)) = \sum_{i=1}^{deg_r} P_i^{\pm} - deg_r\,(\mathcal{O}^+ + \mathcal{O}^-).$$

4) $\varphi = y - r(x),\ r(x) \in \bar{K}[x]$:

$$\left\{\begin{array}{rcl} y - r(x) & = & 0 \\ y^2 & = & f(x) \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} y & = & r(x) \\ 0 & = & f(x) - r^2(x) = \prod_{i=1}^{deg_{f-r^2}}(x-\beta_i) \end{array}\right.$$

$$\Rightarrow \left\{\begin{array}{lcl} deg_r < 3 & \Rightarrow & P_i = (\beta_i, r(\beta_i)) \text{ für } (1 \le i \le 6). \\ deg_r = 3 & \Rightarrow & [\ldots \text{Untersuchung unten}\ldots] \\ deg_r > 3 & \Rightarrow & 2\,deg_r \text{ Punkte } P_i = (\beta_i, r(\beta_i)). \end{array}\right.$$

$$\left\{\begin{array}{rcl} y - r(x) & = & \infty \\ y^2 & = & f(x) \end{array}\right. \Rightarrow \left\{\begin{array}{l} y - r(x) = \infty \\ y = \pm\left(g(x) - \frac{h(x)}{2\,g(x)}\right) \end{array}\right.$$

$$\Rightarrow \left\{\begin{array}{l} \pm g(x) - r(x) \mp \frac{h(x)}{2\,g(x)} = \infty \\ y = \pm\left(g(x) - \frac{h(x)}{2\,g(x)}\right) \end{array}\right.$$

$$\Rightarrow \left\{\begin{array}{lcl} deg_r < 3 & \Rightarrow & \text{je 3-fache Polstelle } \mathcal{O}^+, \mathcal{O}^-. \\ deg_r = 3 & \Rightarrow & [\ldots \text{Untersuchung unten}\ldots] \\ deg_r > 3 & \Rightarrow & \text{je } deg_r\text{-fache Polstelle } \mathcal{O}^+, \mathcal{O}^-. \end{array}\right.$$

Hierbei ist zu beachten, dass bei dieser Polstellenuntersuchung der auftretende Nenner $2\,g(x)$ keine Rolle spielt, da $\varphi = y - r(x)$ nur dann „Unendlich

werden“ kann, wenn x oder y „Unendlich sind“, da $r(x) \in \bar{K}[x]$ gilt.

Ist $deg\, r(x) = deg_r = 3$, so wird die anfangs beschriebene Darstellung von $f(x)$ in der Form $f(x) = g^2(x) - h(x)$ mit dem Polynom $r(x)$ für $g(x)$ durchgeführt. In diesem Fall erhält man

$$f(x) = r^2(x) - h(x) = \left(r(x) - \frac{h(x)}{2\,r(x)}\right)^2 - \left(\frac{h(x)}{2\,r(x)}\right)^2$$

mit $deg\, h(x) \leq 5$, und damit

$$y \sim \pm\left(r(x) - \frac{h(x)}{2\,r(x)}\right),$$

was für die Null- und Polstellenberechung ausgenutzt wird. Man beachte dabei, dass – wie zuvor schon erwähnt – $\mathcal{O}^+$ einem positiven Gesamtvorzeichen (in Abhängigkeit vom Vorzeichen von $r(x)$) und $\mathcal{O}^-$ einem negativen Gesamtvorzeichen entspricht. Die folgende Ausführung wird für den Fall gemacht, dass $r(x)$ einen positiven führenden Koeffizienten hat. (Sollte dies nicht der Fall sein, so sind $\mathcal{O}^+$ und $\mathcal{O}^-$ zu vertauschen.)

$$\left\{\begin{array}{rcl} y - r(x) & = & 0 \\ y^2 & = & f(x) \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} y & = & r(x) \\ 0 & = & f(x) - r^2(x) = -h(x) = \prod_{i=1}^{deg_h}(x - \beta_i) \end{array}\right.$$

$$\Rightarrow \quad P_i = (\beta_i, r(\beta_i)) \text{ für } (1 \leq i \leq deg_h).$$

$$\left\{\begin{array}{rcl} y - r(x) & = & \infty \\ y^2 & = & f(x) \end{array}\right. \Rightarrow \left\{\begin{array}{l} y - r(x) = \infty \\ y = \pm\left(r(x) - \frac{h(x)}{2\,r(x)}\right) \end{array}\right.$$

$$\Rightarrow \left\{\begin{array}{l} \pm r(x) - r(x) \mp \frac{h(x)}{2\,r(x)} = \infty \\ y = \pm\left(r(x) - \frac{h(x)}{2\,r(x)}\right) \end{array}\right.$$

$$\Rightarrow \begin{array}{l} \text{entweder } (deg_r - deg_h) - \text{fache Nullstelle } \mathcal{O}^+ \\ \textbf{oder } (deg_h - deg_r) - \text{fache Polstelle } \mathcal{O}^+ \\ \text{(je nachdem, welcher Ausdruck} \geq 0 \text{ ist),} \\ \textbf{und } deg_r - \text{fache Polstelle } \mathcal{O}^-. \end{array}$$

Insgesamt erhält man also in diesem Fall:

$$(\varphi) = (y - r(x)) = \left\{\begin{array}{lcl} deg_r < 3 & \Rightarrow & \sum_{i=1}^{6} P_i - 3(\mathcal{O}^+ + \mathcal{O}^-). \\ deg_r = 3 & \Rightarrow & \sum_{i=1}^{deg_h} P_i - (deg_h - deg_r)\mathcal{O}^+ - deg_r\mathcal{O}^-. \\ deg_r > 3 & \Rightarrow & \sum_{i=1}^{2\,deg_r} P_i - deg_r(\mathcal{O}^+ + \mathcal{O}^-). \end{array}\right.$$

5) $\varphi = q(x)\,y - r(x),\ q(x), r(x) \in \bar{K}[x]$ mit $\mathrm{ggT}(q(x), r(x)) = 1$**:**

$$\left\{\begin{array}{rcl} q(x)\,y - r(x) & = & 0 \\ y^2 & = & f(x) \end{array}\right. \quad \Rightarrow \quad \left\{\begin{array}{l} q(x)\,y = r(x) \\ 0 = q^2(x)\,f(x) - r^2(x) = \prod_{i=1}^{deg_{q^2\,f - r^2}} (x - \beta_i) \end{array}\right.$$

$$\Rightarrow \quad \left\{\begin{array}{lcl} deg_{r^2} < deg_{q^2\,f} & \Rightarrow & P_i = (\beta_i, \frac{r(\beta_i)}{q(\beta_i)}) \\ & & \text{für } (1 \le i \le 2\,deg_q + 6). \\ deg_{r^2} = deg_{q^2\,f} & \Rightarrow & [\ldots \text{ Untersuchung} \\ & & \qquad \text{weiter unten } \ldots] \\ deg_{r^2} > deg_{q^2\,f} & \Rightarrow & 2\,deg_r \text{ Punkte } P_i = (\beta_i, \frac{r(\beta_i)}{q(\beta_i)}). \end{array}\right.$$

$$\left\{\begin{array}{rcl} q(x)\,y - r(x) & = & \infty \\ y^2 & = & f(x) \end{array}\right. \quad \Rightarrow \quad \left\{\begin{array}{l} q(x)\,y - r(x) = \infty \\ y = \pm\left(g(x) - \frac{h(x)}{2\,g(x)}\right) \end{array}\right.$$

$$\Rightarrow \quad \left\{\begin{array}{l} \pm q(x)\,g(x) - r(x) \mp \frac{q(x)\,h(x)}{2\,g(x)} = \infty \\ y = \pm\left(g(x) - \frac{h(x)}{2\,g(x)}\right) \end{array}\right.$$

$$\Rightarrow \quad \left\{\begin{array}{lcl} deg_{r^2} < deg_{q^2\,f} & \Rightarrow & \text{je } (deg_q + 3)\text{-fache} \\ & & \text{Polstelle } \mathcal{O}^+, \mathcal{O}^-. \\ deg_{r^2} = deg_{q^2\,f} & \Rightarrow & [\ldots \text{ Untersuchung} \\ & & \qquad \text{weiter unten } \ldots] \\ deg_{r^2} > deg_{q^2\,f} & \Rightarrow & \text{je } deg_r\text{-fache Polstelle } \mathcal{O}^+, \mathcal{O}^-. \end{array}\right.$$

Auch hier ist der auftretende Nenner $2\,g(x)$ bei der Polstellenberechnung wie zuvor unerheblich. Was noch fehlt, ist die Untersuchung für den Fall $deg\,r^2(x) = 2\,deg_r = 2\,deg_q + 6 = deg\,q^2(x) + deg\,f(x)$.

Sei also $deg\,r(x) - deg\,q(x) = 3$. Der Quotient $\frac{r(x)}{q(x)}$ lässt sich durch Polynomdivison in der Form

$$\frac{r(x)}{q(x)} = \hat{r}(x) + \frac{s(x)}{q(x)} \quad \Leftrightarrow \quad r(x) = q(x)\,\hat{r}(x) + s(x)$$

darstellen, wobei $deg\,\hat{r}(x) = 3$ und $deg\,s(x) < deg\,q(x)$ für $\hat{r}(x), s(x) \in \bar{K}[x]$ gilt. Die anfangs beschriebene Darstellung von $f(x)$ in der Form $f(x) = g^2(x) - h(x)$ wird mit dem gefundenen Polynom $\hat{r}(x)$ vom Grad 3 durchgeführt. In diesem Fall erhält man

$$f(x) = \hat{r}^2(x) - h(x) = \left(\hat{r}(x) - \frac{h(x)}{2\,\hat{r}(x)}\right)^2 - \left(\frac{h(x)}{2\,\hat{r}(x)}\right)^2$$

mit $deg\, h(x) \leq 5$, und damit

$$y \sim \pm \left(\hat{r}(x) - \frac{h(x)}{2\,\hat{r}(x)} \right),$$

was für die Null- und Polstellenberechung verwendet wird. Für die folgende Betrachtung gilt wieder die Annahme, dass $\hat{r}(x)$ einen positiven führenden Koeffizienten hat. Ist dies nicht der Fall, so sind $\mathcal{O}^+$ und $\mathcal{O}^-$ im Ergebnis zu vertauschen. Beachte im Folgenden, dass $r(x) = q(x)\,\hat{r}(x) + s(x)$ gilt:

$$\left\{ \begin{array}{rcl} q(x)\,y - r(x) & = & 0 \\ y^2 & = & f(x) \end{array} \right. \quad \Rightarrow \quad \left\{ \begin{array}{rcl} q(x)\,y & = & r(x) \\ 0 & = & q^2(x)\,f(x) - r^2(x) \\ & = & -q^2(x)h(x) - 2q(x)\hat{r}(x)s(x) - s^2(x) \\ & = & \prod_{i=1}^{d}(x - \beta_i) \end{array} \right.$$

Hierbei ist

$$\begin{array}{rcl} d & = & deg\, \left(-q^2(x)h(x) - 2q(x)\hat{r}(x)s(x) - s^2(x) \right) \\ & = & deg_q + deg\, \left(q(x)h(x) + 2\hat{r}(x)s(x) \right), \end{array}$$

da $deg_s < deg_q$ gilt. Somit erhält man d Nullstellen $P_i = (\beta_i, \frac{r(\beta_i)}{q(\beta_i)})$.

$$\left\{ \begin{array}{rcl} q(x)\,y - r(x) & = & \infty \\ y^2 & = & f(x) \end{array} \right. \quad \Rightarrow \quad \left\{ \begin{array}{l} q(x)\,y - r(x) = \infty \\ y = \pm \left(\hat{r}(x) - \frac{h(x)}{2\,\hat{r}(x)} \right) \end{array} \right.$$

$$\Rightarrow \quad \left\{ \begin{array}{l} \pm q(x) \left(\hat{r}(x) - \frac{h(x)}{2\hat{r}(x)} \right) - r(x) = \infty \\ y = \pm \left(\hat{r}(x) - \frac{h(x)}{2\,\hat{r}(x)} \right) \end{array} \right.$$

$$\Rightarrow \quad \left\{ \begin{array}{l} \pm q(x)\hat{r}(x) - q(x)\hat{r}(x) \mp \frac{q(x)h(x)}{2\hat{r}(x)} - \frac{2\hat{r}(x)s(x)}{2\hat{r}(x)} = \infty \\ y = \pm \left(\hat{r}(x) - \frac{h(x)}{2\,\hat{r}(x)} \right) \end{array} \right.$$

$$\Rightarrow \quad \begin{array}{l} \mathcal{O}^+ \text{ ist Polstelle der Ordnung} \\ deg\, (q(x)h(x) + 2\hat{r}(x)s(x)) - deg\, \hat{r}(x), \text{ und} \\ \mathcal{O}^- \text{ ist Polstelle der Ordnung } \; deg\, q(x)\hat{r}(x). \end{array}$$

Insgesamt erhält man also mit $\delta_1 = deg\, (q(x)h(x) + 2\hat{r}(x)s(x)) - deg\, \hat{r}(x)$ und $\delta_2 = deg\, q(x)\hat{r}(x)$:

$$(\varphi) = (q(x)\,y - r(x)) = \left\{ \begin{array}{lcl} deg_r < 3 & \Rightarrow & \sum_{i=1}^{2deg_q+6} P_i - (deg_q + 3)(\mathcal{O}^+ + \mathcal{O}^-). \\ deg_r = 3 & \Rightarrow & \sum_{i=1}^{d} P_i - \delta_1\mathcal{O}^+ - \delta_2\mathcal{O}^-. \\ deg_r > 3 & \Rightarrow & \sum_{i=1}^{2\,deg_r} P_i - deg_r(\mathcal{O}^+ + \mathcal{O}^-). \end{array} \right.$$

Hierbei ist zu bemerken, dass tatsächlich $d - \delta_1 - \delta_2 = 0$ gilt.

Gilt die Bedingung, dass $q(x)$ und $r(x)$ keine gemeinsamen Nullstellen haben, nicht, so ist zum bisher berechneten Hauptdivisor (φ) für jede gemeinsame Nullstelle β_i von $q(x)$ und $r(x)$ in jedem der drei Fälle noch $(\beta_i, \pm\sqrt{f(\beta_i)}) - \mathcal{O}^+ - \mathcal{O}^-$ hinzuzuaddieren.

6) $\varphi \in \bar{K}(\mathcal{C})$**:**

Der letzte Fall $\varphi \in \bar{K}(\mathcal{C})$ wird auf die zuvor besprochenen Fälle zurückgeführt, denn φ lässt sich als Quotient zweier Funktionen aus $\bar{K}[\mathcal{C}]$ darstellen. Da die Ordnung – die als theoretischer Bestandteil hinter der Divisorenberechnung steht – eines Quotienten sich auf die Ordnungen von Zähler und Nenner zurückführt (siehe Satz D.2.6), ist der Divisor des Quotienten φ einfach die Differenz des Divisors des Zählers und des Divisors des Nenners. Manchmal kann es dabei hilfreich sein, y aus dem Nenner zu eliminieren:

$$\varphi = \frac{q(x)\,y - r(x)}{s(x)\,y - t(x)} = \frac{(q(x)\,y - r(x))\,(s(x)\,y + t(x))}{s^2(x)\,f(x) - t^2(x)}.$$

Die bisherigen Ausführungen zur Berechnung von Hauptdivisoren wurden für eine Kurve $\mathcal{C} : y^2 = f(x)$ vom Geschlecht $g = 2$ gemacht, also für $deg\, f(x) = 6$. Ist eine Kurve höheren Geschlechts gegeben (wobei stets der Grad der rechten Seite der Gleichung $y^2 = f(x)$ wieder $2g+2$ ist), so lässt sich das Verfahren analog nutzen mit dem einzigen Unterschied, dass $f(x)$ sich in einer Form $f(x) = g^2(x) - h(x)$ mit $deg\, g(x) = g + 1$ und $deg\, h(x) < 2g + 2$ darstellen lässt. Entsprechend unterscheidet man für $\varphi = y - r(x)$ die Fälle $deg_r < g + 1, deg_r = g + 1$ und $deg_r > g + 1$; für $\varphi = q(x)y - r(x)$ sind es die Fälle $deg_r - deg_q < g + 1, deg_r - deg_q = g + 1$ und $deg_r - deg_q > g + 1$.

Beispiele zur Berechnung von Hauptdivisoren in dieser Form finden sich für Geschlecht $g = 2$ z. B. bei Leprévost [45]. Angewandt wird dieses Verfahren bei allgemeinem Geschlecht g im Beweis von Satz 2.2.5.

2.2 Torsion hyperelliptischer Kurven

Die Bestimmung aller Torsionspunkte der Jacobischen Varietät einer hyperelliptischen Kurve ist ein komplexes Problem, schwieriger als die Bestimmung entsprechender Punkte einer elliptischen Kurve. Zwar gibt es für $g = 2$ und

für eine Kurve $\mathcal{C}/\mathbb{Q}$ mit Gleichung $y^2 = f(x)$ mit ganzzahligen Koeffizienten Algorithmen (vgl. MAGMA [52]), aber darüber hinaus ist die Berechnung von Torsionspunkten bei einer gegebenen Kurve $\mathcal{C}/\mathbb{Q}$ nicht möglich, noch weniger bei einem beliebigen Zahlkörper K.[6] Es existieren auch keine Aussagen über mögliche Strukturen der Torsionsuntergruppe über $\mathbb{Q}$ oder über K.

2.2.1 Bekanntes und Vermutungen

Zur Untersuchung von Torsionspunkten hyperelliptischer Kurven gibt es u.a. zwei Ansatzpunkte: Einmal die Albanese-Einbettung und deren Bilder in der Torsionsuntergruppe der Jacobischen Varietät, und zum anderen die auch in $J_{\mathcal{C}}(K)$ existierende Multiplikation-mit-m-Isogenie $[m]$.

Lemma 2.2.1 (Hindry/Silverman [27], A.7.2.7). *Ist V eine abelsche Varietät der Dimension g über dem algebraischen Abschluss $\bar{K}$ eines Zahlkörpers K, dann ist die Isogenie $[m]$ vom Grad m^{2g} und $V[m] = ker[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$.*

Betrachtet man die m-Torsionsuntergruppe über K selbst, so gibt es keine Strukturaussagen; auch für die ganze Torsionsuntergruppe sind – sogar schon über $\mathbb{Q}$ – die möglichen endlichen Gruppen unbekannt. Offen ist auch, welche Ordnungen eines Torsionspunktes auftreten können.

Hinzu kommt bei einer Kurve $\mathcal{C}/K$ vom Geschlecht $g \geq 2$ die Möglichkeit, dass die Jacobische Varietät $J_{\mathcal{C}}(K)$ reduzibel ist, dass sie also isogen zu einem Produkt abelscher Varietäten geringerer Dimension ist (siehe Lemma 2.1.6). Entsprechend werden in der Betrachtung auch Torsionspunkte von einfachen und von nicht-einfachen Jacobischen Varietäten unterschieden: letztere können durch das geschickte Zusammenfügen von Untervarietäten Torsionspunkte relativ großer Ordnung besitzen. So konnten Howe, Leprévost und Poonen in [28] Kurven bzw. Kurvenfamilien mit nicht-einfachen Jacobischen Varietäten angeben, bei denen die Torsion bis zu $l = 63$ (für $g = 2$) reicht.

Bekannt sind in beiden Fällen bisher nur Beispiele einzelner Kurven oder von Kurvenfamilien. Es wird jedoch vermutet, dass – wie im Fall elliptischer Kurven – die Torsion einer Jacobischen Varietät über $\mathbb{Q}$ und auch über einem Zahlkörper nach oben begrenzt ist, wobei diese Grenze mit dem Körpergrad einerseits und dem Geschlecht der Kurve andererseits größer wird. Flynn [16] hat entsprechend für eine hyperelliptische Kurve $\mathcal{C}/\mathbb{Q}$ über $\mathbb{Q}$ folgende Vermutung formuliert:

[6] Ist K ein endlicher Körper, so kann die Mordell-Weil-Gruppe berechnet werden.

Flynn-Vermutung 2.2.2. *Es gibt eine von g unabhängige Konstante κ, so dass zu jedem $l \leq \kappa g$ eine hyperelliptische Kurve vom Geschlecht g über $\mathbb{Q}$ mit einem rationalen Torsionspunkt der Ordnung l existiert.*

Leprévost [46] hat als Reaktion auf diese Vermutung einen konstruktiven Beweis für $\kappa = 3$ mit folgender Aussage veröffentlicht:

Lemma 2.2.3 (Leprévost [46], 1.1+1.2.). *Seien g, l natürliche Zahlen mit $g \geq 1$ und $1 \leq l \leq 2g+1$. Dann existiert eine 1-parametrige Familie über $\mathbb{Q}$ definierter hyperelliptischer Kurven vom Geschlecht g, deren Jacobische Varietät einen rationalen Punkt der Ordnung l besitzt.*
Analoges gilt für $2g+2 \leq l \leq 3g$, falls l gerade ist. Ist l ungerade und $l < 3g$, so existiert mindestens eine entsprechende Kurve.

In der folgenden Tabelle sind einige Kurven $\mathcal{C}/\mathbb{Q} : y^2 = f(x)$ aufgelistet, deren Jacobische Varietät einen Punkt der Ordnung l besitzt. Die Buchstaben E, F, L, O beziehen sich auf die Autoren (Elkies, Flynn, Leprévost, Ogg), in Klammern ist jeweils die Quelle angegeben. Bei den von Ogg untersuchten unten angegebenen Kurven handelt es sich um die Modulkurven $X_1(13)$ mit Torsion $l = 19$ und $X_1(18)$ mit Torsion $l = 21$.

l	g	$f(x)$	Quelle
11	2	$x^6+2x^5+(2t+3)x^4+2x^3+(t^2+1)x^2+2t(1-t)x+t^2$	F [16]
13	2	$4\,x^5+(t^2+10t+1)\,x^4+4t\,(2t+1)\,x^3$ $+2t^2\,(t+3)\,x^2+4t^3\,x+t^4$	L [39]
15	2	$((t+3)\,x^2-(2t+3)x+t+1)^2-4t\,x^3\,(x-1)^2$	L [40]
17	2	$((t^3+2t^2-3t+1)x^2-t(2t^2+t-1)x+t^3)^2-4t^2(t-1)^3x^3(x-1)^2$	L [40]
19	2	$x^6-2\,x^5+x^4-2\,x^3+6\,x^2-4\,x+1$	O [73]
21	2	$x^6+2\,x^5+5\,x^4+10\,x^3+10\,x^2+4\,x+1$	O [73]
		$4\,x^6-12\,x^5+13\,x^4-6\,x^3+3\,x^2-2\,x+1$	L [43]
22	2	$(2\,x^2-2\,x+1)\,(2\,x^4-2\,x^3+x^2-4\,x+4)$	L [43]
23	2	$x^6-10\,x^5+33\,x^4-36\,x^3+28\,x^2-16\,x+4$	L [43]
24	2	$(2\,x^2-2\,x-1)\,(2\,x^4-10\,x^3+7\,x^2+4\,x-4)$	L [43]
		$(x^2-x+1)\,(x^4-3\,x^3+8\,x^2-3\,x+1)$	L [43]
25	2	$4\,x^6+8\,x^5-48\,x^4+68\,x^3+x^2-60\,x+36$	L [43]
26	2	$(6\,x^2-6\,x+1)\,(6\,x^4-30\,x^3+49\,x^2-20\,x+4)$	L [43]
27	2	$(2\,x^3-15\,x^2+12\,x-3)\,(2\,x^3-15\,x^2-3)$	L [43]

l	g	$f(x)$	Quelle
29	2	$(2\,x-1)\,(2\,x^5-x^4-4\,x^2+8\,x-4)$	L [43]
30	2	*1-Parameter-Familie (unveröffentlicht)*	L
32	2	$(15\,x-1)\cdot$ $(1056\,x^4+156183\,x^3+26297\,x^2+649\,x-121)$	E [11]
34	2	$(9\,x^2+2\,x+1)\,(32\,x^3+81\,x^2-6\,x+1)$	E [11]
		$(10-x)\,(3\,x+2)\,(72\,x^4+96\,x^3+45\,x^2-38\,x+5)$	E [11]
39	2	$x^6+4\,x^4+10\,x^3+4\,x^2-4\,x+1$	E [11]
40	2	$(3\,x+4)\,(x^4+5\,x^3+8\,x^2+\frac{19}{4}\,x+1)$	E [11]

Zwei weitere, einparametrige Kurvenfamilien für $l = 19, 21$ finden sich bei Leprévost [40]. Elkies [11] erwähnt, dass seine Kurve mit einem Torsionspunkt der Ordnung 32 ein Beispiel aus einer Kurvenfamilie ist, welche er jedoch nicht angegeben hat. Außerdem weist er auf die Kurve $y^2 = 5\,x^6 - 4\,x^5 + 20\,x^4 - 2\,x^3 + 24\,x^2 + 20\,x + 5$ hin, die eine $\mathbb{Q}$-rationale 31-Torsionsuntergruppe ohne $\mathbb{Q}$-rationalen Erzeuger besitzt.

Flynn und Leprévost haben auch einige parametrisierte Kurvenfamilien bei beliebigem Geschlecht g mit einer von g abhängenden Torsionspunktordnung l veröffentlicht:

l	g	$f(x)$	Quelle
$2g+1$	g	$y^2+y=x^{2g+1}+x^{2g}+x^g$	F [17]
$2g^2+2g+1$	g	$(t\,x^g+(x-1)^g)^2-4t\,x^{g+1}\,(x-1)^g$	L [40, 41]
$2g^2+3g+1$	g	$(x^{g+1}-(x-1)^g\,(x-1-t))^2-4t\,x^{g+1}\,(x-1)^g$	L [40, 41]
$2g^2+4g+1$	g	*(1-Parameter-Familie)*	L [44]

Die eingangs erwähnte zweite Möglichkeit, Aussagen über die Torsionspunkte einer hyperelliptischen Kurve zu erhalten, ist die Untersuchung der Albanese-Einbettung i_Q und der durch diese erreichten Torsionspunkte. Nach der Manin-Mumford-Vermutung sind dies endlich viele für eine beliebige Kurve $\mathcal{C}/K$ mit beliebigem Geschlecht g über einem Zahlkörper K. Poonen [80] hat einen Algorithmus entwickelt, der zu einer Kurve $\mathcal{C}/\mathbb{Q}$ vom Geschlecht $g = 2$ die Punkte von $\mathcal{C}(\bar{\mathbb{Q}}) \cap J(\bar{\mathbb{Q}})_{tors}$ berechnet, falls die Albanese-Einbettung i_Q durch einen Weierstraßpunkt[7] Q gegeben ist.

[7] Weierstraßpunkte: Ist $\mathcal{C} : y^2 = f(x) = \prod_{i=1}^{2g+1}(x-\alpha_i)$ gegeben, so heißen die Punkte $P = (\alpha_i, 0)$ und $\mathcal{O}$ Weierstraß- oder Verzweigungspunkte von $\mathcal{C}$. (Siehe Hindry/Silverman [27], S. 297.)

Torsion hyperelliptischer Modulkurven

Für Modulkurven $X_0(N)(\mathbb{Q})$ für eine Primzahl $N \geq 23$ konnten die Torsionspunkte, die von der Kurve selbst kommen, beschrieben werden. Ist i_∞ die über $\mathbb{Q}$ definierte Albanese-Einbettung von $X_0(N)(\mathbb{Q})$ in die Jacobische Varietät $J_0(N)(\mathbb{Q})$, so wird die Spitze (∞) trivialerweise auf einen Torsionspunkt abgebildet. Das Bild der zweiten Spitze (0), die Klasse $[(0)-(\infty)]$, ist ein Torsionspunkt der Ordnung $l = \frac{N-1}{\mathrm{ggT}(N-1,12)}$ (siehe Ogg [73]). Coleman, Kaskel und Ribet vermuteten, dass dies fast immer alle von $X_0(N)$ kommenden Torsionspunkte[8] sind, was von Baker [1] bewiesen wurde.

CKR-Vermutung 2.2.4 (Baker [1], 1.2). *Sei $N \geq 23$ eine Primzahl. Ist die Modulkurve $X_0(N)$ hyperelliptisch[9] mit $N \neq 37$, so besitzt sie die Torsionspunkte $\{(0),(\infty)\} \cup \{$Weierstraßpunkte$\}$; in allen anderen Fällen sind nur die Punkte $\{(0),(\infty)\}$ Torsionspunkte, die von $X_0(N)$ kommen.*

Ogg zeigte in [73] weiter, dass $[(0)-(\infty)]$ die gesamte Torsionsuntergruppe $J_0(N)(\mathbb{Q})_{tors}$ erzeugt, falls $N \in \mathbb{N}$ eine Primzahl ist. Dabei sind (0) und (∞) die oben erwähnten rationalen Spitzen (siehe auch Abschnitt D.3.2). Ist N keine Primzahl, so erzeugt die Divisorenklasse $[(0)-(\infty)]$ eine Untergruppe der Ordnung l von $J_0(N)(\mathbb{Q})_{tors}$, die sogenannte „Spitzen-Untergruppe“.[10] Eine zweite Untergruppe dieser Ordnung, die Shimura-Untergruppe Σ von $J_0(N)$, ist der Kern einer Abbildung $J_0(N) \to J_1(N)$, die durch die kanonische Abbildung $X_1(N) \to X_0(N)$ (siehe Abschnitt D.3.4) induziert wird.

Ogg hat auch die 19 Werte von N bestimmt, für die $X_0(N)$ hyperelliptisch vom Geschlecht $g \geq 2$ ist (siehe Ogg [74], vgl. auch Abschnitt D.3.3). Im Folgenden werden die Fälle betrachtet, in denen beide Eigenschaften zutreffen, also N eine Primzahl ist und $X_0(N)$ hyperelliptisch vom Geschlecht $g \geq 2$ ist. Die entsprechenden Werte für N sind somit $23, 29, 31, 37$ $(g=2)$, 41 $(g=3)$, 47 $(g=4)$, 59 $(g=5)$, und 71 $(g=6)$. Zu diesen Werten werden in der folgenden Tabelle die Gleichungen von $X_0(N)$ in der Form $y^2 = f_N(x)$ angegeben, wie sie González Rovira[11] [22] (und Murabayashi [65] für $N=31$) veröffentlicht haben. (Vgl. Abschnitt D.3.3.)

[8] Unter Torsionspunkten sind immer Divisorenklassen in J_C bzw. $J_0(N)$ zu verstehen.

[9] Die Bedingung, dass $X_0(N)$ hyperelliptisch ist, erfüllen (neben $N=37$) nur sieben verschiedene Primzahlen N (vgl. Abschnitt D.3.3).

[10] Im Englischen heißt diese Untergruppe *cuspidal subgroup*; ein anderer deutscher Name wurde nicht gefunden.

[11] Bei $N=31$ findet sich im Artikel von González Rovira ein Druckfehler.

g	N	l	$f_N(x)$
2	23	11	$x^6+4\,x^5-18\,x^4-142\,x^3-351\,x^2-394\,x-175$
2	29	7	$x^6+2\,x^5-17\,x^4-66\,x^3-83\,x^2-32\,x-4$
2	31	5	$x^6-8\,x^5+6\,x^4+18\,x^3-11\,x^2-14\,x-3$
2	37	3	$x^6-4\,x^5-40\,x^4+348\,x^3-1072\,x^2+1532\,x-860$
3	41	10	$x^8+4\,x^7-8\,x^6-66\,x^5-120\,x^4-56\,x^3+53\,x^2+36\,x-16$
4	47	23	$x^{10}+4\,x^9+2\,x^8-32\,x^7-135\,x^6-294\,x^5-424\,x^4-410\,x^3$ $-268\,x^2-100\,x-19$
5	59	29	$x^{12}+4\,x^{11}-28\,x^9-84\,x^8-152\,x^7-202\,x^6-212\,x^5$ $-176\,x^4-120\,x^3-68\,x^2-24\,x-11$
6	71	35	$x^{14}+4\,x^{13}-2\,x^{12}-38\,x^{11}-77\,x^{10}-26\,x^9+111\,x^8+148\,x^7$ $+x^6-122\,x^5-70\,x^4+30\,x^3+40\,x^2+4\,x-11$

Nicht alle Gleichungen von $X_0(N)$ werden in diesen Formen am Ende des Abschnitts 2.2.3 wieder aufgegriffen. Vielmehr werden für $N = 23, 31$ und 47 Transformationen $x \mapsto x - \alpha$ mit $\alpha = 2, -2$ und 1 (für die jeweiligen N) durchgeführt, die übersichtlichere Gleichungen zur Folge haben. (Details siehe in „Hyperelliptische Modulkurven $X_0(N)$ in den konstruierten Familien“, am Ende von Abschnitt 2.2.3.)

Außerdem wird die Modulkurve $X_0(37)$ nicht weiter untersucht, denn sie verhält sich anders als die anderen Kurven:

Berechnungen gemäß Abschnitt 2.1.2 zeigen, dass der Divisor der Funktion

$$\varphi_{37} = y - r(x) = y - \left(-(x-4)\,(x^2+2\,x-14)\right)$$

gleich

$$(\varphi_{37}) = 3\,\left((3,1) - \mathcal{O}^+\right)$$

ist. Tatsächlich gilt $f_{37} - r^2(x) = 2^2 37(x-3)^3$.

Die Spitze (0) entspricht dem Punkt $(3,1)$ auf der Kurvengleichung und die Spitze (∞) dem Punkt $\mathcal{O}^+$. Die Begründung für dieses unterschiedliche Verhalten beruht darin, dass die hyperelliptische Involution im Fall $N = 37$ nicht die Atkin-Lehner-Involution ist (siehe z. B. Lehner [38]). Ogg hat bewiesen (siehe [74], S. 450), dass nur für $N = 37$ die Modulkurve $X_0(N)$ sowohl hyperelliptisch ist und außerdem ihre hyperelliptische Involution nicht zur Untergruppe von $\mathrm{Aut}(X_0(N))$ gehört, die durch Automorphismen der oberen Halbebene gegeben ist.

2.2.2 Die Polynomgleichung

Eine bekannte Methode, hyperelliptische Kurven (und auch Kurvenfamilien) $\mathcal{C} : y^2 = f(x)$ über $\mathbb{Q}$ zu konstruieren, basiert auf der Idee, $f(x)$ in der Form $f(x) = A^2(x) + \lambda x^2(x-1)^3$ mit $A(x) \in \mathbb{Q}[x]$ vom Grad 2 und $\lambda \in \mathbb{Q}^\times$ darzustellen. Dann besitzt $\mathcal{C}$ die Punkte $P_0 = (0, A(0))$ und $P_1 = (1, A(1))$. Der Divisor der Funktion $\varphi_1 = y - A(x) \in K(\mathcal{C})$ lautet gemäß Abschnitt 2.1.2 (Berechnung von Hauptdivisoren) $2P_0 + 3P_1 - 5\mathcal{O}$. Unter der Annahme, dass es eine weitere Funktion $\varphi_2 \in K(\mathcal{C})$ mit Divisor $5P_0 + P_1 - 6\mathcal{O}$ gibt, folgt mit dem linearen System

$$\begin{pmatrix} \varphi_1 \\ \varphi_2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} P_0 - \mathcal{O} \\ P_1 - \mathcal{O} \end{pmatrix},$$

dass die Klasse des Divisors $P_0 - \mathcal{O}$ die Ordnung 13 hat, denn $13(P_0 - \mathcal{O}) = \frac{\varphi_2^3}{\varphi_1}$. Analoges gilt für den Divisor $P_1 - \mathcal{O}$. Diese Konstruktion beruht auf der Bestimmung von $A(x)$ und λ. (Für weitere Details siehe z. B. Leprévost [45] oder Cassels/Flynn [4], 8.3.)

Eine andere Möglichkeit, hyperelliptische Kurven und Kurvenfamilien zu konstruieren, wird im Folgenden ausführlich vorgestellt und ausgeführt.

Sei K ein Körper der Charakteristik 0 und seien $g, l \in \mathbb{Z}$ ganze Zahlen mit $l \geq g + 1 \geq 2$.

Satz 2.2.5. *Seien P, Q und F normierte Polynome mit Koeffizienten in K. Sei l der Grad von P, $l - (g+1)$ der Grad von Q und $2g+2$ der Grad von F. Außerdem habe F keine mehrfachen Nullstellen und es gelte die folgende Polynomgleichung:*

$$P^2(x) - Q^2(x)F(x) = \lambda \in K^\times. \tag{2.1}$$

Dann ist die Kurve $\mathcal{C} : y^2 = F(x)$ hyperelliptisch vom Geschlecht g und ihre Jacobische Varietät besitzt einen Punkt, dessen Ordnung größer 1 ist und l teilt. Insbesondere hat dieser Punkt die exakte Ordnung l, falls l eine Primzahl ist.

Beweis. Zuerst sei bemerkt, dass die Polynome $P(x)$ und $Q(x)$ keine gemeinsamen Nullstellen haben, falls die Gleichung (2.1) erfüllt ist. Außerdem ist die Bedingung, dass P und Q normierte Polynome sind, äquivalent dazu, dass man bei beliebigen P, Q die Konstante $\lambda \in K^\times$ als quadratfrei annimmt.[12]

[12] Voraussetzung ist, dass λ sich eindeutig als Produkt von Primelementen beschreiben lässt, was im Allgemeinen nicht der Fall sein muss.

Da F den Grad $2g+2$ besitzt und keine mehrfachen Nullstellen hat, ist die Kurve $\mathcal{C}$ mit Gleichung $y^2 = F(x)$ unmittelbar hyperelliptisch vom Geschlecht g. Da $F(x)$ ein normiertes Polynom ist, sind die Punkte $\mathcal{O}^+$ und $\mathcal{O}^-$ rationale Punkte über K. (Das wäre auch der Fall, falls der führende Koeffizient von F ein Quadrat in K wäre. Dieser Fall ist nicht allgemeiner als die im Satz formulierte Aussage mit normiertem $F(x)$.) Damit enthält die Gruppe $J_{\mathcal{C}}(K)$ der K-rationalen Punkte der Jacobischen Varietät von $\mathcal{C}$ die Divisorenklasse des rationalen Divisors $D_\infty = \mathcal{O}^+ - \mathcal{O}^-$. Ist nun die Polynomgleichung $P^2(x) - Q^2(x)F(x) = \lambda$ für ein bestimmtes $\lambda \in K^\times$ erfüllt, so ist der Divisor der Funktion $\varphi(x,y) = P(x) - y\,Q(x)$ gerade $(\varphi) = lD_\infty$, was nach einer einfachen Rechnung im Sinne der „Berechnung von Hauptdivisoren“ 2.1.2 folgt. Somit ist die Divisorenklasse des K-rationalen Divisors D_∞ ein Element von $J_{\mathcal{C}}(K)$, dessen Ordnung l teilt. Darüber hinaus kann dieser Punkt nicht die Ordnung 1 haben, da ansonsten die Kurve $\mathcal{C}$ birational zu $\mathbb{P}^1$ wäre, also Geschlecht 0 hätte, was ausgeschlossen ist ($g \geq 1$). □

Der folgende Satz beschreibt eine Methode zur Konstruktion von Polynomen $P(x), Q(x)$ und $F(x)$, die die Voraussetzungen von Satz 2.2.5 erfüllen.

Satz 2.2.6. *Seien Q_1, Q_2, F_1, F_2 vier normierte Polynome aus $K[x]$ mit den jeweiligen Graden q_1, q_2, f_1, f_2. Angenommen, F_1 und F_2 haben jeweils keine mehrfachen Nullstellen und es gelten die Beziehungen $2q_1 + f_1 = 2q_2 + f_2 = l$ und $f_1 + f_2 = 2g + 2$. Erfüllen zusätzlich die vier Polynome die Gleichung*

$$Q_1^2(x)F_1(x) - Q_2^2(x)F_2(x) = 2t, \tag{2.2}$$

für ein $t \in K^\times$, dann gelten die Voraussetzungen des Satzes 2.2.5 für die Polynome $P(x) = Q_1^2(x)F_1(x) - t$, $Q(x) = Q_1(x)Q_2(x)$ und $F(x) = F_1(x)F_2(x)$, und diese drei Polynome erfüllen die Gleichung

$$P^2(x) - Q^2(x)F(x) = t^2 \in K^\times.$$

Beweis. Der Grad von $P(x)$ ist l und der Grad von $F(x)$ ist $2g+2$. Da $2q_1 + f_1 + 2q_2 + f_2 = 2l$ ist, folgt $q_1 + q_2 = l - (g+1)$, also hat auch $Q(x)$ den in Satz 2.2.5 vorausgesetzten Polynomgrad. Weiter besitzt $F(x) = F_1(x)\,F_2(x)$ keine mehrfachen Nullstellen, da einerseits $F_1(x)$ und $F_2(x)$ jeweils keine mehrfachen Nullstellen besitzen und andererseits eine Nullstelle von $F_1(x)$ nicht auch Nullstelle von $F_2(x)$ sein kann, da ansonsten die linke Seite von (2.2) eine Nullstelle hätte, was einen Widerspruch zu $t \in K^\times$ darstellt.
Schließlich lässt sich die Polynomgleichung (2.1) mit (2.2) leicht verifizieren:
$P^2 - Q^2F = (Q_1^2\,F_1 - t)^2 - Q_1^2\,Q_2^2\,F_1\,F_2 = Q_1^2\,F_1\,(Q_1^2\,F_1 - 2t - Q_2^2\,F_2) + t^2 = t^2$ □

Lassen sich also Polynome Q_1, Q_2, F_1 und F_2 mit den in Satz 2.2.6 beschriebenen Eigenschaften finden, so ist die Kurve mit Gleichung $y^2 = F_1(x)\,F_2(x)$ hyperelliptisch und von Geschlecht g, und ihre Jacobische Varietät besitzt einen K-rationalen Punkt, dessen Ordnung l teilt.

Gilt nun $l \equiv g+1 \pmod 2$ und $f_1 = f_2 = g+1$ und $q_1 = q_2 = \frac{l-(g+1)}{2}$, so lässt sich folgende Variante des vorangegangenen Satzes formulieren.

Satz 2.2.7. *Seien $l \geq g+1 \geq 2$ ganze Zahlen mit $l \equiv g+1 \pmod 2$. Gelte $d \in K \setminus K^2$ und seien Q_1 und F_1 zwei normierte Polynome aus $K(\sqrt{d})[x]$, die nicht über K definiert sind. Sei $\frac{l-(g+1)}{2}$ der Polynomgrad von Q_1 und $g+1$ der Polynomgrad von F_1 und bezeichne der Strich $\overline{\ }$ das Bild unter der Abbildung $K(\sqrt{d})[x] \longrightarrow K(\sqrt{d})[x]$ mit $\sqrt{d} \longmapsto -\sqrt{d}$.*
Falls dann die Gleichung

$$Q_1^2(x)F_1(x) - \overline{Q_1}^2(x)\overline{F_1}(x) = t - \bar{t} = 2u\sqrt{d} \tag{2.3}$$

erfüllt ist, wobei $t = u\sqrt{d}$ für ein $u \in K^\times$ gilt, so sind die Polynome $P(x) = Q_1^2(x)F_1(x) - t$, $Q(x) = Q_1(x)\overline{Q_1}(x)$ und $F(x) = F_1(x)\overline{F_1}(x)$ Elemente aus $K[x]$, der Grad von $P(x)$ ist l, der von $Q(x)$ ist $l-(g+1)$ und $2g+2$ ist der Grad von $F(x)$, und diese drei Polynome erfüllen die Gleichung

$$P^2(x) - Q^2(x)F(x) = t^2 = u^2 d \in K^\times.$$

Beweis. Die Polynomgrade von $P(x), Q(x)$ und $F(x)$ lassen sich unmittelbar berechnen. Dass $Q(x) \in K[x]$ gilt, ist klar, da $Q(x)$ gerade die Norm von $Q_1(x)$ im Sinne der Polynomnorm in Pohst/Zassenhaus ([78], 5.4.6) ist. Analoges gilt für $F(x)$. Mit Gleichung (2.3) folgt $Q_1^2\,F_1 - t - (\overline{Q_1}^2\overline{F_1} - \bar{t}) = 0$, was nur sein kann, wenn $Q_1^2\,F_1 - t = \overline{Q_1^2\,F_1 - t}$ gilt, so dass also $P(x)$ ebenfalls in $K[x]$ liegen muss. Die Gültigkeit der Gleichung $P^2 - Q^2\,F = t^2$ folgt sofort durch Einsetzen der Polynome analog zum Beweis von Satz 2.2.6. □

Im folgenden Abschnitt werden an Hand der vorgenannten Sätze zwei Familien von Kurven vom Geschlecht 2 konstruiert, die über $\mathbb{Q}$ definiert sind und deren Jacobische Varietäten jeweils einen rationalen Punkt der Ordnung 5 besitzen.

2.2.3 Kurvenfamilien

Konstruktion von Kurven vom Geschlecht 2 mit Punkten der Ordnung 5

Familie 1 Ausgehend von Satz 2.2.6 folgt aus den Bedingungen $l = 5 = 2q_1+f_1 = 2q_2+f_2$ und $6 = f_1+f_2$, dass entweder $(f_1, f_2) = (1, 5)$ oder $= (3, 3)$ gelten muss. In den folgenden Untersuchungen wird nicht vorausgesetzt, dass die Kurve vom Geschlecht 2 einen rationalen Weierstraßpunkt besitzt.[13] Aus diesem Grund wird $(f_1, f_2) = (3, 3)$ und $(q_1, q_2) = (1, 1)$ betrachtet.

Seien also $Q_1 = x - u_1$ und $Q_2 = x - u_2$ aus $\mathbb{Q}[x]$, und seien F_1 und F_2 zwei normierte Polynome vom Grad 3 ebenfalls aus $\mathbb{Q}[x]$. Da diese Polynome laut Satz 2.2.6 die Gleichung

$$Q_1^2 F_1 - Q_2^2 F_2 = 2t \in \mathbb{Q}^\times$$

erfüllen sollen, kann $u_1 = 0$ angenommen werden. (Die Transformation $x \mapsto x + u_1$ hat eine entsprechende Gleichung zur Folge.) Da Q_1 und Q_2 keine gemeinsamen Nullstellen haben, (ansonsten würde die linke Seite der Gleichung eine Nullstelle besitzen,) ist also $u_2 \neq 0$. Daher kann durch $x \mapsto u_2 x$ eine weitere Vereinfachung erreicht und $u_2 = 1$ angenommen werden. [14] Somit ist also die Gleichung $x^2 F_1 - (x-1)^2 F_2 = const.$ zu lösen.

Das Ergebnis beinhaltet der folgende

Satz 2.2.8. *Seien a und b zwei Parameter. Sei die Kurve $\mathcal{C}_{a,b,5}$ durch die Gleichung*

$$y^2 = \left(x^3 + (a-2)x^2 + (2b-2a+1)x + a - 3b\right)\left(x^3 + ax^2 + 2bx + b\right)$$

definiert. Falls die rechte Seite dieser Gleichung keine mehrfache Nullstelle besitzt, so ist $\mathcal{C}_{a,b,5}$ hyperelliptisch und von Geschlecht 2 und in ihrer Jacobischen Varietät existiert ein $\mathbb{Q}(a, b)$-rationaler Punkt der Ordnung 5.[15]

Beweis. Eine einfache Rechnung zeigt, dass die vier Polynome $Q_1 = x$, $Q_2 = x-1$, $F_1 = x^3+(a-2)x^2+(2b-2a+1)x+a-3b$ und $F_2 = x^3+ax^2+2bx+b$ die Gleichung

$$Q_1^2 F_1 - Q_2^2 F_2 = -b$$

[13] Dieser Fall wurde ausführlich von Boxall, Grant und Leprévost in [3] bearbeitet.

[14] Man beachte bei diesen Transformationen, dass sich die Polynome F_1 und F_2 zwar ändern, die Kurve $y^2 = F_1 F_2$ jedoch dieselbe bleibt.

[15] Die Kurve $\mathcal{C}_{a,b,5}$ ist isomorph zu $\mathcal{C}_{-a-1,b,5}$.

erfüllen. Falls nun $b \in \mathbb{Q}^\times$ gewählt wird, so sind die Voraussetzungen von Satz 2.2.6 erfüllt und mit Satz 2.2.5 folgt die Behauptung. □

Nun soll noch die Bedingung der Nichtexistenz mehrfacher Nullstellen der rechten Seite von $\mathcal{C}_{a,b,5}$ untersucht werden. Seien dazu a und b beliebige Parameter. Dann ist die Kurve über $\mathbb{Q}(a,b)$ definiert. Mehrfache Nullstellen können auftreten, wenn diese mehrfach in $F_1(x)$ oder mehrfach in $F_2(x)$ oder jeweils einfach in beiden auftreten. Im letzten Fall wäre die Resultante der beiden Polynome Null. Diese lautet

$$\text{Resultant}\,(F_1(x), F_2(x)) = b,$$

aber $b = 0$ ist ausgeschlossen. Für die anderen beiden Fälle sind die Diskriminanten zu untersuchen. Diese lauten

$$\text{disc}(F_1) = b\left(4\,a^3 + 4\,(b+3)\,a^2 + 4\,(3-7\,b)\,a - (32\,b^2 + 59\,b - 4)\right)$$

und

$$\text{disc}(F_2) = b\left(-4\,a^3 + 4\,b\,a^2 + 36\,b\,a - b\,(32\,b + 27)\right).$$

disc(F_1):

Da $b \neq 0$ ist, muss der zweite Faktor der Diskriminante 0 werden, das heißt

$$b = \tfrac{1}{16}a^2 - \tfrac{7}{16}a - \tfrac{59}{64} \pm \tfrac{2\,a+11}{64}\sqrt{(2\,a+3)\,(2\,a+11)}.$$

Dabei ist $(3+2\,a)\,(2\,a+11)$ genau dann ein Quadrat in $\mathbb{Q}(a,b)$, falls sich a in der Form $a = \frac{11\,k^2-3}{2(1-k^2)}$ für ein gewisses $k \in \mathbb{Q}(a,b)$ schreiben lässt.[16] Somit wird die Diskriminante von F_2 Null, falls für ein $k \in \mathbb{Q}(a,b)$ die Parameter a, b die Werte $a = \frac{11\,k^2-3}{2(1-k^2)}$ und $b = \frac{(3\,k-1)^3}{8(k+1)\,(k-1)^2}$ bzw. $b = \frac{(3\,k+1)^3}{8(k-1)\,(k+1)^2}$ gleichzeitig annehmen.

disc(F_2):

Da wiederum $b \neq 0$ ist, muss der zweite Faktor der Diskriminante 0 werden, das heißt

$$b = \tfrac{1}{16}a^2 + \tfrac{9}{16}a - \tfrac{27}{64} \pm \tfrac{2a-9}{64}\sqrt{(2\,a-1)(2\,a-9)}.$$

Genau für $a = \frac{k^2-9}{2(k^2-1)}$ ist $(2\,a-1)(2\,a-9)$ ein Quadrat in $\mathbb{Q}(a,b)$ und b berechnet sich zu $\frac{(-k-3)^3}{8((k+1)^2\,(k-1))}$ bzw. zu $\frac{(-k+3)^3}{8((k-1)^2\,(k+1))}$.

[16] Die Parametrisierung erhält man ausgehend vom Punkt $(-\frac{3}{2}, 0)$ auf der Quadrik $c^2 = (3+2\,a)\,(2\,a+11)$ und der Untersuchung von $a = \frac{-3+kc}{2}$. Die Wahl von $k = \pm 1$ entspricht dann den beiden Punkten $\pm\infty$ auf der Quadrik.

Nach diesen Überlegungen lässt sich folgende Bemerkung formulieren.

Bemerkung 2.2.9. *Seien a und b beliebige Parameter. Die Kurve $\mathcal{C}_{a,b,5}$ aus Satz 2.2.8 ist hyperelliptisch und von Geschlecht 2, falls a, b folgende Bedingungen erfüllen:*

- $b \neq 0$.
- *Gilt* $(2a+3)(2a+11) = t^2$ *für* $t \in \mathbb{Q}(a,b)$, *dann* $b \neq \frac{4a^2-28a-59}{64} \pm \frac{2a+11}{64}t$.
- *Gilt* $(2a-1)(2a-9) = s^2$ *für* $s \in \mathbb{Q}(a,b)$, *dann* $b \neq \frac{4a^2+36a-27}{64} \pm \frac{2a-9}{64}s$.

Familie 2 Analog zur vorangehenden Ausführungen lässt sich eine weitere Familie mit Hilfe von Satz 2.2.7 über $\mathbb{Q}$ konstruieren. Sei dazu $d \in \mathbb{Q}\backslash\mathbb{Q}^2$.

Mit den selben Gradüberlegungen $l = 5 = 2q_1 + f_1 = 2q_2 + f_2$ und $6 = f_1 + f_2$ wie zuvor und der erneuten Beschränkung auf den Fall $(f_1, f_2) = (3,3)$ gelte $Q_1(x) = x - (v + w\sqrt{d})$. Mit der Transformation $x \mapsto wx + v$ (da $w \neq 0$) lässt sich Q_1 zu $Q_1 = x - \sqrt{d}$ vereinfachen. Die Gleichung $Q_1^2 F_1 - \overline{Q_1}^2 \overline{F_1} = 2u\sqrt{d}$ für ein $u \in \mathbb{Q}^\times$ führt dann zu

$$F_1 = (x^3 + ax^2 + bx + ad) + 2(x^2 + ax + b - d)\sqrt{d}.$$

Somit erhält man

$$Q_1^2 F_1 - \overline{Q_1}^2 \overline{F_1} = 4d(b-d)\sqrt{d},$$

und die gesuchte Polynomfamilie lautet

$$\begin{aligned} F(x) = F_1(x)\overline{F_1}(x) \quad = \quad & x^6 + 2ax^5 + (a^2 + 2b - 4d)x^4 - 2a(3d - b)x^3 \\ & + (b^2 + 8d^2 - 8bd - 2a^2 d)x^2 + 2ad(4d - 3b)x \\ & - d(4b^2 + 4d^2 - 8bd - a^2 d). \end{aligned}$$

Eine Untersuchung von $F(x)$ ergibt, dass $b \neq d$ sein muss, da ansonsten $F(x) = (x^2 - d)^2 (x + a)^2$. Darüber hinaus hat die Kurve $\mathcal{C}_{b,d,0,5}$ für $a = 0$ die Gleichung

$$y^2 = x^6 + 2(b - 2d)x^4 + (8d^2 - 8db + b^2)x^2 - 4d(b - d)^2,$$

deren Jacobische Varietät nach Satz 2.1.7 isogen zu einem Produkt elliptischer Kurven ist[17], was nicht weiter untersucht wird.

[17] Kurven mit sich zerlegenden Jacobischen Varietäten werden z. B. von Howe, Leprévost und Poonen in [28] untersucht.

Sei also $a \neq 0$. Mit der Transformation $x \mapsto ax, b \mapsto b\,a^2$ und $d \mapsto d\,a^2$ erhält man eine Darstellung von $F(x)$, die der Wahl $a = 1$ entspricht. Somit wurde der folgende Satz hergeleitet:

Satz 2.2.10. *Sei b ein Parameter und d ein Element aus $\mathbb{Q} \setminus \mathbb{Q}^2$. Die Kurve $\mathcal{C}_{b,d,1,5}$, die durch die Gleichung*

$$\begin{aligned} y^2 = \quad & x^6 + 2x^5 + (2b - 4d + 1)x^4 + 2(b - 3d)x^3 \\ & +(b^2 + 8d^2 - 8bd - 2d)x^2 - 2d(3b - 4d)x - d(4b^2 - 8bd + 4d^2 - d) \end{aligned}$$

definiert wird, ist generisch hyperelliptisch und von Geschlecht 2 und ihre Jacobische Varietät hat einen $\mathbb{Q}(b)$-rationalen Punkt der Ordnung 5.

Die Igusa-Invarianten[18] der konstruierten Familien $\mathcal{C}_{a,b,5}$ und $\mathcal{C}_{b,d,1,5}$, die auf Grund ihres Umfangs hier nicht wiedergegeben werden, sind nicht konstant, so dass sich durch Spezialisierung der Parameter unendlich viele Kurven vom Geschlecht 2 ergeben, die über $\mathbb{Q}$ definiert sind und in deren Jacobischen Varietäten ein $\mathbb{Q}$-rationaler Punkt der Ordnung 5 existiert. Darüber hinaus kann mit den Methoden von Leprévost [45] bzw. Stoll [91] gezeigt werden, dass die Jacobischen Varietäten dieser Familien generisch einfach sind.

Bei der Konstruktion von $\mathcal{C}_{b,d,1,5}$ war es notwendig, $d \in \mathbb{Q} \setminus \mathbb{Q}^2$ zu wählen, damit Satz 2.2.7 angewandt werden konnte. Die Aussage von Satz 2.2.10 gilt jedoch auch für $d \in \mathbb{Q}^2$, wie die folgende Bemerkung zeigt.

Bemerkung 2.2.11. *Auch für $d \in \mathbb{Q}^2$ ist $\mathcal{C}_{b,d,1,5}$ generisch hyperelliptisch und von Geschlecht 2 und ihre Jacobische Varietät hat einen $\mathbb{Q}(b)$-rationalen Punkt der Ordnung 5.*

Beweis. Wird d in der Kurve $\mathcal{C}_{b,d,1,5}$ durch $d = t^2$ mit $t \in \mathbb{Q}$ ersetzt, so zerlegt sich die rechte Seite in der Form

$$\begin{aligned} y^2 \;=\; & (x^3 + (1 + 2\,t)\,x^2 + (b + 2\,t)\,x - t\,(2\,t^2 - t - 2\,b))\cdot \\ & (x^3 + (1 - 2\,t)\,x^2 + (b - 2\,t)\,x + t\,(2\,t^2 + t - 2\,b)), \end{aligned}$$

wobei der erste Faktor des Produktes genau F_1 der vorangegangenen Konstruktion entspricht. Der zweite Faktor entspricht der formalen Bildung von $\overline{F_1}$; wird dieser F_2 genannt, so gilt $(x-t)^2\,F_1 - (x+t)^2\,F_2 = 4\,t^3\,(b - t^2)$. Für $t \in \mathbb{Q}^\times$ und $b \neq t^2$ sind die Voraussetzungen von Satz 2.2.6 erfüllt und mit Satz 2.2.5 folgt die Behauptung. □

[18] Siehe dazu z. B. die Originalarbeit [29] von Igusa.

Konstruktion von Kurven vom Geschlecht 2 mit Punkten der Ordnung 7

Familie 1 Analog zu dem vorangegangenen Abschnitt werden die Sätze 2.2.6 und 2.2.7 genutzt, um Familien von Kurven zu konstruieren, die über $\mathbb{Q}$ definiert sind, Geschlecht $g = 2$ besitzen und deren Jacobische Varietät einen Punkt der Ordnung $l = 7$ beinhaltet.

Die Polynomgrade aus Satz 2.2.6 müssen für $g = 2$ und $l = 7$ die Zusammenhänge $2q_1+f_1 = 2q_2+f_2 = 7$ und $f_1+f_2 = 6$ erfüllen, was $(f_1, f_2) = (1, 5)$ oder $(3, 3)$ impliziert. Dabei existiert im ersten Fall wieder ein rationaler Weierstraßpunkt in der Jacobischen Varietät, so dass die Techniken von Leprévost (siehe [39] und [40]) angewendet werden können. Aus diesem Grunde wird im Folgenden nur der Fall $(f_1, f_2) = (3, 3)$ und $(q_1, q_2) = (2, 2)$ betrachtet.

Wie bei der Konstruktion von Kurven mit Punkten der Ordnung 5 lassen sich auch hier Q_1 und Q_2 durch eine Transformation vereinfachen, die die Gültigkeit der Gleichung (2.2) nicht ändert.[19] Seien somit $Q_1 = x^2 + q$ und $Q_2 = x^2 + x + p$. Seien darüber hinaus $F_1 = x^3 + a_2x^2 + a_1x + a_0$ und $F_2 = x^3 + b_2x^2 + b_1x + b_0$. Ist weiterhin $w_{p,q}$ der Nenner der Koeffizienten mit der Form

$$w_{p,q} = 3\,p^2 + (q - 2\,p)(3\,q + 1),$$

dann ergeben sich die Koeffizienten von F_1 und F_2 (sortiert nach p) wie folgt:

$$\begin{aligned}
2\,w_{p,q}\,a_2 &= -2\,p^3 + 3(5 + 2\,q)\,p^2 - 2(3\,q^2 + 12\,q + 4)\,p + q(2q^2 + 9\,q + 3),\\
w_{p,q}\,a_1 &= p\,(3\,p^2 - 2(3\,q - 1)\,p + (3\,q^2 - 3\,q - 2))\,,\\
2\,w_{p,q}\,a_0 &= -3p^4 + 2(5q + 6)p^3 - (12\,q^2 + 21\,q + 5)p^2 + 6q(q^2 + 2q + 1)p\\
&\quad -q(q^3 + 3\,q^2 + 3\,q + 1),\\
2\,w_{p,q}\,b_2 &= -2\,p^3 + 3(2\,q + 1)\,p^2 - 6\,q^2\,p + q(2\,q^2 - 3\,q - 1),\\
w_{p,q}\,b_1 &= -p^3 + 6\,q\,p^2 - 3q(3\,q + 1)\,p + 2q^2(2\,q + 1),\\
2\,w_{p,q}\,b_0 &= p^4 - 6\,q\,p^3 + 3q(4\,q + 1)\,p^2 - 10\,q^3\,p + q^2(3\,q^2 - 3\,q - 2).
\end{aligned}$$

Mit dieser Konstruktion ergibt Satz 2.2.6 das folgende Ergebnis:

Satz 2.2.12. *Die Gleichung* $y^2 = (x^3 + a_2x^2 + a_1x + a_0)(x^3 + b_2x^2 + b_1x + b_0)$ *definiert generisch eine hyperelliptische Kurve* $\mathcal{C}_{p,q,7}$ *vom Geschlecht* 2 *über* $\mathbb{Q}(p, q)$*, deren Jacobische Varietät einen rationalen Punkt der Ordnung* 7 *besitzt.*

[19] Sind Q_1, Q_2 in der Form $Q_1 = x^2 + ax + b$ und $Q_2 = x^2 + cx + d$ gegeben, so lautet die Transformation $x \mapsto (c - a)x - \frac{a}{2}$.

Sieht man sich die in Satz 2.2.6 formulierte Gleichung (2.2) für die konstruierten Polynome Q_1, Q_2, F_1 und F_2 genauer an, so ergibt sich

$$Q_1^2(x)F_1(x) - Q_2^2(x)F_2(x) = 2t = \frac{-\left(p^2 - 2\,q\,p + q(q+1)\right)^3}{2w_{p,q}},$$

und die Resultante von F_1 und F_2 lautet

$$\text{Resultant}\left(F_1(x), F_2(x)\right) = 2\,w_{p,q}\left(p^2 - 2\,q\,p + q(q+1)\right).$$

Beides muss ungleich Null sein, damit einerseits $t \in \mathbb{Q}(a,b)^\times$ erfüllt ist, andererseits die rechte Seite der Kurve $\mathcal{C}_{p,b,7}$ keine mehrfachen Nullstellen besitzt. Außerdem müssen auch die Diskriminanten von F_1 und F_2 ungleich Null sein, um mehrfache Nullstellen zu verhindern; eine entsprechende Untersuchung ergibt jedoch keine detaillierteren Bedingungen an p und q.

Bemerkung 2.2.13. *Seien p, q beliebige Parameter. Die Kurve $\mathcal{C}_{p,q,7}$ ist über $\mathbb{Q}(p,q)$ definiert. Es gilt:*

- *Ist $3q+1$ ein Quadrat in $\mathbb{Q}(p,q)$ und ist $p = \frac{1}{3}\left(3\,q + 1 \pm \sqrt{3\,q+1}\right)$, so ist $w_{p,q} = 0$.*
- *Ist $-q$ ein Quadrat in $\mathbb{Q}(p,q)$ und ist $p = q \pm \sqrt{-q}$, so ist $t = 0$.*

Familie 2 Mit Satz 2.2.7 lassen sich weitere Familien von Kurven konstruieren. Sei $Q_1 = x^2 + (u_1 + v_1\sqrt{d})x + (u_0 + v_0\sqrt{d})$. Mit der Transformation $x \mapsto x - \frac{u_1}{2}$ lässt sich u_1 eliminieren, so dass von vorneherein $u_1 = 0$ angenommen werden kann: $Q_1 = x^2 + v_1\sqrt{d}x + (u + v_0\sqrt{d})$. Zur weiteren Vereinfachung lassen sich zwei Fälle unterscheiden: $v_1 = 0$ oder $v_1 \neq 0$. Im ersten Fall ist $Q_1 = x^2 + (u + v\sqrt{d})$ zu untersuchen, was jedoch zu keiner Lösung führt. Im zweiten Fall erhält man durch $x \mapsto v_1 x$ die vereinfachte Form $Q_1 = x^2 + \sqrt{d}\,x + (u + v\sqrt{d})$.[20]

Wird nun F_1 in der Form $F_1 = x^3 + (a_2 + b_2\sqrt{d})\,x^2 + (a_1 + b_1\sqrt{d})\,x + (a_0 + b_0\sqrt{d})$ $= x^3 + a_2\,x^2 + a_1\,x + a_0 + (b_2\,x^2 + b_1\,x + b_0)\sqrt{d}$ angesetzt, so erhält man über die Gleichung (2.3) für die Koeffizienten a_2, b_2, a_1, b_1, a_0 und b_0 Ausdrücke in u und v. Zur vereinfachten Darstellung sei $w_{u,v} = 3\,v^2 - u - d$ der Nenner dieser Koeffizienten:

[20] Die für $v_1 \neq 0$ erlaubte Transformation $x \mapsto v_1 x$ ermöglicht ein Ausklammern von ${v_1}^2$ aus Q_1 und aus $\overline{Q_1}$, was an der Gültigkeit der Gleichung $Q_1^2 F_1 - \overline{Q_2}^2\overline{F_2} = t - \bar{t}$ nichts ändert.

$$\begin{aligned} w_{u,v}\, a_2 &= v\,(3\,u - v^2 + d), \\ b_2 &= -2, \\ w_{u,v}\, a_1 &= -u^2 + 3\,(v^2 - d)\,u + d\,(2\,v^2 - d), \\ w_{u,v}\, b_1 &= -4\,v\,(v^2 + u), \\ w_{u,v}\, a_0 &= v\,\left(3\,u^2 - (v^2 - 3\,d)\,u + d\,(6\,v^2 - d)\right), \\ w_{u,v}\, b_0 &= 2\,\left((-3\,v^2 + d)\,u + v^4\right). \end{aligned}$$

Mit dem entsprechend berechneten $F_1(x)$ und mit $Q_1(x)$ ergibt sich

$$Q_1^2\,F_1 - \overline{Q_1}^2\,\overline{F_1} = \frac{4\,(v^2+u)^3\,d\,\sqrt{d}}{w_{u,v}},$$

und der folgende Satz wurde hergeleitet.

Satz 2.2.14. *Seien u, v Parameter und sei d ein Element aus $\mathbb{Q}\backslash\mathbb{Q}^2$. Die Kurve $\mathcal{C}_{u,v,d,7}$, die durch die Gleichung*

$$\begin{aligned} y^2 = &\left(x^3 + \tfrac{v\,(3\,u - v^2 + d)}{w_{u,v}}\,x^2 - \tfrac{(u^2 - 3(v^2-d)\,u - d\,(2v^2-d))}{w_{u,v}}\,x + \tfrac{v\,(3\,u^2 - (v^2-3d)\,u + d\,(6v^2-d))}{w_{u,v}}\right)^2 \\ &-4\,d\left(x^2 + \tfrac{2\,v\,(v^2+u)}{w_{u,v}}\,x - \tfrac{(-3v^2+d)\,u + v^4)}{w_{u,v}}\right)^2 \end{aligned}$$

definiert ist, ist generisch hyperelliptisch vom Geschlecht 2 und ihre Jacobische Varietät besitzt einen $\mathbb{Q}(u,v)$-rationalen Punkt der Ordnung 7.

In diesem Satz ist v ein echter Parameter, der sich nicht durch Transformation eliminieren lässt. Somit ist Satz 2.2.14 eine allgemeinere Version des entsprechenden Satzes in dem Artikel LPS2 [49] (Theorem 4.2, S. 198), dessen Fassung durch Spezialisierung durch $v = -1$ entsteht.

Auch die dort erwähnte Kurvenfamilie, deren Jacobische Varietäten isogen zu Produkten elliptischer Kurven sind, lässt sich durch $v = 0$ wiederfinden:

$$y^2 = x^2\left(x^2 + \frac{u^2 + 3\,u\,d + d^2}{u + d}\right)^2 - 4\,d\left(x^2 + \frac{u\,d}{u+d}\right)^2.$$

Die Igusa-Invarianten der beiden Familien $\mathcal{C}_{p,q,7}$ und $\mathcal{C}_{u,v,d,7}$ sind nicht konstant und die Jacobischen Varietäten dieser Familien von Kurven vom Geschlecht 2 sind im Allgemeinen einfach. Die Spezialisierung der Parameter dieser Kurven führt zu unendlich vielen Kurven vom Geschlecht 2, die über

$\mathbb{Q}(p,q)$ bzw. über $\mathbb{Q}(u,v)$ definiert sind und deren Jacobische Varietäten jeweils einen $\mathbb{Q}(p,q)$- bzw. $\mathbb{Q}(u,v)$-rationalen Punkt der Ordnung 7 besitzen.

Analog zu Bemerkung 2.2.11 lässt sich auch für $\mathcal{C}_{u,v,d,7}$ folgende Bemerkung formulieren:

Bemerkung 2.2.15. *Auch für $d \in \mathbb{Q}^2$ ist $\mathcal{C}_{u,v,d,7}$ generisch hyperelliptisch vom Geschlecht 2 und ihre Jacobische Varietät besitzt einen $Q(u,v)$-rationalen Punkt der Ordnung 7.*

Der Beweis dieser Bemerkung verläuft analog zum Beweis zu Bemerkung 2.2.11: In den Polynomen $F_1, \overline{F_1}, Q_1$ und $\overline{Q_1}$, mit denen $\mathcal{C}_{u,v,d,7}$ konstruiert wurde, wird d durch $d = t^2$ mit $t \in \mathbb{Q}$ ersetzt. Die erhaltenen Polynome erfüllen die Voraussetzungen von Satz 2.2.6.

Konstruktion von Kurven vom Geschlecht 3 mit Punkten der Ordnung 10

Wie in den beiden vorangegangenen Abschnitten wird mit Hilfe des Satzes 2.2.7 eine Familie von hyperelliptischen Kurven konstruiert, wobei hier $g = 3$ und $l = 10$ gelten soll und der Fall $q_1 = 3$ und $f_1 = 4$ untersucht wird. Da die Vorgehensweise dieselbe wie zuvor ist, wird im Folgenden alleine das Ergebnis angegeben:

Mit

$$\begin{aligned} Q_1 = &\quad x^3 + x^2 + q(x + q - t) - \sqrt{qt}\, x, \\ F_1 = &\quad x^4 + (t - q + 2)x^3 + (1 + 2t)x^2 + (q + t)x + q(t - q^2 + 2qt + q - t^2) \\ &+2(x^2 + (t + 1 - q)x + t)\sqrt{qt}. \end{aligned}$$

gilt die Gleichung

$$Q_1^2 F_1 - \overline{Q_1}^2 \overline{F_1} = 4qt(q - t)^2\sqrt{qt},$$

und damit der folgende

Satz 2.2.16. *Seien q, t zwei Parameter, so dass qt ein Element von $\mathbb{Q} \setminus \mathbb{Q}^2$ ist. Die Kurve $\mathcal{C}_{q,t,10}$ mit der Gleichung*

$$\begin{aligned} y^2 = &\Big(x^4 + (t - q + 2)x^3 + (1 + 2t)x^2 + (q + t)x + q(t - q^2 + 2qt + q - t^2)\Big)^2 \\ &-4qt\Big(x^2 + (t + 1 - q)x + t\Big)^2 \end{aligned}$$

hat generisch Geschlecht 3 *und ihre Jacobische Varietät besitzt einen* $\mathbb{Q}(q,t)$*-rationalen Punkt der Ordnung* 10.

Es lässt sich leicht überprüfen, dass die Klasse des Divisors $\mathcal{O}^+ - \mathcal{O}^-$ eine Ordnung besitzt, die verschieden von 2 und 5 ist, somit muss sie 10 sein. Da das Geschlecht der Kurve 3 ist, können die Igusa-Invarianten nicht benutzt werden. Die Techniken, die von Leprévost entwickelt wurden (siehe [41, 44, 46, 47]) sind jedoch anwendbar und zeigen, dass die Kurve $\mathcal{C}_{q,t,10}$ nicht isotrivial ist. Spezialisierungen der Parameter dieser Kurve erzeugen unendlich viele hyperelliptische Kurven vom Geschlecht 3, die über $\mathbb{Q}$ definiert sind und deren Jacobische Varietäten jeweils einen $\mathbb{Q}$-rationalen Punkt der Ordnung 10 besitzen.

Konstruktion weiterer Familien

Bisher wurden die Sätze 2.2.6 und 2.2.7 mit der im Vergleich zu Satz 2.2.5 vereinfachten Polynomgleichung $Q_1^2F_1 - Q_2^2F_2 = t \in K^\times$ genutzt, um Familien von hyperelliptischen Kurven zu konstruieren. Dies hat den Vorteil, dass die Polynomgrade, die zu betrachten sind, kleiner bleiben. So muss z. B. in $P^2 - Q^2F = t \in K^\times$ das Polynom P den Grad 7 haben, um eine Kurve mit einem Punkt der Ordnung 7 zu konstruieren. Weiter muss F vom Grad 6 sein, damit die Kurve Geschlecht $g = 2$ besitzt. Folglich hat Q Grad 4. Bei der Konstruktion mit Hilfe von Satz 2.2.6 bleiben die Grade von F und Q gleich, aber P hingegen wird nicht betrachtet.

Möchte man von Satz 2.2.5 ausgehend Familien konstruieren, so ist dies eine leichte Aufgabe, wenn man sich z. B. des Artikels von Webb und Yokota [94] bedient. Es ist damit jedoch nicht möglich, große Torsion bei kleinem Geschlecht zu erzeugen. Beispielhaft wird im Folgenden die Konstruktion für Geschlecht $g = 2$ und mögliche Torsion $l = 3, 5$ bzw. $g = 3$ und $l = 5, 7$ durchgeführt.

Der Artikel [94] von Webb und Yokota beschäftigt sich mit polynomialen Pell-Gleichungen der Form $X^2 - DY^2 = 1$, wobei die auftretenden Polynome X, D, Y ganzzahlige Koeffizienten besitzen. $\Omega = U + V\sqrt{D}$ heißt eine Lösung dieser Gleichung, falls $U^2 - DV^2 = 1$ gilt. Ω heißt fundamentale Lösung, falls zusätzlich gilt, dass Ω ganzzahlige Koeffizienten besitzt und jede weitere ganzzahlige Lösung sich als Potenz Ω^n schreiben lässt. Ziel des Artikels ist es, fundamentale Lösungen in Abhängigkeit von D anzugeben. Eine Hauptaussage ist dabei in Theorem 2, Seite 131 formuliert:

Satz 2.2.17 (Webb/Yokota [94], Theorem 2). *Sei $D = A^2 + 2C$ ein Polynom in $\mathbb{Z}[x]$ mit $A \in \mathbb{Z}[x]$ und $B = A/C \in \mathbb{Z}[x]$, und bezeichne $\sigma(B)$ das Vorzeichen des führenden Koeffizienten von B. Dann gilt:*

$$\Omega = \begin{cases} A + \sqrt{D} & falls \;\; 2C = -\frac{1}{k^2}, k = 1, \\ (kA + k\sqrt{D})^2 & falls \;\; 2C = -\frac{1}{k^2}, k \neq 1, \\ \sigma(B)(AB + 1 + B\sqrt{D}) & falls \;\; 2C \neq -\frac{1}{k^2}. \end{cases}$$

Ähnliche Aussagen werden für $B \notin \mathbb{Z}[x]$ und $2B \in \mathbb{Z}[x]$ bzw. $B \notin \mathbb{Z}[x]$ und $pB \in \mathbb{Z}[x]$ für eine Primzahl $p \neq 2$ bewiesen.

Vergleicht man $P^2 - Q^2F = t$ aus Satz 2.2.5 mit $U^2 - DV^2 = 1$ aus dem zitierten Artikel, so übernimmt D die Rolle von F und U die Rolle von P, so dass der Grad von D in Zusammenhang mit dem Geschlecht g der hyperelliptischen Kurve $y^2 = F(x)$ steht (konkret $deg(D) = 2g + 2$) und der Grad von U die gewünschte Ordnung l eines Torsionspunktes dieser Kurve ist. Wird nach Torsionspunkten mit Primzahlordnung gesucht, führt nur der 1. und der 3. Fall im zitierten Satz weiter. [21] Aus diesem Grund sind auch die anderen Sätze des Artikels nicht nutzbar, da dort V nie primen Grad besitzen kann. Außerdem ist auch der 1. Fall im zitierten Satz nicht von großem Interesse, da dann $U = A$ und $F = A^2 - 1$ gilt, was die enge Beziehung $l = g + 1$ zur Folge hat.

Aus diesen Gründen wird nur der 3. Fall, also $2C \neq -\frac{1}{k^2}$ näher betrachtet. Rechnerisch ergibt sich $l = deg(U) = deg(A) + deg(B)$ mit $g = deg(A) - 1$. Soll nun l prim sein bei $g = 2, 3$, so ergeben sich mit $C \mid A$ folgende vier Möglichkeiten (unter der Voraussetzung, dass A, B normiert sind), wobei die Kurve $y^2 = F(x)$ einen rationalen Punkt besitzt, wenn $deg(C) = 1$ gilt:

g	l	$deg(A)$	$deg(B)$	$deg(C)$	$F = D = A^2 + 2C = C(AB + 2)$
2	3	3	0	3	$(x^3+ax^2+bx+c)(x^3+ax^2+bx+c+2)$
2	5	3	2	1	$(x+a)((x+a)(x^2+bx+c)^2+2)$
3	5	4	1	3	$(x^3+ax^2+bx+c)((x+d)^2(x^3+ax^2+bx+c)+2)$
3	7	4	3	1	$(x+a)((x+a)(x^3+bx^2+cx+d)^2+2)$

[21] Im 2. Fall besitzt U die Gestalt $k^2A^2 + k^2D = k^2(A^2 + A^2 + 2C) = 2k^2(A^2 + C)$, so dass der Grad von U gerade $2\,deg(A)$ ist, da $deg(C) \leq deg(A)$ gilt.

Hyperelliptische Modulkurven $X_0(N)$ in den konstruierten Familien

Eine Untersuchung der in den vorgangegangenen Abschnitten konstruierten Familien im Hinblick auf die in Abschnitt 2.2.1 angegebenen Modulkurven $X_0(N)$ ergibt, dass letztere sich in den Familien wiederfinden lassen. So enthält die Familie $\mathcal{C}_{a,b,5}$ die Kurve $X_0(31)$, die sich durch die Wahl der Parameter $(a,b) = (5, \frac{31}{8})$ ergibt. Darüber hinaus findet man mit $(a,b) = (-\frac{7}{2}, \frac{11}{8})$ die Kurve $X_0(22)$ vom Geschlecht 2, die Rovira [22] mit der Gleichung $y^2 = x^6 + 12\,x^5 + 56\,x^4 + 148\,x^3 + 224\,x^2 + 192\,x + 64$ angibt. In der Kurvenschar $\mathcal{C}_{u,v,d,7}$ liegt $X_0(29)$, was sich durch $(u,v,d) = (-\frac{57}{25}, -1, \frac{116}{25})$ bestätigt. Und schließlich entspricht die Kurve $X_0(41)$ den Parametern $(q,t) = (\frac{1}{50}, \frac{41}{50})$ in $\mathcal{C}_{q,t,10}$.

Darüber hinaus gibt es für alle betrachteten N eine Zerlegung von $f_N(x)$ über $\mathbb{Q}$ oder über einem quadratischen Zahlkörper in der Form

$$f_N(x) = F_{1,N}(x)F_{2,N}(x),$$

und es existieren Polynome $Q_{1,N}$ und $Q_{2,N}$ in $\mathbb{Q}[x]$, so dass die Gleichung

$$Q_{1,N}^2 F_{1,N} - Q_{2,N}^2 F_{2,N} = 2t$$

für ein gewisses $t \in \mathbb{Q}^\times$ erfüllt ist, oder es gibt ein Polynom $Q_{1,N}$ aus $\mathbb{Q}(\sqrt{d})$ für $d \in \mathbb{Q} \setminus \mathbb{Q}^2$, so dass die Gleichung

$$Q_{1,N}^2 F_{1,N} - \overline{Q_{1,N}}^2 \overline{F_{1,N}} = t - \bar{t} = 2u\sqrt{d},$$

für ein gewisses $u \in \mathbb{Q}^\times$ gilt.

In der folgenden Tabelle werden die einzelnen Polynome und die Werte $2t$ bzw. $t - \bar{t}$ aufgeführt. Im letzteren Fall wird die Bezeichnung $Q_{2,N} = \overline{Q_{1,N}}$ beibehalten, und $F_{2,N} = \overline{F_{1,N}}$. Somit kann die Modulfunktion φ_N als eine Funktion der Polynome Q_1 und Q_2 ausgedrückt werden.

(Ein Druckfehler im entsprechenden Artikel LPS2 [49] bei den Polynomen $F_{1,41}(x)$ und $F_{2,41}(x)$ ist hier berichtigt.)

g	N	l	$f_N(x) = F_{1,N}(x)F_{2,N}(x), Q_{1,N}(x), Q_{2,N}(x)$ und $Q_{1,N}^2F_{1,N} - Q_{2,N}^2F_{2,N}$
2	23	11	$F_{1,23}(x) = x^3 - x + 1$ $F_{2,23}(x) = x^3 - 8\,x^2 + 3\,x - 7$ $Q_{1,23}(x) = x^4 - 17\,x^3 + 91\,x^2 - 143\,x - 40$ $Q_{2,23}(x) = x^4 - 13\,x^3 + 45\,x^2 - 9\,x - 82$ $Q_{1,23}^2F_{1,23} - Q_{2,23}^2F_{2,23} = 2^2\,23^3$

g	N	l	$f_N(x) = F_{1,N}(x)F_{2,N}(x), Q_{1,N}(x), Q_{2,N}(x)$ und $Q_{1,N}^2F_{1,N} - Q_{2,N}^2F_{2,N}$
2	29	7	$F_{1,29}(x) = x^3 + (1+\sqrt{29})x^2 + (\frac{11+3\sqrt{29}}{2})x + 5 + \sqrt{29}$ $F_{2,29}(x) = x^3 + (1-\sqrt{29})x^2 + (\frac{11-3\sqrt{29}}{2})x + 5 - \sqrt{29}$ $Q_{1,29}(x) = x^2 - (\frac{7+\sqrt{29}}{2})x - (\frac{1-3\sqrt{29}}{2})$ $Q_{2,29}(x) = x^2 - (\frac{7-\sqrt{29}}{2})x - (\frac{1+3\sqrt{29}}{2})$ $Q_{1,29}^2F_{1,29} - Q_{2,29}^2F_{2,29} = 2^2\,29\sqrt{29}$
2	31	5	$F_{1,31}(x) = x^3 - 17\,x - 27$ $F_{2,31}(x) = x^3 + 4\,x^2 + 3\,x + 1$ $Q_{1,31}(x) = x - 2$ $Q_{2,31}(x) = x - 4$ $Q_{1,31}^2F_{1,31} - Q_{2,31}^2F_{2,31} = -2^2\,31$
3	41	10	$F_{1,41}(x) = x^4 + 2x^3 - (6-\sqrt{41})x^2 - (21-3\sqrt{41})x - (\frac{31-5\sqrt{41}}{2})$ $F_{2,41}(x) = x^4 + 2x^3 - (6+\sqrt{41})x^2 - (21+3\sqrt{41})x - (\frac{31+5\sqrt{41}}{2})$ $Q_{1,41}(x) = x^3 - 4x^2 - (\frac{5+\sqrt{41}}{2})x + \frac{29+3\sqrt{41}}{2}$ $Q_{2,41}(x) = x^3 - 4x^2 - (\frac{5-\sqrt{41}}{2})x + \frac{29-3\sqrt{41}}{2}$ $Q_{1,41}^2F_{1,41} - Q_{2,41}^2F_{2,41} = 2^2 41\sqrt{41}$
4	47	23	$F_{1,47}(x) = x^5 - x^4 + x^3 + x^2 - 2\,x + 1$ $F_{2,47}(x) = x^5 - 5\,x^4 + 5\,x^3 - 15\,x^2 + 6\,x - 11$ $Q_{1,47}(x) = x^9 - 17\,x^8 + 112\,x^7 - 355\,x^6 + 546\,x^5 - 388\,x^4 + 149\,x^3 + 292\,x^2 - 740\,x + 36$ $Q_{2,47}(x) = x^9 - 15\,x^8 + 84\,x^7 - 207\,x^6 + 172\,x^5 + 120\,x^4 - 283\,x^3 + 266\,x^2 - 66\,x - 194$ $Q_{1,47}^2F_{1,47} - Q_{2,47}^2F_{2,47} = 2^2\,47^3$
5	59	29	$F_{1,59}(x) = x^3 + 2x^2 + 1$ $F_{2,59}(x) = x^9 + 2\,x^8 - 4\,x^7 - 21\,x^6 - 44\,x^5 - 60\,x^4 - 61\,x^3 - 46\,x^2 - 24\,x - 11$ $Q_{1,59}(x) = x^{13} - 7\,x^{12} + 2\,x^{11} + 70\,x^{10} - 68\,x^9 - 276\,x^8 + 161\,x^7 + 644\,x^6 + 210\,x^5$ $\quad - 808\,x^4 - 727\,x^3 - 202\,x^2 + 332\,x + 720$ $Q_{2,59}(x) = x^{10} - 7\,x^9 + 4\,x^8 + 63\,x^7 - 99\,x^6 - 166\,x^5 + 306\,x^4 + 183\,x^3 - 194\,x^2 - 312\,x + 166$ $Q_{1,59}^2F_{1,59} - Q_{2,59}^2F_{2,59} = 2^2\,59^3$
6	71	35	$F_{1,71}(x) = x^7 + 4\,x^6 + 5\,x^5 + x^4 - 3\,x^3 - 2\,x^2 + 1$ $F_{2,71}(x) = x^7 - 7\,x^5 - 11\,x^4 + 5\,x^3 + 18\,x^2 + 4\,x - 11$ $Q_{1,71}(x) = x^{14} - 8\,x^{13} + 7\,x^{12} + 82\,x^{11} - 132\,x^{10} - 414\,x^9 + 610\,x^8 + 1533\,x^7 - 1366\,x^6 - 3829\,x^5$ $\quad + 1313\,x^4 + 5207\,x^3 + 338\,x^2 - 3100\,x - 612$ $Q_{2,71}(x) = x^{14} - 6\,x^{13} - 5\,x^{12} + 76\,x^{11} - 8\,x^{10} - 408\,x^9 + 2\,x^8 + 1231\,x^7 + 484\,x^6 - 2049\,x^5$ $\quad - 1575\,x^4 + 1185\,x^3 + 1570\,x^2 + 500\,x - 310$ $Q_{1,71}^2F_{1,71} - Q_{2,71}^2F_{2,71} = 2^2\,71^3$

Kapitel 3

Zahlentheoretische Anwendungen

Die in Abschnitt 1.3.1 angegebenen Gleichungen elliptischer Kurven E_l mit einem Torsionspunkt der Ordnung $3 \leq l \leq 10$ bzw. $l = 12$ werden in diesem Kapitel zur Konstruktion von Polynomfamilien mit rationalen Koeffizienten vom Grad l genutzt, deren Zerfällungskörper über $\mathbb{Q}$ jeweils die Galoisgruppe D_l und in Spezialfällen deren Untergruppe C_l (siehe Abschnitt 3.2) besitzt. Darüber hinaus werden ausgehend von den in Abschnitt 2.2.3 berechneten Kurvenfamilien vom Geschlecht 2 mit einem Torsionspunkt der Ordnung $l = 5, 7$ imaginärquadratische Zahlkörper angegeben, deren Idealklassengruppen einen 5-Rang 3 und einen 7-Rang 2 besitzen. Bei den folgenden Berechnungen wurden die Computeralgebrasysteme KANT [32], MAGMA [52], MAPLE [53] und PARI [77] intensiv genutzt.

3.1 Zahlkörper mit Galoisgruppe D_l

3.1.1 Allgemeine Konstruktion

Sei $\mathbb{Q}(E_l)$ der von E_l definierte elliptische Funktionenkörper. Für die Abbildung $n_l : E_l \to \mathbb{Q}(E_l)$ ist für $P \in E_l$ das Bild

$$n_l(P) := \sum_{i=0}^{l-1} x(P \oplus i\,A)$$

eine Funktion in $\mathbb{Q}(E_l)$. Dabei ist $P = (x_P, y_P)$ ein beliebiger, fest gewählter Punkt auf E_l, $A = (0, 0)$ ist ein Punkt der Ordnung l auf E_l und das Bild $x(P \oplus iA)$ der Funktion $x \in \mathbb{Q}(E_l)$ ist als $x(P \oplus iA) = x_{P \oplus iA}$ zu verstehen.

Korollar 3.1.1. *Die Koordinaten von $P \oplus iA$ sind rationale Ausdrücke in x_P, y_P und den Parametern von E_l.*

Beweis. Dies folgt sofort aus den Formeln zur Punktaddition 1.1.4. □

Lemma 3.1.2. *Wird der Startpunkt P durch den Punkt $P \oplus jA$ für ein $0 \leq j \leq l-1$ ersetzt, so gilt*

$$n_l(P) = \sum_{i=0}^{l-1} x(P \oplus iA) = \sum_{i=0}^{l-1} x((P \oplus jA) \oplus iA) = n_l(P \oplus jA).$$

Die Aussage gilt auch, wenn $j \in \mathbb{Z}$ beliebig gewählt wird.

Beweis. Da A ein l-Torsionspunkt der elliptischen Kurve E_l ist, gilt $lA = \mathcal{O}$. Damit ist $P \oplus jA \oplus iA = P \oplus (\overline{j+i})A$, wobei $\overline{j+i}$ der Repräsentant von $i+j$ in $\mathbb{Z}/l\mathbb{Z}$ ist. Durchläuft nun i alle Zahlen 0 bis $l-1$, so durchläuft auch $\overline{j+i}$ alle Zahlen 0 bis $l-1$. □

Nach der Konstruktion von $n_l(P)$ entsteht der über $\mathbb{Q}(E_l)$ definierte rationale Ausdruck in x_P (und den Parametern von E_l)

$$n_l(P) = \frac{{x_P}^l + (\ldots){x_P}^{l-2} + (\ldots){x_P}^{l-3} + \ldots + (\ldots)}{{x_P}^{l-1} + (\ldots){x_P}^{l-2} + (\ldots){x_P}^{l-3} + \ldots + (\ldots)},$$

der unmittelbar zur Gleichung

$$0 \quad = \quad {x_P}^l - n_l(P){x_P}^{l-1} + (\ldots){x_P}^{l-2} + \ldots \tag{3.1}$$

führt.

Wird nun die Bezeichnung $n_l(P)$ durch n vereinfacht und wird das Polynom $F_l(x)$ vom Grad l durch $F_l(x) := x^l - n\,x^{l-1} + (\ldots)x^{l-2} + \ldots$ in Übernahme der Koeffizienten aus (3.1) definiert, so gilt, dass $F_l(x_P) = 0$ ist. Da aber nach Lemma 3.1.2 zu jedem Startpunkt $P \oplus A$, $P \oplus 2A$, $P \oplus 3A$, ... die rationale Funktion n_l dieselbe ist, sind auch die x-Koordinaten der anderen Startpunkte Nullstellen von $F_l(x)$. Es gilt also:

Satz 3.1.3.

$$F_l(x) = \prod_{i=0}^{l-1}(x - x(P \oplus iA)).$$

Offensichtlich gilt bezüglich der Irreduzibilität von $F_l(x)$ folgendes:

Bemerkung 3.1.4. *$F_l(x)$ zerfällt über $\mathbb{Q}$ in Linearfaktoren, falls $x(P)$ rational ist. Anders ausgedrückt: Falls n aus einem Punkt P mit rationaler x-Koordinate $x(P) = x_P$ konstruiert wird, zerfällt $F_l(x)$ in Linearfaktoren.*

Für die Galoisgruppe von $F_l(x)$ über $\mathbb{Q}(n, c)$ (exakter, für die Galoisgruppe des Zerfällungskörpers von $F_l(x)$ über $\mathbb{Q}(n, c)$) gilt:

Satz 3.1.5. *Sei $F_l(x)$ irreduzibel und die davon erzeugte Körpererweiterung nicht normal. Dann ist*

$$Gal(F_l(x)) = D_l.$$

Beweis. Ist $F_l(x)$ irreduzibel, so definiert dieses Polynom eine Körpererweiterung vom Grad l über $\mathbb{Q}(n, c)$, wobei c der Parameter von E_l ist (bei $l = 3$ steht c für zwei Parameter). Diese Körpererweiterung ist nach Voraussetzung nicht schon der Zerfällungskörper von $F_l(x)$. Da die Nullstellen von $F_l(x)$ gerade die x-Koordinaten der Punkte P, $P \oplus A$, ..., $P \oplus (l-1)A$ sind, die jeweils rationale Ausdrücke in x_P und y_P sind (siehe Korollar 1.1.4), muss zu dem von $F_l(x)$ erzeugten Körper $\mathbb{Q}(n, c)(x_P)$ noch y_P hinzuadjungiert werden, um eine (minimale) Körpererweiterung zu erhalten, über der $F_l(x)$ zerfällt. Diese wird durch die Gleichung der elliptischen Kurve E_l erzeugt, exakter: durch das Polynom zweiten Grades in y über $\mathbb{Q}(n, c)(x_P)$ der Gestalt $y^2+((1-c)x_P-b)\,y-(x_P^3-bx_P^2)$ (bzw. für $l = 3$ durch $y^2+(a_1x_P+a_3)y-x_P^3$). Somit ist $\mathbb{Q}(n, c)(x_P, y_P)$ der Zerfällungskörper von $F_l(x)$ und die Galoisgruppe der galoisschen Körpererweiterung besitzt $2l$ Elemente. Ist nun l eine Primzahl (also $l \in \{3, 5, 7\}$), so folgt unmittelbar, dass die Galoisgruppe $Gal(\mathbb{Q}(n, c)(x_P, y_P) \,/\, \mathbb{Q}(n, c)) = D_l$ ist. Ist l keine Primzahl, so zeigen Berechnungen mit MAPLE [53] (für $l \in \{4, 6, 8\}$ und F_l in parametrisierter Form) bzw. MAGMA [52] (für $l \in \{9, 10, 12\}$ und Spezialisierungen von n und den Kurvenparametern von E_l), dass auch dann D_l die Galoisgruppe ist.[1] □

3.1.2 Konstruktion der Polynome

Die explizite Konstruktion der Polynome $F_l(x)$ folgt den vorstehenden Ausführungen: Es müssen in jedem der neun Fälle $3 \le l \le 10$ und $l = 12$ die Punkte iA und $P \oplus iA$ für $1 \le i \le l-1$ berechnet werden. Mit diesen ergibt sich $n_l = n_l(P)$ und daraus das gesuchte Polynom $F_l(x) = x^l - n\,x^{l-1} + \cdots$.

[1] Bei geeigneter Spezialisierung von n und den Parametern von E_l treten Untergruppen der D_l auf. Siehe dazu die Abschnitte 3.2 und 3.3.

1. Fall: $l = 3$

Die mit den Formeln zur Punktaddition in Korollar 1.1.4 berechneten Punkte P, $P \oplus A$ und $P \oplus 2A$ haben folgende x-Koordinaten:

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$-\frac{a_3\, y_P}{{x_P}^2}$
$P \oplus 2A$	$\frac{a_3\,(y_P + a_1\, x_P + a_3)}{{x_P}^2}$

Daraus berechnet sich $n_3 = \frac{{x_P}^3 + a_1\, a_3\, x_P + {a_3}^2}{{x_P}^2}$. Das zugehörige Polynom mit Galoisgruppe D_3 lautet

$$F_3(x) = x^3 - n x^2 + a_1\, a_3\, x + {a_3}^2.$$

Mit der Transformation $x \mapsto \frac{a_3}{x}$ kommt man zu der Polynomfamilie

$$\tilde{F}_3(x) = x^3 + a_1\, x^2 - n\, x + a_3,$$

die dieselben Körper wie $F_3(x)$ erzeugt. Die Polynomdiskriminanten lauten:

$$\begin{aligned} \operatorname{disc}(F_3) &= a_3^2\,(4\,n^3 + a_1^2\, n^2 - 18\, a_1\, a_3\, n - 27\, a_3^2 - 4\, a_3\, a_1^3), \\ \operatorname{disc}(\tilde{F}_3) &= 4\, n^3 + a_1^2\, n^2 - 18\, a_1\, a_3\, n - 27\, a_3^2 - 4\, a_3\, a_1^3. \end{aligned}$$

2. Fall: $l = 4$

Die x-Koordinaten der vier benötigten Punkte lauten:

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{y_P\, b}{{x_P}^2}$
$P \oplus 2A$	$\frac{b\, x_P}{x_P - b}$
$P \oplus 3A$	$-\frac{b(y_P + x_P - b)}{{x_P}^2}$

Es ergibt sich daraus $n_4 = \frac{{x_P}^4 - b\,{x_P}^2 + 2\,b^2\,x_P - b^3}{(x_P - b)\,{x_P}^2}$. Das entsprechende Polynom mit Galoisgruppe D_4 lautet

$$F_4(x) = x^4 - n\,x^3 + b\,(n-1)\,x^2 + 2\,b^2\,x - b^3$$

und führt mit der Transformation $x \mapsto \frac{b}{x}$ zu

$$\tilde{F}_4(x) = x^4 - 2\,x^3 + (1-n)\,x^2 + n\,x - b,$$

wobei sich die Polynomdiskriminanten zu

$$\begin{aligned} \mathrm{disc}(F_4) &= b^6\,(4\,n + 1 - 16\,b)\,(4\,b + n^2)^2, \\ \mathrm{disc}(\tilde{F}_4) &= (4\,n + 1 - 16\,b)\,(4\,b + n^2)^2 \end{aligned}$$

berechnen.

3. Fall: $l = 5$

Die x-Koordinaten der fünf benötigten Punkte lauten:

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{b\,y_P}{{x_P}^2}$
$P \oplus 2A$	$\frac{b\left(-b\,y_P + {x_P}^2 + b(b-2)x_P + b^2\right)}{(b - x_P)^2}$
$P \oplus 3A$	$\frac{b\,(b\,y_P + x_P(x_P - b))}{(b - x_P)^2}$
$P \oplus 4A$	$\frac{b\,(-y_P + x_P(b-1) + b)}{{x_P}^2}$

Es ergibt sich daraus $n_5 = \frac{{x_P}^5 + b\,(b^2 - b - 1)\,{x_P}^3 - b^2\,(b-3)\,{x_P}^2 + b^3\,(b-3)\,x_P + b^4}{{x_P}^2\,(x_P - b)^2}$. Das zugehörige Polynom mit Galoisgruppe D_5 lautet

$$F_5(x) = x^5 - n\,x^4 + b\,(2n + b^2 - b - 1)\,x^3 - b^2\,(n + b - 3)\,x^2 + b^3\,(b-3)\,x + b^4$$

bzw. nach Transformation $x \mapsto \frac{b}{x}$

$$\tilde{F}_5(x) = x^5 + (b-3)\,x^4 - (n+b-3)\,x^3 + (2\,n+b^2-b-1)\,x^2 - n\,x + b$$

mit Diskriminanten

$$\begin{aligned} \mathrm{disc}(F_5) &= b^{14}\left(4\,n^3+(b^2-30b+1)\,n^2-2b\,(3b+1)\,(4b-7)\,n-b\,(4b^4-4b^3-40b^2+91b-4)\right)^2, \\ \mathrm{disc}(\tilde{F}_5) &= b^2\left(4\,n^3+(b^2-30b+1)\,n^2-2b\,(3b+1)\,(4b-7)\,n-b\,(4b^4-4b^3-40b^2+91b-4)\right)^2. \end{aligned}$$

Die Substitution $(x,n,b) \mapsto (\frac{s}{x}, -u, s)$ für $F_5(x)$ bzw. $(n,b) \mapsto (-u,s)$ für $\tilde{F}_5(x)$ führt zur generischen Familie $B_{s,u}(x)$ von Brumer, die Martinais und Schneps [54] zitiert haben. (Siehe auch LPS1 [48].)

Diese Familie ist nach Brumer in folgendem Sinne generisch: für jeden Körper L, der $\mathbb{Q}$ enthält und eine galoissche Erweiterung L' mit Galoisgruppe D_5 besitzt, gilt, dass L' der Zerfällungskörper eines Polynoms der Form $B_{s,u}(x)$ mit $s,u \in L$ ist.

Auch Kihel hat in [33] eine ebenfalls zu $B_{s,u}(x)$ durch $(x,s,u) \mapsto (-x, S+3, T+2S+5)$ isomorphe Familie beschrieben, die von Darmon ([8]) konstruiert worden war.

4. Fall: $l = 6$

In diesem Fall ergibt sich

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{c(c+1)\,y_p}{{x_P}^2}$
$P \oplus 2A$	$\frac{c(c+1)\left(-c\,y_P+{x_P}^2-2c\,x_P+c^2(c+1)\right)}{(c(c+1)-x_P)^2}$
$P \oplus 3A$	$\frac{c\,(\,c(c+1)-x_P\,)}{c-x_P}$
$P \oplus 4A$	$\frac{c(c+1)(\,c\,y_P-x_P(\,c(c+1)-x_P\,)\,)}{(\,c(c+1)-x_P\,)^2}$
$P \oplus 5A$	$\frac{c(c+1)(\,-y_P+(c-1)x_P+c(c+1)\,)}{{x_P}^2}$

und daraus

$$n_6 = \frac{{x_P}^6 - c(c+1)(4c+1){x_P}^4 + 2c^2(c+2)(c+1)^2{x_P}^3 - 2c^3(c+3)(c+1)^2{x_P}^2 + 4c^4(c+1)^3 x_P - c^5(c+1)^4}{{x_P}^2(x_P-c)(x_P-c(c+1))^2}.$$

Das Polynom mit Galoisgruppe D_6 lautet

$$\begin{aligned} F_6(x) &= x^6 - n\,x^5 + \\ &\quad c\,((2c+3)n - (c+1)(4c+1))x^4 - \\ &\quad c^2(c+1)((c+3)n - 2(c+2)(c+1))x^3 + \\ &\quad c^3(c+1)^2(n-2(c+3))\,x^2 + \\ &\quad c^4(c+1)^3\,4\,x - c^5(c+1)^4, \end{aligned}$$

und mit $x \mapsto \frac{c\,(c+1)}{x+1}$ erhält man

$$\begin{aligned} \tilde{F}_6(x) &= x^6 + 2\,x^5 - (n - 2\,c - 1)\,x^4 + \\ &\quad (n-2\,c)\,(c-1)\,x^3 + c\,(n-2\,c-1)\,x^2 + 2\,c^2\,x - c^3. \end{aligned}$$

Beide Polynome erzeugen dieselben Körper. Die Diskriminanten lauten

$$\operatorname{disc}(F_6) = c^{26}(c+1)^{12}\,(-4\,n + (c+1)\,(27\,c-1))^2\,(n^2 - 4\,c\,n + 4\,c\,(c+1))^3,$$
$$\operatorname{disc}(\tilde{F}_6) = c^6\,(c+1)^2\,(-4\,n + (c+1)\,(27\,c-1))^2\,(n^2 - 4\,c\,n + 4\,c\,(c+1))^3.$$

5. Fall: $l = 7$

In diesem Fall ergibt sich

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{d^2\,(d-1)\,y_P}{{x_P}^2}$
$P \oplus 2A$	$\frac{d^2\,(d-1)\left(d\,(1-d)\,y_P + {x_P}^2 + d\,(d-1)\,(d^2-2\,d-1)\,x_P + d^3\,(d-1)^2\right)}{(x_P - d^2\,(d-1))^2}$
$P \oplus 3A$	$\frac{d\,(d-1)\left((d-1)^2\,y_P + (x_P - d + 1)\,(x_P - d^2\,(d-1))\right)}{(x_P - d\,(d-1))^2}$
$P \oplus 4A$	$\frac{d\,(d-1)\left(-(d-1)^2\,y_P + {x_P}^2 + d^2\,(d-1)\,(d-3)\,x_P + d^3\,(d-1)^2\right)}{(x_P - d\,(d-1))^2}$
$P \oplus 5A$	$\frac{d^2\,(d-1)\left(d\,(d-1)\,y_P + x_P\,(x_P - d^2\,(d-1))\right)}{(x_P - d^2\,(d-1))^2}$
$P \oplus 6A$	$\frac{d^2\,(d-1)\left(-y_P + (d^2-d-1)\,x_P + d^2\,(d-1)\right)}{{x_P}^2}$

und daraus

$$\begin{aligned} n_7 &= \Big({x_p}^7 + d\,(d-1)\,(d^5 - 2\,d^4 - 7\,d^3 + 9\,d^2 - 3\,d + 1)\,{x_p}^5 - d^3\,(4\,d^4 - 17\,d^3 + 12\,d^2 - 5\,d + 1)\,(d-1)^2\,{x_p}^4 + \\ &\quad d^4\,(d^5 - 3\,d^4 - 4\,d^2 - 3\,d - 1)\,(d-1)^3\,{x_p}^3 - d^6\,(d+1)\,(d^2 - 3\,d - 3)\,(d-1)^4\,{x_p}^2 + d^8\,(d^2 - 3\,d - 3)\,(d-1)^5\,x_p + \\ &\quad d^{10}\,(d-1)^6 \Big) / \Big({x_p}^2\,(x_p - d^2\,(d-1))^2\,(x_p - d\,(d-1))^2 \Big). \end{aligned}$$

Das zugehörige Polynom mit Galoisgruppe D_7 lautet

$$\begin{aligned} F_7(x) &= x^7 - n\,x^6 + \\ &\quad d\,(d-1)\,(2\,(d+1)\,n + d^5 - 2\,d^4 - 7\,d^3 + 9\,d^2 - 3\,d + 1)\,x^5 - \\ &\quad d^2\,(d-1)^2\,((d^2 + 4\,d + 1)\,n + d\,(4\,d^4 - 17\,d^3 + 12\,d^2 - 5\,d + 1))\,x^4 + \\ &\quad d^4\,(d-1)^3\,(2\,(d+1)\,n + d^5 - 3\,d^4 - 4\,d^2 - 3\,d - 1)\,x^3 - \\ &\quad d^6\,(d-1)^4\,(n + (d+1)\,(d^2 - 3\,d - 3))\,x^2 + \\ &\quad d^8\,(d-1)^5\,(d^2 - 3\,d - 3)\,x + d^{10}\,(d-1)^6 \end{aligned}$$

bzw. in kürzerer Form nach $x \mapsto \frac{d^2\,(d-1)}{x}$

$$\begin{aligned} \tilde{F}_7(x) &= x^7 + (d^2 - 3\,d - 3)\,x^6 - (n + (d+1)\,(d^2 - 3\,d - 3))\,x^5 + \\ &\quad (2\,n\,(d+1) + d^5 - 3\,d^4 - 4\,d^2 - 3\,d1)\,x^4 - \\ &\quad ((d^2 + 4\,d + 1)\,n + d\,(4\,d^4 - 17\,d^3 + 12\,d^2 - 5\,d + 1))\,x^3 + \\ &\quad d\,(2\,(d+1)\,n + d^5 - 2\,d^4 - 7\,d^3 + 9\,d^2 - 3\,d + 1)\,x^2 - \\ &\quad n\,d^2\,x + (d-1)\,d^4 \end{aligned}$$

mit den Polynomdiskriminanten

$$\begin{aligned} \mathrm{disc}(F_7) &= d^{44}\,(d-1)^{44}\,(4\,n^3 + (d^4 - 30\,d^3 + 3\,d^2 + 26\,d + 1)\,n^2 - \\ &\quad 2\,d\,(d-1)\,(12\,d^5 - 24\,d^4 - 91\,d^3 + 115\,d^2 - 29\,d + 12)\,n - \\ &\quad d\,(d-1)\,(4\,d^9 - 8\,d^8 - 136\,d^7 + 612\,d^6 - 916\,d^5 + 747\,d^4 - \\ &\quad 395\,d^3 + 112\,d^2 - 28\,d + 4))^3, \\ \mathrm{disc}(\tilde{F}_7) &= d^8\,(d-1)^{14}\,(4\,n^3 + (d^4 - 30\,d^3 + 3\,d^2 + 26\,d + 1)\,n^2 - \\ &\quad 2\,d\,(d-1)\,(12\,d^5 - 24\,d^4 - 91\,d^3 + 115\,d^2 - 29\,d + 12)\,n - \\ &\quad d\,(d-1)\,(4\,d^9 - 8\,d^8 - 136\,d^7 + 612\,d^6 - 916\,d^5 + 747\,d^4 - \\ &\quad 395\,d^3 + 112\,d^2 - 28\,d + 4))^3. \end{aligned}$$

6. Fall: $l = 8$

In diesem Fall ergibt sich mit der Bezeichnung $b = (2d-1)(d-1)$ (siehe Abschnitt 1.3.1)

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{d^3\, b\, y_P}{{x_P}^2}$
$P \oplus 2A$	$\frac{d^2\, b\left(-b\, y_P + {x_P}^2 + b\,(d^2-4\,d+1)\, x_P + d^3\, b^2\right)}{(d^2\, b - x_P)^2}$
$P \oplus 3A$	$\frac{d\, b\left((d-1)^2\, y_P + (x_P - d^2\,(d-1))\,(x_P - d^2\, b)\right)}{(d\, b - x_P)^2}$
$P \oplus 4A$	$\frac{d^3\,(d-1)\,(x_P - d\, b)}{(x_P + d^3\,(1-d))}$
$P \oplus 5A$	$\frac{d\, b\left(-(d-1)^2\, y_P + {x_P}^2 - (3\,d-1)\, b\, x_P + d^3\, b^2\right)}{(d\, b - x_P)^2}$
$P \oplus 6A$	$\frac{d^2\, b\left(b\, y_P + x_P\,(x_P - d^2\, b)\right)}{(d^2\, b - x_P)^2}$
$P \oplus 7A$	$\frac{d^3\, b\left(-y_P + (2\,d^2 - 4\,d+1)\, x_P + d^3\, b\right)}{{x_P}^2}$

und damit

$$
\begin{aligned}
n_8 \;=\; & \Big({x_P}^8 - d\, b\,(20\,d^4 - 24\,d^3 + 2\,d^2 + 4\,d - 1)\,{x_P}^6 + 2\,d^3\, b^2\,(8\,d^4 + 10\,d^3 - 26\,d^2 + 13\,d - 2)\,{x_P}^5 - \\
& d^4\, b^2\,(d-1)\,(8\,d^6 + 52\,d^5 - 68\,d^4 + 17\,d^3 + 12\,d^2 - 7\,d + 1)\,{x_P}^4 + 4\,d^9\, b^3\,(d-1)\,(4\,d^2 + 2\,d - 1)\,{x_P}^3 - \\
& d^9\, b^4\,(d-1)\,(4\,d-1)\,(2\,d^2 + 4\,d - 1)\,{x_P}^2 + 2\,d^{12}\, b^5\,(d-1)\,(4\,d-1)\,x_P - d^{15}\, b^6\,(d-1)\Big) / \\
& \Big({x_P}^2\,(x_P - d^2\, b)^2\,(x_P - d\, b)^2\,(x_P - d^3\,(d-1))\Big).
\end{aligned}
$$

Das entsprechende Polynom mit Galoisgruppe D_8 lautet

$$
\begin{aligned}
F_8(x) \;=\; & x^8 - n\, x^7 + \\
& d\,(d-1)\,((5\,d^2 + 2\,d - 2)\, n - (2\,d-1)\,(20\,d^4 - 24\,d^3 + 2\,d^2 + 4\,d - 1))\, x^6 - \\
& d^2\,(d-1)\, b \cdot \\
& \quad ((4d+1)\,(d^2 + 2d - 1)\, n - 2d(2d-1)\,(8d^4 + 10d^3 - 26d^2 + 13d - 2))\, x^5 +
\end{aligned}
$$

$$
\begin{aligned}
& d^4\,(d-1)\,b^2\cdot \\
& \quad ((d^3+8d^2+3d-2)\,n-8d^6-52d^5+68d^4-17d^3-12d^2+7d-1)x^4- \\
& d^6\,(d-1)\,b^3\,((2\,d^2+4\,d-1)\,n-4\,d^3\,(4\,d^2+2\,d-1))\,x^3+ \\
& d^9\,(d-1)\,b^4\,(n-(4\,d-1)\,(2\,d^2+4\,d-1))\,x^2+ \\
& d^{12}\,(d-1)\,b^5\,(4\,d-1)\,2\,x- \\
& d^{15}\,(d-1)\,b^6.
\end{aligned}
$$

Die Transformation $x \mapsto \frac{d^3\,(d-1)\,(2\,d-1)}{x}$ führt zur etwas kompakteren Polynomfamilie

$$
\begin{aligned}
\tilde{F}_8(c) \;=\; & x^8-2\,(4\,d-1)\,x^7-(n-(4\,d-1)\,(2\,d^2+4\,d-1))\,x^6+ \\
& ((2\,d^2+4\,d-1)\,n-4\,d^3\,(4\,d^2+2\,d-1))\,x^5- \\
& d\,((d^3+8d^2+3d-2)\,n-(8d^6+52d^5-68d^4+17d^3+12d^2-7d+1))\,x^4+ \\
& d^2\,((4d+1)(d^2+2d-1)\,n-2d(2d-1)(8d^4+10d^3-26d^2+13d-2))\,x^3- \\
& d^4\,((5d^2+2d-2)\,n-(2d-1)\,(20d^4-24d^3+2d^2+4d-1))\,x^2+ \\
& d^6\,n\,(2\,d-1)\,x-d^9\,(d-1)\,(2\,d-1)^2.
\end{aligned}
$$

Die beiden Diskriminanten berechnen sich zu:

$$
\begin{aligned}
\operatorname{disc}(F_8) \;=\; & d^{68}\,(2\,d-1)^{32}\,(d-1)^{68}\,(4\,n+1-32\,d^2\,(2\,d-1)\,(d-1))^3\cdot \\
& (n^2-8\,d\,(2\,d-1)\,(d-1)\,n+4\,d\,(d-1)\,(2\,d-1)^4)^4, \\
\operatorname{disc}(\tilde{F}_8) \;=\; & d^{26}\,(2\,d-1)^4\,(d-1)^{26}\,(4\,n+1-32\,d^2\,(2\,d-1)\,(d-1))^3\cdot \\
& (n^2-8\,d\,(2\,d-1)\,(d-1)\,n+4\,d\,(d-1)\,(2\,d-1)^4)^4.
\end{aligned}
$$

Restliche Fälle: $l = 9, 10, 12$

Die weiteren Fälle finden sich auf Grund der umfangreichen Formeln im Anhang (siehe B.1, B.2 und B.3).

3.1.3 Arithmetik für Zahlkörper vom Grad 4

In diesem Abschnitt werden für ganze Zahlen n und $b = \pm 1$ die Polynome

$$F_4(x) := x^4 - nx^3 + b(n-1)x^2 + 2b^2x - b^3$$

betrachtet, die in Abschnitt 3.1.2 ($l = 4$) berechnet wurden. Diese Polynome besitzen die Diskriminante

$$\operatorname{disc}(F_4) = b^6\,(4\,(n-4b)+1)\,(n^2+4\,b)^2.$$

Ein Ziel der folgenden Ausführungen ist die Berechnung parametrisierter Einheiten von Zahlkörpern, die durch $F_4(x)$ erzeugt werden. Da $F_4(x)$ und $\tilde{F}_4(x)$ aus Abschnitt 3.1.2 ($l = 4$) dieselben Zahlkörper erzeugen, könnte ebenfalls das kürzere Polynom $\tilde{F}_4(x)$ betrachtet werden. Zur späteren Bestimmung von Unterfamilien mit Galoisgruppe C_l in Abschnitt 3.2 ist die Kenntnis der Nullstellen von $F_4(x)$ notwendig; eine entsprechende Bestimmung mittels $\tilde{F}_4(x)$ würde weitere Betrachtungen erfordern. Somit werden die Untersuchungen zur Arithmetik auch für $F_4(x)$ ausgeführt.[2]

Zur Einheitenbestimmung werden im Folgenden nur die Fälle $b = \pm 1$ betrachtet. In beiden Fällen besitzt $F_4(x)$ keine rationalen Nullstellen (für $n \in \mathbb{Z}$). Eine Zerlegung von $F_4(x)$ in zwei quadratische Faktoren tritt genau dann auf, wenn $(b, n) \in \{(-1, \pm 2), (1, 0), (1, 4)\}$ gewählt wird. Diese Fälle werden im Folgenden ausgeschlossen.

Gelte also für den Rest dieses Abschnittes $n \neq \pm 2$ falls $b = -1$ bzw. $n \neq 0, 4$ falls $b = 1$ ist.

Satz 3.1.6. *Das Polynom $F_4(x)$ besitzt mit $b = 1$ die Signatur $(2, 1)$, falls $n \leq 3$, und die Signatur $(4, 0)$, falls $n > 4$ ist.*
Für $b = -1$ hat $F_4(x)$ die Signaturen $(2, 1)$, falls $n \leq -5$, $(0, 2)$ für $n \in \{-4, -3, -1, 0, 1\}$ und $(4, 0)$, falls $n \geq 3$ ist.

Beweis. Sei $b = 1$.
Im Fall $n \leq 3$ ist die Diskriminante $\operatorname{disc}(F_4)$ negativ und falls $n > 4$ positiv. Da $F_4(0) = -1$ ist, besitzt das betrachtete Polynom mindestens eine reelle Nullstelle, also sind für $n > 4$ alle Nullstellen reell.

[2] Die Transformation von $F_4(x)$ zu $\tilde{F}_4(x)$ erfolgt durch $x \mapsto \frac{b}{x}$, so dass n nicht variiert wird. Entsprechend stimmen Signatur, der quadratische Zahlkörper Ω_b und die Einheit $\varepsilon = \frac{1}{2}(-n + \sqrt{n^2 + 4\,b})$ überein. Über Ω_b zerfällt $\tilde{F}_4(x)$ in $(x^2 - x + \varepsilon)(x^2 - x + \bar{\varepsilon})$.

Sei $b = -1$. Die Diskriminante $\operatorname{disc}(F_4)$ ist negativ für $n \leq -5$ und für $n \geq -4$ positiv. Falls $n \geq 3$ ist, gilt $F_4(1) = 1 - n + (1 - n) + 2 + 1 = 5 - 2n < 0$, so dass $F_4(x)$ wiederum eine und deshalb folglich vier reelle Nullstellen besitzt. In den verbliebenen Fällen $n \in \{-4, -3, -1, -0, 1\}$ berechnet sich die Signatur leicht zu $(0, 2)$. □

Die Fälle, in denen $F_4(x)$ einen Zahlkörper vom Grad 4 mit genau einem quadratischen Teilkörper erzeugt, sind von besonderem Interesse. Auf Grund der Gestalt von $\operatorname{disc}(F_4)$ ist $n^2 + 4\,b$ eine mögliche Diskriminante (einer Ordnung) eines solchen quadratischen Zahlkörpers.

Deshalb wird für den Rest dieses Abschnittes angenommen, dass $n^2 + 4\,b$ kein Quadrat ist. (Dies ist äquivalent zu $(n, b) \neq (0, 1)$.)

Satz 3.1.7. *Das Polynom $F_4(x)$ zerfällt über dem quadratischen Zahlkörper $\Omega_b := \mathbb{Q}(\sqrt{n^2 + 4b})$ in*

$$F_4(x) = (x^2 + \varepsilon x - \varepsilon b)(x^2 + \bar{\varepsilon} x - \bar{\varepsilon} b),$$

wobei $\varepsilon = \frac{1}{2}(-n + \sqrt{n^2 + 4b}) \in \Omega_b$ eine Einheit in Ω_b mit Norm $-b$ ist. (Mit $\bar{}$ wird der nicht triviale Automorphismus des quadratischen Zahlkörpers bezeichnet.)

Beweis. Einfaches Nachrechnen liefert die Behauptung. □

Bemerkung 3.1.8. *Nagell [3] hat in [68] gezeigt, dass $n^2 + 4\,b$ für unendlich viele $n \in \mathbb{Z}$ quadratfrei ist. In diesen Fällen ist ε eine Fundamentaleinheit von Ω_b.*

Bemerkung 3.1.9. *Falls $F_4(x)$ irreduzibel mit Galoisgruppe V_4 ist, dann ist $4(n - 4b) + 1$ ein Quadrat in $\mathbb{Z}$.*

Satz 3.1.10. *Falls $4(n - 4b) + 1$ kein Quadrat in $\mathbb{Z}$ ist, dann erzeugt das Polynom $F_4(x)$ einen Zahlkörper vom Grad 4 mit Galoisgruppe D_4 oder C_4.*

Beweis. Das Polynom $F_4(x)$ ist genau dann irreduzibel über $\mathbb{Q}$, wenn

$$x^2 + \varepsilon x - \varepsilon b$$

irreduzibel in $\Omega_b[x]$ ist. Die Reduzibilität von Letzterem ist äquivalent dazu, dass $\alpha := \varepsilon^2 + 4\varepsilon b$ ein Quadrat in Ω_b ist; in diesem Fall ist $N(\alpha) = N(\varepsilon(\varepsilon + 4b)) = 4n + 1 - 16b$ ein Quadrat in $\mathbb{Q}$, was einen Widerspruch zur Voraussetzung darstellt. Mit der Bemerkung 3.1.9 folgt somit Satz 3.1.10. □

[3] Der Autor heißt richtig Trygve Nagell. In der zitierten Publikation [68] wird er jedoch als Trygve Nagel angegeben.

Bemerkung 3.1.11. *$4n+1-16b$ ist genau dann ein Quadrat in $\mathbb{Z}$, wenn $n \in \mathbb{Z}$ die Form $n = u^2+u+4b$ mit $u \in \mathbb{Z}$ besitzt.*

Zur Charakterisierung der beiden nach Satz 3.1.10 möglichen Fälle D_4 oder C_4 für die Galoisgruppe sei im Folgenden $4(n-4b)+1$ kein Quadrat in $\mathbb{Z}$.

Satz 3.1.12. *Das Polynom $F_4(x)$ erzeugt genau dann eine Galoiserweiterung über $\mathbb{Q}$ (mit Galoisgruppe C_4), wenn für $\alpha = \varepsilon^2 + 4\varepsilon b$ der Quotient $\frac{\alpha}{\bar{\alpha}}$ ein Quadrat in Ω_b ist. Dies ist äquivalent dazu, dass $4(n-4b)+1$ ein Quadrat in Ω_b ist.*

Beweis. Eine Nullstelle ρ von $F_4(x)$ erzeugt eine Erweiterung vom Grad 4 von $\mathbb{Q}$, und die Quadratwurzeln von α und von $\bar{\alpha}$ erzeugen quadratische Erweiterungen von Ω_b. Genau dann, wenn diese Erweiterungen zusammenfallen, sind sie zyklische Erweiterungen von $\mathbb{Q}$. In dem Fall gilt $\sqrt{\alpha} = \mu + \nu\sqrt{\bar{\alpha}}$ mit Elementen $\mu, \nu \in \Omega_b$. Quadrieren dieser Gleichung führt zu $\mu\nu = 0$, was $\mu = 0$ impliziert. Deshalb muss $\frac{\alpha}{\bar{\alpha}}$ ein Quadrat in Ω_b sein. Darüber hinaus gilt

$$\frac{\alpha}{\bar{\alpha}} = \frac{N(\alpha)}{(\bar{\alpha})^2}$$

und $N(\alpha) = 4n+1-16b$, so dass die Behauptung folgt. □

Bemerkung 3.1.13. *Die Aussage, dass $4(n-4b)+1$ ein Quadrat in Ω_b ist, ist äquivalent zu der Aussage, dass $v^2(1+4n-16b) = n^2+4b$ mit $n, v \in \mathbb{Q}$ gilt.*

Satz 3.1.14. *Das Polynom $F_4(x)$ erzeugt eine Galoiserweiterung über $\mathbb{Q}$ mit Galoisgruppe C_4 nur für $(b,n) \in \{(1,8),(-1,-3),(-1,7)\}$.* [4]

Beweis. Wir betrachten zuerst den Fall $b = 1$. Das bedeutet nach der Bemerkung 3.1.13, dass Lösungen von $v^2(4n-15) = n^2+4$ gesucht sind, woraus unmittelbar $n_{1/2} = 2v^2 \pm \sqrt{4v^4-15v^2-4}$ folgt. Dabei liegt $n \in \mathbb{Q}$, falls $4v^4-15v^2-4$ ein Quadrat in $\mathbb{Q}$ ist, anders ausgedrückt, falls die elliptische Kurve E_1 mit Gleichung $y^2 = 4v^4-15v^2-4$ mindestens einen rationalen Punkt $(v,y) \in \mathbb{Q}^2$ besitzt.

Die Weierstraßform von E_1 lautet

$$z^2 = t^3 - 11t - 890 = (t-10)\,(t^2+10\,t+89).$$

Berechnungen mit dem Computeralgebra-Paket MAGMA [52] zeigen, dass $E_1(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} = \{\mathcal{O}, P, 2P, 3P\}$ ist, wobei

[4] Beachte, dass in diesem Abschnitt nur $b = \pm 1$ betrachtet wird.

	t	z	v	y
$\mathcal{O}$	∞	∞	2	0
P	27	136	∞	∞
$2P$	10	0	-2	0
$3P$	27	-136	∞	∞

gilt. Dies bedeutet, dass mit $b = 1$ die Galoisgruppe C_4 nur im Fall $n = 8$ mit dem korrespondierenden Polynom $x^4 - 8x^3 + 7x^2 + 2x - 1$ auftritt.

Im zweiten Fall $b = -1$ führen dieselben Betrachtungen dazu, dass $n_{1/2} = 2v^2 \pm \sqrt{4v^4 + 17v^2 + 4}$ eine rationale Zahl sein muss, was die Existenz von rationalen Punkten auf der elliptischen Kurve E_{-1} mit Weierstraßgleichung

$$z^2 = t^3 - 12987t - 263466 = (t + 21)\,(t + 102)\,(t - 123).$$

impliziert. Analoge Rechnungen zeigen, dass die Mordell-Weil-Gruppe $E_{-1}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \{\mathcal{O}, P\} \times \{\mathcal{O}, R, 2R, 3R\}$ ist, wobei

	t	z	v	y
$\mathcal{O}$	∞	∞	0	-2
P	-21	0	∞	∞
R	-57	-540	-1	5
$2R$	123	0	∞	∞
$3R$	-57	540	1	5
$P \oplus R$	303	-4860	-1	-5
$P \oplus 2R$	-102	0	0	2
$P \oplus 3R$	303	4860	1	-5

gilt. Somit tritt im Fall $b = -1$ die Galoisgruppe C_4 nur für $n = -3, 7$ auf, was den Polynomen $x^4 + 3x^3 + 4x^2 + 2x + 1$ und $x^4 - 7x^3 - 6x^2 + 2x + 1$ entspricht. □

Sei im Folgenden K_b der durch eine Nullstelle ρ von $F_4(x)$ erzeugte Zahlkörper über $\mathbb{Q}$ vom Grad 4, der die Galoisgruppe D_4 besitzt. Vorhergehende Konstruktion führt unmittelbar zu zwei unabhängingen Einheiten von K_b, nämlich ρ und ε aus Ω_b. Es werden außerdem nur Zahlkörper der Signatur $(2, 1)$ betrachtet.[5] In diesen Fällen bilden diese beiden Einheiten eine maximal unabhängige Menge von Einheiten von K_b.

[5] Für die Zahlkörper mit Signatur $(4, 0)$ war es leider nicht möglich, eine dritte unabhängige Einheit in parametrisierter Form anzugeben.

Der Rest dieses Abschnitts dient dazu zu beweisen, dass ρ und ε ein System von Fundamentaleinheiten der Ordnung $\mathbb{Z}[\rho]$ bilden. Falls n^2+4b und $4(n-4b)+1$ quadratfrei und koprim sind, so bilden die beiden Einheiten sogar ein System von Fundamentaleinheiten für den Zahlkörper $\mathbb{Q}(\rho)$.

Bemerkung 3.1.15. *Da* $16(n^2+4b) = (4n+(16\,b-1))(4n-(16\,b-1))+(16\,b+1)^2$ *ist, folgt sofort, dass ein gemeinsamer Faktor von* n^2+4b *und* $4(n-4b)+1$ *notwendigerweise auch* $(16b+1)^2$ *teilt.*

Zum Beweis der Fundamentalität wird eine untere Regulatorschranke von Nakamula [70] genutzt. Proposition 3 seines Artikels besagt, dass der Quotient der Regulatoren von K_b und Ω_b nach unten beschränkt ist durch

$$L \;:=\; \frac{1}{2}\log\left(\sqrt[3]{\left|4(n-4b)+1\right|\frac{(n^2+4b)^2}{4}+\left(\frac{317}{27}\right)^3}-\frac{290}{27}\right)\;.$$

Es wird nun eine untere Abschätzung von L gesucht. Dabei wird mit dem Radikand der Kubikwurzel begonnen. Für $n \leq -10$ ist dieser von der Form

$$|n|^5(1+\lambda),$$

wobei $\lambda \in \mathbb{R}$ mit

$$\lambda > \begin{cases} \frac{15}{4|n|}+\frac{8}{n^2}+0,048 & \text{für} \quad b=1 \\ -\frac{17}{4|n|}-\frac{8}{n^2}+0,051 & \text{für} \quad b=-1 \end{cases}$$

gilt. Damit folgt

$$L \;>\frac{1}{2}\log\left(|n|^{(5/3)}\left(1+\frac{\lambda}{3}-\frac{\lambda^2}{6}\right)-\frac{290}{27}\right),$$

was zu

$$L \;>\; \frac{2}{3}\log|n|$$

führt.

Im nächsten Schritt wird eine obere Abschätzung für den Regulator R_{K_b} der unabhängigen Einheiten ρ und ε berechnet. Dazu werden die ersten beiden Konjugierten $\rho^{(1)}$ und $\rho^{(2)}$ von ρ genutzt. Man erhält

$$\begin{aligned} R_{K_b} &= \left|\det\begin{pmatrix}\log|\rho^{(1)}| & \log|\rho^{(2)}| \\ \log|\varepsilon| & \log|\varepsilon|\end{pmatrix}\right| \\ &= \left|\log|\varepsilon|\right|\left|\log\frac{|\rho^{(1)}|}{|\rho^{(2)}|}\right|\;. \end{aligned}$$

Zuerst wird der Quotienten $|\frac{\rho^{(1)}}{\rho^{(2)}}|$ abgeschätzt: Es ergibt sich

$$\frac{\rho^{(1)}}{\rho^{(2)}} \;=\; \frac{-\varepsilon+\sqrt{\varepsilon^2+4b\varepsilon}}{-\varepsilon-\sqrt{\varepsilon^2+4b\varepsilon}}\,,$$

und man berechnet leicht

$$\mu := \varepsilon^2+4b\varepsilon \;=\; \frac{n^2-4bn+2b-(n-4b)\sqrt{n^2+4b}}{2}.$$

Als Ergebnis folgt die Abschätzung

$$L_\varepsilon < \varepsilon < U_\varepsilon,$$

wobei

$$L_\varepsilon := |n| + \frac{b}{|n|} - \frac{2}{n^3}, \quad U_\varepsilon := |n| + \frac{b}{|n|}$$

gilt, und

$$L_\mu < \sqrt{\mu} < U_\mu$$

mit

$$L_\mu := |n| + 2b + \frac{b-4}{|n|} - \frac{2}{n^2} - \frac{8b+2}{|n|^3} - \frac{4b}{n^4}$$

und

$$U_\mu := |n| + 2b + \frac{b}{|n|} + \frac{2}{n^2}$$

ist. Betrachtet man nun die Fälle $b = \pm 1$ separat, so ergibt sich

$$\left|\frac{\rho^{(1)}}{\rho^{(2)}}\right| \;<\; C = \frac{|n|+1,11}{0,779}$$

für $|n| \geq 10$.

Falls nun die Einheitengruppe $U := \langle -1, \rho, \varepsilon\rangle$ eine echte Untergruppe der vollen Einheitengruppe $U_{\mathbb{Z}[\rho]}$ von $\mathbb{Z}[\rho]$ ist, dann ist der Quotient aus dem Regulator von K_b und dem Regulator von Ω_b kleiner als $\frac{\log C}{2}$. Zeigt man, dass $\frac{\log C}{2} < L$ gilt, so beweist dies, dass ρ und ε ein System von Fundamentaleinheiten für $\mathbb{Z}[\rho]$ bilden. Es ist einfach nachzuvollziehen, dass

$$\frac{1}{2}\log\frac{|n|+1,11}{0,779} \;<\; \frac{2}{3}\log|n|$$

äquivalent zu

$$\frac{|n|+1,11}{0,779|n|^{4/3}} \;<\; 1$$

ist; die zweite Ungleichung ist für alle $n < -5$ erfüllt.

Somit wurde der folgende Satz bewiesen:

Satz 3.1.16. *Falls der Zahlkörper $K_b = \mathbb{Q}(\rho)$ die Galoisgruppe D_4 besitzt, so sind ρ und ε Fundamentaleinheiten der Ordnung $\mathbb{Z}[\rho]$. Sie sind darüber hinaus Fundamentaleinheiten von K_b, wenn $4(n-4b)+1$ und n^2+4b quadratfrei und koprim sind.*

Die obigen Abschätzungen beweisen den Satz für alle Fälle $n \leq -10$. Für größere Werte von n wurde der Satz durch direktes Berechnen der Einheitengruppe von K_b mit dem Computeralgebrasystem KANT [32] gezeigt.

3.1.4 Arithmetik für Zahlkörper vom Grad 5

Analog zum Abschnitt 3.1.3 werden nun für ganzzahlige n und $b = \pm 1$ die Polynome

$$F_5(x) = x^5 - n\,x^4 + b\,(2\,n + b^2 - b - 1)\,x^3 - b^2\,(n + b - 3)\,x^2 + b^3\,(b-3)\,x + b^4$$

im Hinblick auf Einheiten untersucht.[6] Für $b = 1$ erhält man die Polynome

$$x^5 - n\,x^4 + (2\,n - 1)\,x^3 - (n-2)\,x^2 - 2\,x + 1,$$

die sich durch die Transformation $x \mapsto x + 1$ und $n \mapsto n + 5$ in die entsprechenden Polynome mit $b = -1$

$$x^5 - n\,x^4 - (2\,n + 1)\,x^3 - (n-4)\,x^2 + 4\,x + 1$$

überführen lassen.

Somit sei im Folgenden $b = 1$.

Die zugehörigen Polynome besitzen die schon in Abschnitt 3.1.2 ($l = 5$) berechnete Diskriminante $(d(n))^2$ mit

$$d(n) := 4\,n^3 - 28\,n^2 + 24\,n - 47.$$

Für jede ganzzahlige Wahl von n bleiben die $F_5(x)$ irreduzibel, wie eine einfache Rechnung modulo 2 zeigt.

Satz 3.1.17. *Das Polynom $F_5(x)$ besitzt (mit $b = 1$) die Signatur $(1, 2)$, falls $n \leq 6$, und die Signatur $(5, 0)$, falls $n \geq 7$ ist.*

[6] Aus demselben Grund wie bei Grad 4 wird auch hier $F_5(x)$ und nicht $\tilde{F}_5(x)$ untersucht: Die später notwendige Kenntnis der Nullstellen des Polynoms ist nur für $F_5(x)$ gegeben, so dass aus Einheitlichkeitsgründen hier ebenfalls $F_5(x)$ betrachtet wird.

Beweis. Die Diskriminante ist für $b = 1$ immer positiv, so dass $F_5(x)$ genau eine oder genau fünf reelle Nullstellen besitzt.

Es ist $F_5(-1) = -4\,n + 5 < 0$ für $n \geq 2$ und $F_5(0) = F_5(1) = 1 > 0$. Außerdem ist $F_5(\frac{1}{2}) = \frac{-2\,n+13}{32} < 0$ für $n \geq 7$, so dass also für $n \geq 7$ drei reelle Nullstellen existieren, was die Signatur $(5, 0)$ liefert.
Ist $n < 7$, so lässt sich mit Hilfe eines Satzes von Sturm (in algorithmischer Form z. B. in H. Cohen [6], 4.1.10+4.1.11) die Signatur zu $(2, 1)$ berechnen: Sei l_0 der führende Koeffizient von $A_0 = F_5$ (also $l_0 = 1$), l_1 der führende Koeffizient der Ableitung $A_1 = F_5'$ (also $l_1 = 5$) und $l_i(n)$ für $2 \leq i \leq 5$ die führenden Koeffizienten der Restglieder $A_i(x)$ nach sukzessiver Polynomdivision von $A_{i-2}(x)$ durch $A_{i-1}(x)$ in der Form $A_{i-2}(x) = A_{i-1}(x)Q_i(x) - A_i(x)$. Bei der konkreten Berechnung erhält man (bis auf positive konstante Faktoren und quadratische Nenner)

$$l_2(n) = 2\,n^2 - 10\,n + 5, \quad l_3(n) = n^4 - 4\,n^3 - 14\,n^2 + 6\,n - 22,$$

$$l_4(n) = (2\,n^2 + 6\,n + 3)\,(4\,n^3 - 28\,n^2 + 24\,n - 47)\,(2\,n^2 - 10\,n + 5)^2$$

und

$$l_5(n) = (n^4 - 4\,n^3 - 14\,n^2 + 6\,n - 22)^2.$$

Ist nun $\omega(n)$ die Anzahl der Vorzeichenwechsel in der von n abhängigen Sequenz $-l_0, l_1, -l_2(n), l_3(n), -l_4(n), l_5(n)$ und $\nu(n)$ die Anzahl der Vorzeichenwechsel in $l_0, l_1, l_2(n), l_3(n), l_4(n), l_5(n)$, so ist $\omega(n) - \nu(n)$ die Anzahl der reellen Nullstellen von $F_5(x)$. Für jedes $n < 7$ erhält man $\omega(n) = 3$ und $\nu(n) = 2$ (auch wenn sich die einzelnen Sequenzen unterscheiden), so dass die Behauptung folgt. □

Die Galoisgruppe von $F_5(x)$ ist, wie in Satz 3.1.5 ausgeführt, im Allgemeinen die Diedergruppe mit 10 Elementen. Auf die Frage, wann C_l als Untergruppe der Galoisgruppe auftritt, wird in Abschnitt 3.2 detailliert eingegangen. Im Vorgriff darauf wird zur Abrundung dieses Abschnitts folgendes erwähnt:

Lemma 3.1.18. *Für $b = 1$ besitzt $F_5(x)$ nur in den zwei Fällen $n \in \{7, 18\}$ die Galoisgruppe C_l, wobei beide Polynome dieselbe Körpererweiterung erzeugen.*

Beweis. In Lemma 3.2.1 und in der zweiten Tabelle von Abschnitt 3.2.2 wird gezeigt, dass die Galoisgruppe von $F_5(x)$ genau dann zyklisch ist, wenn die elliptische Kurve $z^2 = 4\,n^3 - 28\,n^2 + 24\,n - 47$ rationale Punkte besitzt. Mit

dem Computeralgebra-Paket MAGMA [52] berechnet sich leicht die Mordell-Weil-Gruppe zu $\mathbb{Z}/5\mathbb{Z}$, wobei nur $n \in \{7, 18\}$ auftritt. Somit besitzen nur die beiden Polynome

$$F_5^{n=7}(x) = x^5 - 7\,x^4 + 13\,x^3 - 5\,x^2 - 2\,x + 1,$$

und

$$F_5^{n=18}(x) = x^5 - 18\,x^4 + 35\,x^3 - 16\,x^2 - 2\,x + 1$$

die C_5 als Galoisgruppe. Darüber hinaus lässt sich z. B. mit KANT [32] einfach kontrollieren, dass für eine Nullstelle ρ des Polynoms $F_5^{n=7}(x)$ die algebraische Zahl $2\rho^3 - 9\rho^2 + 2\rho + 1$ Nullstelle von $F_5^{n=18}(x)$ ist. □

Die von $F_5(x)$ erzeugten Zahlkörper besitzen laut Satz 3.1.17 genau zwei Grundeinheiten, falls $n \leq 6$ gilt. Ist ρ eine Nullstelle von $F_5(x)$, so ist diese eine Einheit in dem erzeugten Zahlkörper, da der konstante Term des Polynoms 1 ist. Auf Grund der Form $F_5(x) = x(x-1)(x^3-(n-1)\,x^2+n\,x+2)+1$ kann unmittelbar $\rho - 1$ als zweite Einheit angegeben werden.[7] Es gilt sogar:

Satz 3.1.19. *Die beiden Elemente $\rho, \rho - 1$ bilden ein System unabhängiger Einheiten der Gleichungsordnung $\mathbb{Z}[\rho]$. Darüber hinaus sind sie Fundamentaleinheiten in $\mathbb{Z}[\rho]$ für $n < 6$.*

Der Beweis dieses Satzes erfordert eine Abschätzung der Beträge der betrachteten Elemente ρ und $\rho - 1$ und deren Konjugierter. Da ρ eine Nullstelle von $F_5(x)$ ist, sind die Konjugierten von ρ die weiteren Nullstellen des Polynoms.

Lemma 3.1.20. *Sei $n \geq 7$. Seien $\rho^{(1)}, \rho^{(2)}, \rho^{(3)}, \rho^{(4)}$ und $\rho^{(5)}$ die reellen Nullstellen von $F_5(x)$ (mit $b = 1$). Dann gelten folgende Abschätzungen:*

$$-1 < -\frac{1}{\sqrt{n}} - \frac{1}{n} < \rho^{(1)} < -\frac{1}{\sqrt{n}} < 0 < \frac{1}{\sqrt{n}} < \rho^{(2)} < \frac{1}{\sqrt{n}} + \frac{1}{n} < \frac{3}{5},$$

$$\frac{3}{5} < 1 - \frac{1}{\sqrt{n}} < \rho^{(3)} < 1 - \frac{1}{\sqrt{n}} + \frac{1}{n} < 1 < 1 + \frac{1}{\sqrt{n}} + \frac{1}{n} < \rho^{(4)} < 1 + \frac{1}{\sqrt{n}} + \frac{5}{n} < 3$$

und

$$3 < n - 3 < \rho^{(5)} < n - 2.$$

[7] In den anderen Fällen $n \geq 7$ konnten keine weiteren parametrisierten unabhängigen Einheiten gefunden werden.

Beweis. Dies überprüft man leicht anhand der Vorzeichenwechsel von $F_5(x)$ an den entsprechenden Stellen. Für $n \geq 7$ gelten die Ungleichungen:

$$F_5(-\tfrac{1}{\sqrt{n}} - \tfrac{1}{n}) = \tfrac{-2\,n^{4,5}-4\,n^4-5\,n^{3,5}-3\,n^3-2\,n^{2,5}-5\,n^2-10\,n^{1,5}-10\,n-5\,\sqrt{n}-1}{n^5} < 0,$$
$$F_5(-\tfrac{1}{\sqrt{n}}) = \tfrac{n^{1,5}+n-1}{n^{2,5}} > 0,$$
$$F_5(\tfrac{1}{\sqrt{n}}) = \tfrac{n^{1,5}-n+1}{n^{2,5}} > 0,$$
$$F_5(\tfrac{1}{\sqrt{n}} + \tfrac{1}{n}) = \tfrac{-2\,n^{4,5}+4\,n^4+5\,n^{3,5}-5\,n^3-6\,n^{2,5}+3\,n^2+10\,n^{1,5}+10\,n+5\,\sqrt{n}+1}{n^5} < 0,$$
$$F_5(1 - \tfrac{1}{\sqrt{n}}) = \tfrac{-2\,n^2+8\,n^{1,5}-9\,n+5\,\sqrt{n}-1}{n^{2,5}} < 0,$$
$$F_5(1 - \tfrac{1}{\sqrt{n}} + \tfrac{1}{n}) = \tfrac{5\,n^4-17\,n^{3,5}+33\,n^3-44\,n^{2,5}+43\,n^2-30\,n^{1,5}+15\,n-5\,\sqrt{n}+1}{n^5} > 0,$$
$$F_5(1 + \tfrac{1}{\sqrt{n}} + \tfrac{1}{n}) = \tfrac{5\,n^4+17\,n^{3,5}+33\,n^3+44\,n^{2,5}+43\,n^2+30\,n^{1,5}+15\,n+5\,\sqrt{n}+1}{n^5} > 0,$$
$$F_5(1 + \tfrac{1}{\sqrt{n}} + \tfrac{5}{n}) =$$
$$\tfrac{-8\,n^{4,5}-27\,n^4-71\,n^{3,5}-35\,n^3+276\,n^{2,5}+1275\,n^2+2750\,n^{1,5}+4375\,n+3125\,\sqrt{n}+3125)}{n^5} < 0,$$
$$F_5(n-3) = -n^4 + 16\,n^3 - 91\,n^2 + 220\,n - 191 < 0,$$
$$F_5(n-2) = 2\,n^3 - 12\,n^2 + 22\,n - 11 > 0.$$

□

Für $n \leq 6$ müssen Abschätzungen für die Beträge der komplexen Nullstellen gefunden werden. Dabei ist der folgende Satz von Obreschkoff [71] hilfreich:

Satz 3.1.21 (Obreschkoff, Seite 9). *Gegeben seien ein Polynom $f(x)$ vom Grade m und eine beliebige komplexe Zahl α, für die $f(\alpha) \neq 0$ und $f'(\alpha) \neq 0$ ist. Dann gibt es innerhalb und außerhalb jedes Kreises C, der durch die Punkte α und $\alpha - \frac{mf(\alpha)}{f'(\alpha)}$ geht, mindestens je eine Wurzel von $f(x) = 0$, es sei denn, alle Wurzeln von $f(x) = 0$ liegen gerade auf C.*

Mit Hilfe dieses Satzes wird das folgende Ergebnis gezeigt.

Lemma 3.1.22. *Sei $\rho^{(1)}$ die reelle und seien $\rho^{(2)} = \overline{\rho^{(3)}}, \rho^{(4)} = \overline{\rho^{(5)}}$ die Paare konjugiert komplexer Nullstellen von $F_5(x)$ (mit $b = 1$). Dann gelten folgende Abschätzungen:*

$$-n + 2 + \frac{2}{n} < |\rho^{(1)}| < -n + 2 + \frac{1}{n} \quad \textit{für} \quad n < -4$$

$$-n + 3 + \frac{2}{n} < |\rho^{(1)} - 1| < -n + 3 + \frac{1}{n} \quad \textit{für} \quad n < -4$$

$$\frac{1}{2\sqrt{-n}} < |\rho^{(2)}| < \frac{2}{\sqrt{-n}} \quad \textit{für} \quad n < -4$$

$$\sqrt{1-\frac{3}{4\,n}} < |\rho^{(2)}-1| < \sqrt{1-\frac{6}{5\,n}} \quad \textit{für} \quad n<-144$$
$$\sqrt{1+\frac{3}{n}} < |\rho^{(4)}| < \sqrt{1-\frac{1}{n^2}} \quad \textit{für} \quad n<-174$$
$$\sqrt{-\frac{5}{6\,n}} < |\rho^{(4)}-1| < \sqrt{-\frac{14}{13\,n}} \quad \textit{für} \quad n<-139$$

Beweis. Die folgenden Überlegungen gelten für $n<-4$. Da n negativ ist, gestalten sich die Ausführungen übersichtlicher, wenn die Notation modifiziert wird: n wird durch $-n$ substituiert. Untersucht wird das aus $F_5(x)$ entstehende Polynom

$$f(x)=x^5+n\,x^4-(2\,n+1)\,x^3+(n+2)\,x^2-2\,x+1$$

und dessen Nullstellen $\varrho^{(1)},\ldots,\varrho^{(5)}$.

Die Lage der reellen Nullstelle ist einfach durch Vorzeichenwechsel zu bestimmen. Die Bestimmung der Lage der komplexen Nullstellen ist aufwändiger: Mit Hilfe von Satz 3.1.21 wird um eine Nullstelle eines Paares konjugiert komplexer Nullstellen ein Kreis gelegt. Um den Kreis wird ein Quadrat konstruiert, dessen Ecken eine Abschätzung des Betrages der Nullstelle liefern. Diese Konstruktion hat zum Teil umfangreiche Ausdrücke zur Folge, die hier meist verkürzt wiedergegeben werden. Im Anhang sind die exakten Formeln zu finden.

Reelle Nullstelle $\rho^{(1)}$ von $F_5(x)$

Für die reelle Nullstelle $\varrho^{(1)}$ von $f(x)$ gilt

$$-n-2+\frac{1}{n}<\varrho^{(1)}<-n-2+\frac{2}{n},$$

da für $n>4$ die Ungleichungen

$$f(-n-2+\frac{1}{n})=\frac{-n^8-2\,n^7+17\,n^6+43\,n^5-16\,n^4-42\,n^3+35\,n^2-10\,n+1}{n^5}<0$$

und

$$f(-n-2+\frac{2}{n})=\frac{8\,n^7+48\,n^6+37\,n^5-156\,n^4-48\,n^3+248\,n^2-160\,n+32}{n^5}>0$$

gelten. Die Abschätzungen für $|\rho^{(1)}|$ folgen unmittelbar.

1. Paar konjugiert komplexer Nullstellen $\rho^{(2)} = \overline{\rho^{(3)}}$ von $F_5(x)$

Um die Nullstellen $\varrho^{(2)} = \overline{\varrho^{(3)}}$ von $f(x)$ mit Hilfe von Satz 3.1.21 abzuschätzen, wird für $n > 4$ die komplexe Zahl $\alpha = \frac{1}{2n^2} + \frac{i}{\sqrt{n}}$ gewählt. Für die betrachteten n gilt $0 < \Re(\alpha), \Im(\alpha) < 1$. Weiter gilt $f(\alpha) \neq 0$ und ebenfalls $f'(\alpha) \neq 0$. Der Realteil von $\frac{5f(\alpha)}{f'(\alpha)}$ berechnet sich zu[8]

$$\frac{5(96\,n^{16}-16\,n^{15}+48\,n^{14}-240\,n^{13}+78\,n^{12}+27\,n^{11}-16\,n^{10}+78\,n^9+\ldots)}{4n^2\,(16\,n^{17}+64\,n^{16}+32\,n^{15}+48\,n^{14}+16\,n^{13}+76\,n^{12}+112\,n^{11}-13\,n^{10}+149\,n^9+\ldots)}$$

und der Imaginärteil zu

$$\frac{5(16\,n^{16}+32\,n^{15}+20\,n^{14}+48\,n^{13}-8\,n^{12}+104\,n^{11}-29\,n^{10}+38\,n^9+\ldots)}{2\,\sqrt{n}\,(16\,n^{17}+64\,n^{16}+32\,n^{15}+48\,n^{14}+16\,n^{13}+76\,n^{12}+112\,n^{11}-13\,n^{10}+149\,n^9+\ldots)}.$$

Für alle betrachteten $n > 4$ ist $0 < \Im(\alpha - \frac{5f(\alpha)}{f'(\alpha)}) < 1$. Für $4 < n \leq 10$ liegt die komplexe Zahl $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ im 2. Quadranten mit $-1 < \Re(\alpha - \frac{5f(\alpha)}{f'(\alpha)}) < 0$. Für $n > 10$ gilt $0 < \Re(\alpha - \frac{5f(\alpha)}{f'(\alpha)}) < 1$.

Sei C für $n > 4$ der Kreis durch α und $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ mit exaktem Durchmesser $\frac{5f(\alpha)}{f'(\alpha)}$. Aufgrund der Lage von α und $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ kann die reelle Nullstelle $\varrho^{(1)}$ nicht im Innern und nicht auf dem Rand dieses Kreises liegen, da sie bei $-n-2$ liegt. Somit gibt es nach Satz 3.1.21 (mindestens) eine Nullstelle $\varrho^{(2)}$ von $f(x)$ im Kreisinnern. Um den Abstand von $\varrho^{(2)}$ zum Ursprung abzuschätzen, wird nun ein Quadrat um den Kreis C gelegt.

Vom Kreismittelpunkt $\alpha - \frac{5f(\alpha)}{2f'(\alpha)}$ ausgehend werden die Ecken des Quadrates konstruiert. Da für das Quadrat des Kreisdurchmessers die Ungleichung

$$\left|\frac{5f(\alpha)}{f'(\alpha)}\right|^2 = \frac{25(16\,n^{18}+72\,n^{16}-16\,n^{15}+57\,n^{14}-44\,n^{13}+24\,n^{12}+10\,n^{11}+\ldots)}{4\,n^4(16\,n^{17}+64\,n^{16}+32\,n^{15}+48\,n^{14}+16\,n^{13}+76\,n^{12}+112\,n^{11}+\ldots)} < \frac{25}{4n(n+1)^2}$$

für alle $n > 2$ gilt, ist der Kreisradius kleiner $\frac{5}{4\sqrt{n}(n+1)}$. Die Ecken des Quadrates berechnen sich somit durch

$$\alpha - \frac{5f(\alpha)}{2f'(\alpha)} \pm \frac{5}{4\sqrt{n}(n+1)} \pm \frac{5i}{4\sqrt{n}(n+1)}$$

zu

$$E_1 = \frac{-5\,n^{19}+2\,n^{18,5}-20\,n^{18}-5\,n^{17,5}-10\,n^{17}+\ldots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+2\,n^{15}+3\,n^{14}\ldots)} + \frac{4\,n^{18}+20\,n^{17}+29\,n^{16}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}\ldots)}\;i,$$

[8] Die exakten Ausdrücke finden sich im Anhang (siehe C.1).

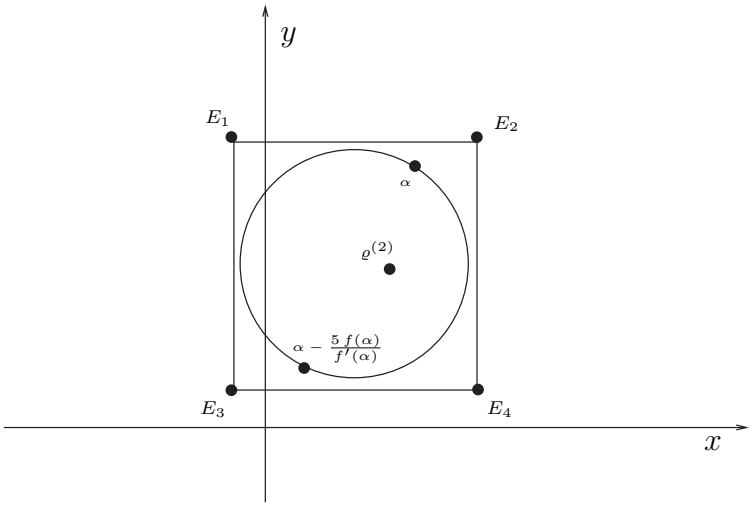

Abbildung 3.1: Approximation von $\varrho^{(2)}$

$$E_2 = \frac{5\,n^{19}+2\,n^{18,5}+20\,n^{18}-5\,n^{17,5}+10\,n^{17}+\ldots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+2\,n^{15}+3\,n^{14}\ldots)} + \frac{4\,n^{18}+20\,n^{17}+29\,n^{16}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}+\ldots)}\;i,$$

$$E_3 = \frac{-5\,n^{19}+2\,n^{18,5}-20\,n^{18}-5\,n^{17,5}-10\,n^{17}+\ldots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+2\,n^{15}+3\,n^{14}+\ldots)} + \frac{4\,n^{18}+10\,n^{17}-11\,n^{16}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}+\ldots)}\;i,$$

$$E_4 = \frac{5\,n^{19}+2\,n^{18,5}+20\,n^{18}-5\,n^{17,5}+10\,n^{17}+\ldots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+2\,n^{15}+3\,n^{14}+\ldots)} + \frac{4\,n^{18}+10\,n^{17}-11\,n^{16}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}+\ldots)}\;i.$$

Man stellt fest, dass die Ecken E_1 und E_3 für alle betrachteten $n > 4$ im 2. Quadranten liegen. [9] Außerdem sieht man anhand der Vorzeichen der Koeffizienten, dass der Abstand von E_1 zum Ursprung kleiner als der Abstand von E_2 zum Ursprung ist, so dass sich zusammen folgende Abschätzung für $|\varrho^{(2)}|$ ergibt:

$$|\Im(E_3)| < \left|\varrho^{(2)}\right| < |E_2|\,.$$

Mit der für $n > 4$ geltenden Ungleichung

$$\Im(E_3) = \frac{4\,n^{18}+10\,n^{17}-11\,n^{16}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}+\ldots)} > \frac{1}{2\sqrt{n}}$$

und mit der Abschätzung für alle $n > 4$

$$|E_2| = \left(\left(\frac{5\,n^{19}+2\,n^{18,5}+\ldots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+\ldots)}\right)^2 + \left(\frac{4\,n^{18}+20\,n^{17}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}+\ldots)}\right)^2\right)^{(1/2)} < \frac{2}{\sqrt{n}}$$

folgt die Behauptung für $|\rho^{(2)}|$.

[9] Auch bessere Abschätzungen des Kreisradius und damit eine bessere Quadratkonstruktion führen dazu, dass E_1 und E_3 im zweiten Quadranten liegen.

Zur Abschätzung von $\left|\varrho^{(2)}-1\right|$ muss beachtet werden, dass sich die Verschiebung um -1 nur im Realteil auswirkt, so dass die Abschätzung in diesem Schritt mehr Aufwand als bei den reellen Nullstellen bedeutet.

Da die Ecken des Quadrates $E_1,\dots E_4$ alle nahe[10] beim Ursprung liegen, ergibt sich durch Verschiebung von $\varrho^{(2)}$ um -1 die Situation wie in Abbildung 3.2 dargestellt.

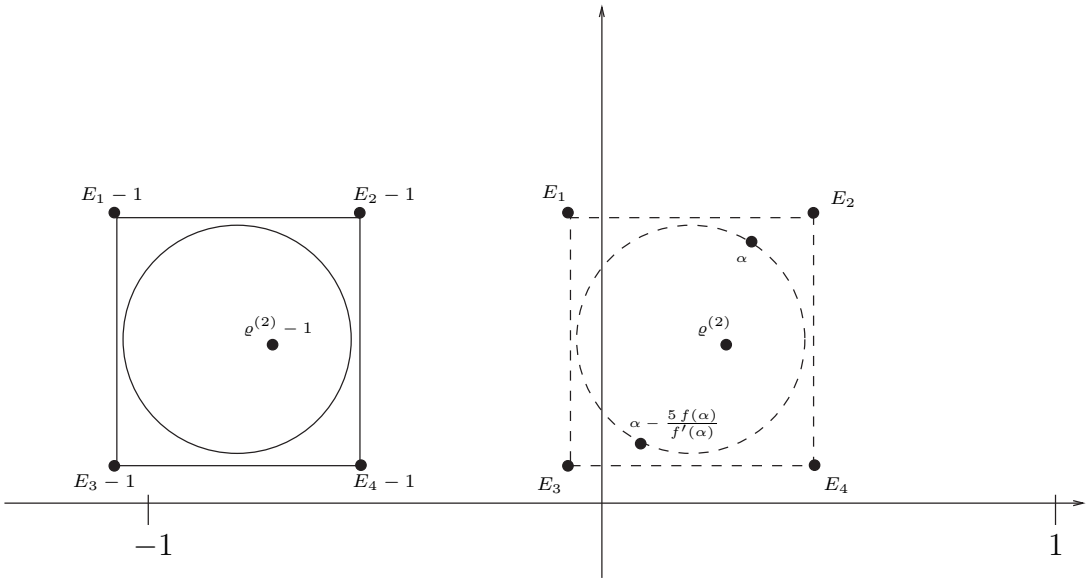

Abbildung 3.2: Approximation von $\varrho^{(2)}-1$

Nun liegen alle vier neuen Ecken $E_1-1,\dots E_4-1$ im 2. Quadranten und es folgt die Abschätzung

$$|E_1-1|>\left|\varrho^{(2)}-1\right|>|E_4-1|\,.$$

Die konkrete Berechnung liefert die Ungleichungen

$$|E_1-1|=\left(\left(\tfrac{-5\,n^{19}+2\,n^{18,5}+\dots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+\dots)}-1\right)^2+\left(\tfrac{4\,n^{18}+20\,n^{17}+\dots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}\dots)}\right)^2\right)^{(1/2)}<\sqrt{1+\tfrac{6}{5n}}$$

[10] Das heißt, dass für $n>4$ gilt: $0<\Re(E_i)<1$ für $i=2,4$ und $-1<\Re(E_j)<0$ für $j=1,3$ und $0<\Im(E_i)<1$ für $i=1,2,3,4$.

für $n > 144$ und

$$|E_4-1| = \left(\left(\frac{5\,n^{19}+2\,n^{18,5}+\ldots}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+\ldots)} - 1 \right)^2 + \left(\frac{4\,n^{18}+10\,n^{17}+\ldots}{4\,\sqrt{n}\,(n+1)(n^{17}+4\,n^{16}+\ldots)} \right)^2 \right)^{(1/2)} > \sqrt{1+\frac{3}{4n}}$$

für $n > 141$, so dass damit die Behauptung für $\rho^{(2)} - 1$ folgt.

2. Paar konjugiert komplexer Nullstellen $\rho^{(4)} = \overline{\rho^{(5)}}$ von $F_5(x)$

Die Abschätzung der verbleibenden Nullstellen $\varrho^{(4)} = \overline{\varrho^{(5)}}$ von $f(x)$ erfolgt analog zur vorangegangenen Abschätzung. In diesem Fall wird $\alpha = 1 - \frac{1}{n} + \frac{3}{n^2} + \frac{i}{\sqrt{n}}$ gewählt und wiederum gilt $f(\alpha) \neq 0 \neq f'(\alpha)$. Der Realteil von $\frac{5f(\alpha)}{f'(\alpha)}$ lautet[11]

$$\frac{-5\,(2\,n^{17}-99\,n^{16}+269\,n^{15}-1653\,n^{14}+4000\,n^{13}-14112\,n^{12}+27794\,n^{11}-68041\,n^{10}+120950\,n^9+\ldots)}{n^2\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^9+\ldots)}$$

und der Imaginärteil

$$\frac{5\,(10\,n^{16}+12\,n^{15}+89\,n^{14}-50\,n^{13}+1092\,n^{12}-1186\,n^{11}+4850\,n^{10}-5108\,n^9+\ldots)}{\sqrt{n}(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^9+\ldots)}.$$

Der Realteil von $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ ist für alle $n > 4$ größer 0, während der Imaginärteil dieser Zahl erst ab $n > 6$ positiv ist, so dass ab $n > 6$ sowohl α als auch $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ im 1. Quadranten liegen. Wie zuvor auch sind beide Real- und Imaginärteile kleiner 1.

Wieder der Kreis C und ein ihn umschließendes Quadrat mit den Ecken $R_1, \ldots R_4$ konstruiert. Die Abschätzung des Kreisdurchmessers

$$\left| \frac{5f(\alpha)}{f'(\alpha)} \right|^2 = \frac{25\,(25\,n^{18}-89\,n^{17}+491\,n^{16}-1286\,n^{15}+4809\,n^{14}-11164\,n^{13}+29414\,n^{12}+\ldots)}{n^4\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+\ldots)} < \frac{625}{4n^3}$$

gilt für alle $n > 0$. Die Ecken $R_1, \ldots, R_4$ des Quadrates erhält man in diesem Fall durch

$$\alpha - \frac{5f(\alpha)}{2\,f'(\alpha)} \pm \frac{25}{4n\sqrt{n}} \pm \frac{25\,i}{4n\sqrt{n}}$$

und die konkrete Berechnung ergibt:

$$R_1 = \frac{4\,n^{20,5}+20\,n^{19,5}-25\,n^{19}+61\,n^{18,5}+\ldots}{4\,n^{20,5}+24\,n^{19,5}+68\,n^{18,5}+\ldots} + \frac{8\,n^{18}+48\,n^{17}+376\,n^{16}+1319\,n^{15}+\ldots}{8\,n^{18,5}+48\,n^{17,5}+136\,n^{16,5}+914\,n^{15,5}+\ldots}\,i,$$

$$R_2 = \frac{4\,n^{20,5}+20\,n^{19,5}+25\,n^{19}+61\,n^{18,5}+\ldots}{4\,n^{20,5}+24\,n^{19,5}+68\,n^{18,5}+\ldots} + \frac{8\,n^{18}+48\,n^{17}+376\,n^{16}+1319\,n^{15}+\ldots}{8\,n^{18,5}+48\,n^{17,5}+136\,n^{16,5}+914\,n^{15,5}+\ldots}\,i,$$

[11] Die exakten Formeln finden sich in Anhang C.2.

$$R_3 = \frac{4\,n^{20,5}+20\,n^{19,5}-25\,n^{19}+61\,n^{18,5}+\ldots}{4\,n^{20,5}+24\,n^{19,5}+68\,n^{18,5}+\ldots} + \frac{8\,n^{18}-52\,n^{17}-224\,n^{16}-381\,n^{15}+\ldots}{8\,n^{18,5}+48\,n^{17,5}+136\,n^{16,5}+914\,n^{15,5}+\ldots}\,i,$$

$$R_4 = \frac{4\,n^{20,5}+20\,n^{19,5}+25\,n^{19}+61\,n^{18,5}+\ldots}{4\,n^{20,5}+24\,n^{19,5}+68\,n^{18,5}+\ldots} + \frac{8\,n^{18}-52\,n^{17}-224\,n^{16}-381\,n^{15}+\ldots}{8\,n^{18,5}+48\,n^{17,5}+136\,n^{16,5}+914\,n^{15,5}+\ldots}\,i.$$

Alle vier Ecken liegen für $n > 10$ im 1. Quadranten.[12] Eine Abschätzung für $\varrho^{(4)}$ lautet also

$$|R_3| < \left|\varrho^{(4)}\right| < |R_2|\,.$$

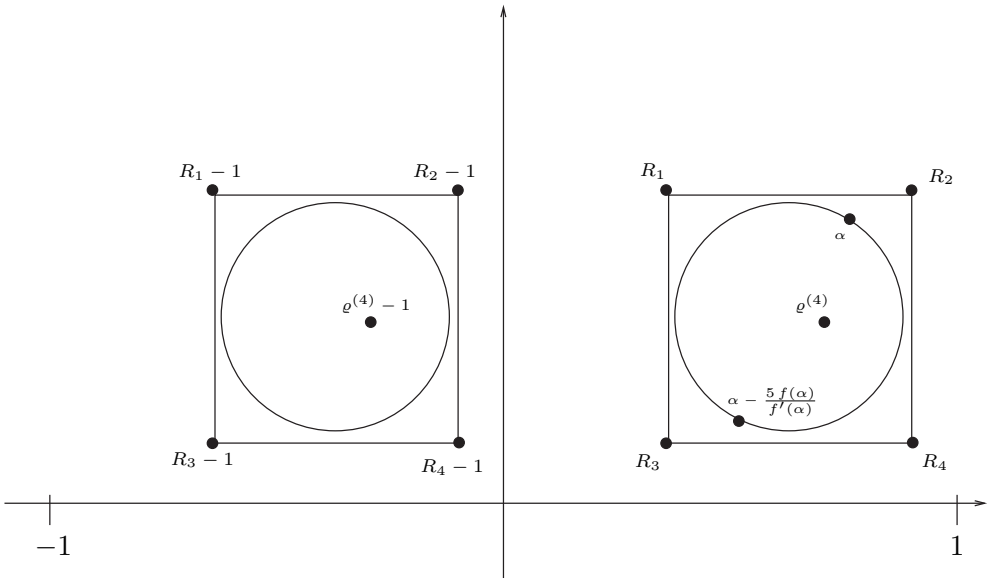

Abbildung 3.3: Approximation von $\varrho^{(4)}$ und $\varrho^{(4)} - 1$

Da für $n > 174$ die Abschätzung[13]

$$|R_2| = \left(\left(\frac{n^{20,5}+5\,n^{19,5}+\ldots}{n^{20,5}+6\,n^{19,5}+\ldots}\right)^2 + \left(\frac{n^{18}+6\,n^{17}+47\,n^{16}\ldots}{n^{18,5}+6\,n^{17,5}+17\,n^{16,5}+\ldots}\right)^2\right)^{(1/2)} < \sqrt{1-\frac{1}{n^2}}$$

und für $n > 49$

$$|R_3| = \left(\left(\frac{n^{20,5}+5\,n^{19,5}-\ldots}{n^{20,5}+6\,n^{19,5}+\ldots}\right)^2 + \left(\frac{2\,n^{18}-13\,n^{17}-\ldots}{2\,n^{18,5}+12\,n^{17,5}+\ldots}\right)^2\right)^{(1/2)} > \sqrt{1-\frac{3}{n}}$$

gilt, folgt die Behauptung für $\rho^{(4)}$.

[12] Konkret gilt: $\Re(R_3) > 0$ für $n > 4$ und $\Im(R_3) > 0$ für $n > 10$.
[13] Selbst die gröbere Abschätzung $|R_2| < 1$ gilt erst für $n > 172$.

Zur Abschätzung von $\varrho^{(4)} - 1$ ist die Beobachtung $\Re(R_i) < 1$ für $1 \leq i \leq 4$ hilfreich, denn somit liegen die vier verschobenen Ecken $R_1 - 1, \ldots R_4 - 1$ alle im zweiten Quadranten (siehe Abb. 3.3) und es gilt

$$|R_1 - 1| > \left|\varrho^{(4)} - 1\right| > |R_4 - 1| .$$

Die konkrete Rechnung und Abschätzung ergibt die Ungleichung

$$|R_1 - 1| = \left((\tfrac{n^{20,5}+5\,n^{19,5}-\ldots}{n^{20,5}+6\,n^{19,5}+\ldots} - 1)^2 + (\tfrac{n^{18}+6\,n^{17}+47\,n^{16}\ldots}{n^{18,5}+6\,n^{17,5}+17\,n^{16,5}\ldots})^2 \right)^{(1/2)} < \sqrt{\tfrac{14}{13\,n}}$$

für $n > 54$, und die Ungleichung

$$|R_4 - 1| = \left((\tfrac{n^{20,5}+5\,n^{19,5}+\ldots}{n^{20,5}+6\,n^{19,5}+\ldots} - 1)^2 + (\tfrac{2\,n^{18}-13\,n^{17}-\ldots}{2\,n^{18,5}+12\,n^{17,5}+\ldots})^2 \right)^{(1/2)} > \sqrt{\tfrac{5}{6\,n}}$$

für $n > 139$, aus denen die Behauptung für $\rho^{(4)}$ folgt.

Lage von $\varrho^{(2)}$ und $\varrho^{(4)}$

Zuletzt muss gezeigt werden, dass sich $\varrho^{(2)}$ und $\varrho^{(4)}$ (und damit $\rho^{(2)}$ und $\rho^{(4)}$) tatsächlich unterscheiden. Dies folgt aus der Lage der Nullstellen (dicht bei 0 im ersten Fall und dicht bei 1 im zweiten Fall) beziehungsweise aus der Lage der sie umgebenden Quadrate.

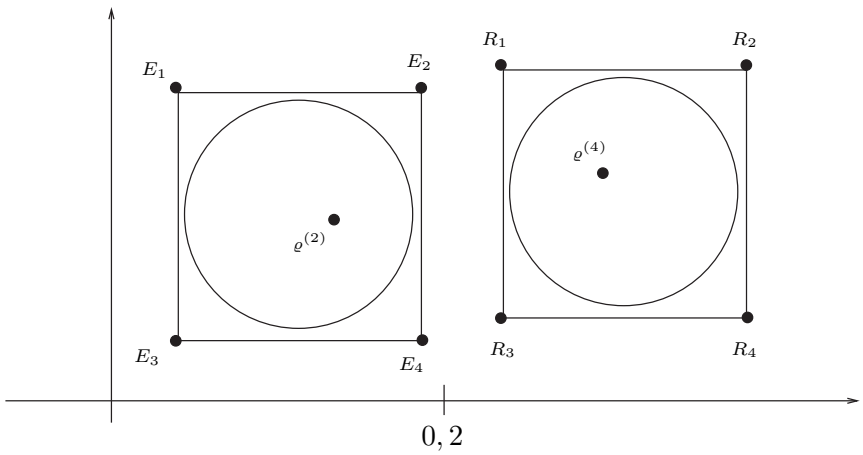

Abbildung 3.4: Lage der Nullstellen $\varrho^{(2)}$ und $\varrho^{(4)}$ im 1. Quadranten

Beim zuerst konstruierten Quadrat für $\alpha = \frac{1}{2n^2} + \frac{i}{\sqrt{n}}$ ist der Realteil der rechten oberen Ecke (ausführlicher als zuvor)

$$\Re(E_2) = \frac{5\,n^{19}+2\,n^{18,5}+20\,n^{18}-5\,n^{17,5}+10\,n^{17}-\frac{1}{2}\,n^{16,5}+15\,n^{16}+5\,n^{15,5}+5\,n^{15}+\ldots+\frac{25}{1024}\sqrt{n}}{4\,n^{2,5}\,(n+1)(n^{17}+4\,n^{16}+2\,n^{15}+3\,n^{14}+n^{13}+\frac{19}{4}\,n^{12}+7\,n^{11}+\ldots+\frac{25}{1024})},$$

während der Realteil der linken oberen Ecke des zu $\alpha = 1 - \frac{1}{n} + \frac{3}{n^2} + \frac{i}{\sqrt{n}}$ gehörenden Quadrates (ebenfalls ausführlicher als zuvor) den Wert

$$\Re(R_1) = \frac{\left(4\,n^{19}+20\,n^{18}-25\,n^{17,5}+61\,n^{17}-150\,n^{16,5}+\frac{427}{2}\,n^{16}+\ldots+\frac{492075}{2}\right)}{n^2\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+\ldots-437400\,n+164025)}$$

besitzt. Für diese beiden Realteile gilt $\Re(E_2) < \frac{1}{5} < \Re(R_1)$ für alle $n > 4$, so dass sich die Situation wie in Abbildung 3.4 ergibt.[14]

Folglich sind die beiden konstruierten Quadrate disjunkt und die Nullstellen $\varrho^{(2)}$ und $\varrho^{(4)}$ verschieden, so dass Lemma 3.1.22 gezeigt ist. □

Mit Hilfe der gezeigten Abschätzungen ist die Lage der fünf Nullstellen von $F_5(x)$ für $n \geq 7$ (siehe Lemma 3.1.20) und für $n \leq -175$ (siehe Lemma 3.1.22) hinreichend bekannt, um Satz 3.1.19 zu beweisen.

Beweis von Satz 3.1.19. Sei zunächst $n \geq 7$. Um die Unabhängigkeit der beiden Einheiten ρ und $\rho-1$ zu zeigen, nimmt man deren Abhängigkeit in der Form $\rho^k = \pm(\rho-1)^l$ mit $k, l \in \mathbb{Z}$ an. Gilt diese Gleichheit, so gilt sie für alle Konjugierten, insbesondere auch für $\rho^{(1)}$ und $\rho^{(3)}$. Nach den Abschätzungen in 3.1.20 hat man $|\rho^{(1)}| < 1 < |\rho^{(1)} - 1|$ und $|\rho^{(3)} - 1| < \frac{2}{5} < \frac{3}{5} < |\rho^{(3)}| < 1$. Für $k > 0$ folgt für die erste Konjugierte somit, dass $l < 0$ ist; andererseits folgt für die dritte Konjugierte, dass $l > 0$ ist. Analoge Überlegungen liefern ebenfalls einen Widerspruch für $k < 0$. Somit folgt die Unabhängigkeit der beiden Einheiten ρ und $\rho - 1$ für $n \geq 7$.

Sei nun $n \leq -175$. In diesem Fall existieren nach 3.1.17 eine reelle und zwei Paar konjugiert komplexer Nullstellen. Gelte $\rho^k = \pm(\rho-1)^l$ mit $k, l \in \mathbb{Z}$. Laut Lemma 3.1.22 gilt einerseits $0 < |\rho^{(2)}| < 1 < |\rho^{(2)} - 1| < 2$ und andererseits $0 < |\rho^{(4)}-1| < |\rho^{(4)}| < 1$, so dass für $k > 0$ mit der zweiten Konjugierten $l < 0$ und mit der vierten Konjugierten $l > 0$ folgt. Einen analogen Widerspruch erhält man für $k < 0$.

Zum Beweis, dass diese Einheiten Fundamentaleinheiten in der Gleichungsordnung $\mathbb{Z}[\rho]$ sind, wird eine obere und eine untere Regulatorabschätzung

[14] Beide Imaginärteile streben mit $n \to \infty$ gegen 0, wobei $\Im(R_1) > \Im(E_2)$ für alle $n > 0$ gilt.

berechnet. Da die durch $F_5(x)$ erzeugte Körpererweiterung $\mathbb{Q}(\rho)/\mathbb{Q}$ keine Zwischenkörper besitzt und da $|\mathrm{disc}(\mathbb{Z}[\rho])| = (4\,n^3 - 28\,n^2 + 24\,n - 47)^2 > 5^5$ für $n \leq -175$ ist, gilt die von Pohst und Zassenhaus ([78], 5.6.22) angegebene untere Regulatorschranke

$$\mathrm{Reg}(\mathbb{Z}[\rho]) \geq \sqrt{\frac{3}{5}}\,\frac{\left(\log(\frac{(4\,n^3-28\,n^2+24\,n-47)^2}{5^5})\right)^2}{36}.$$

Vereinfachungen und Abschätzungen dieser Schranke führen für $n \leq -175$ mit $\sqrt{5}^5 < 56$ zu

$$\begin{aligned}
\mathrm{Reg}(\mathbb{Z}[\rho]) &\geq \sqrt{\frac{3}{5}}\,\frac{1}{36}\left(\log\left(\left(\frac{4n^3}{\sqrt{5}^5}\right)^2\right)\right)^2 \\
&= \sqrt{\frac{3}{5}}\,\frac{1}{9}\left(\log\left(\frac{-4n^3}{\sqrt{5}^5}\right)\right)^2 \\
&\geq \frac{1}{3\sqrt{15}}\,(3\log(-n) - \log(14))^2 \quad =: R_u.
\end{aligned}$$

Eine obere Regulatorschranke wird mit Hilfe der Abschätzungen von $\rho^{(1)}$ und $\rho^{(4)}$ aus Lemma 3.1.22 berechnet:

$$\begin{aligned}
\mathrm{Reg}(\mathbb{Z}[\rho]) &= \left|\det\begin{pmatrix} \log|\rho^{(1)}| & 2\,\log|\rho^{(4)}| \\ \log|\rho^{(1)}-1| & 2\,\log|\rho^{(4)}-1| \end{pmatrix}\right| \\
&= -2\,\left(\log|\rho^{(1)}|\,\log|\rho^{(4)}-1| - \log|\rho^{(1)}-1|\,\log|\rho^{(4)}|\right) \\
&\leq 2\left(\log(-n+2+\frac{1}{n})\cdot(-\log\left((\frac{-5}{6\,n})^{(1/2)}\right))\right).
\end{aligned}$$

Die letzte Ungleichung folgt aus $|\rho^{(1)} - 1| > 1$ und $|\rho^{(4)}| < 1$. Man erhält damit die obere Regulatorschranke

$$\mathrm{Reg}(\mathbb{Z}[\rho]) \leq \left(\log(-n) + \log(1 - \frac{2}{n} - \frac{1}{n^2})\right)\cdot\left(\log(-n) + \log(\frac{6}{5})\right),$$

die mit $n \leq -175$ weiter abgeschätzt und vereinfacht werden kann zu

$$\leq \left(\log(-n) + \log(1 + \frac{2}{175})\right)\cdot\left(\log(-n) + \log(\frac{6}{5})\right) \quad =: R_o.$$

Der Quotient $\frac{R_o}{R_u}$ aus oberer und unterer Regulatorschranke ist für $n < -130$ kleiner als 2. Also ist für alle $n \leq -175$ die Menge $\{\rho, \rho - 1\}$ ein Grundeinheitensystem von $\mathbb{Z}[\rho]$.

Die Unabhängigkeit und die Fundamentalität der Einheiten ρ und $\rho - 1$ in der Gleichungsordnung $\mathbb{Z}[\rho]$ für $-174 \leq n < 6$ wurde mit KANT [32] nachgewiesen. □

Bemerkung 3.1.23. *Im Fall $n = 6$ sind die beiden Einheiten ρ und $\rho - 1$ weiterhin unabhängig, wie sich mit KANT [32] überprüfen lässt. Sie erzeugen jedoch nicht die Einheitengruppe von $\mathbb{Z}[\rho]$. Die Menge $\{2\rho^4 - 11\rho^3 + 16\rho^2 + 2\rho - 4, \rho^4 - 5\rho^3 + 6\rho^2 + 3\rho - 2\}$ ist ein System von Grundeinheiten. Die Gleichungsordnung ist in diesem Fall maximal.*

Die diesen Abschnitt 3.1.4 abschließende Überlegung beschäftigt sich mit der Maximalität der Gleichungsordnung. Bekanntlich kann eine Gleichungsordnung nur bezüglich der Primzahlen $p \in \mathbb{P}$ nicht maximal sein, die quadratisch in der Diskriminante der Gleichungsordnung aufgehen. Die Gleichungsordnung $\mathbb{Z}[\rho]$ besitzt in den betrachteten Fällen, in denen ρ eine Nullstelle von $F_5(x) = x^5 - n\,x^4 + (2\,n - 1)\,x^3 - (n - 2)\,x^2 - 2\,x + 1$ ist, die Diskriminante $(d(n))^2 = (4\,n^3 - 28\,n^2 + 24\,n - 47)^2$, die also ein reines Quadrat ist. Damit ist $\mathbb{Z}[\rho]$ bzgl. jeder Primzahl p, die $d(n)$ teilt, zu untersuchen. Offensichtlich ist die Gleichungsordnung p-maximal, falls $p \nmid d(n)$.

Einfache Untersuchungen zeigen, dass $2 \nmid d(n)$ für alle $n \in \mathbb{Z}$ gilt, denn sowohl für $n \equiv 0 \bmod 2$ als auch $n \equiv 1 \bmod 2$ ist $d(n) \equiv 1 \bmod 2$. Analoges folgt für $p = 3, 5, 23, \ldots$. Entsprechende Betrachtungen zeigen, dass für $p \in \{2, 3, 5, 23, 31, 37, 59, 67, 71, 89, 97, 113, 137, 157, 179, 181, 191, 223\}$ die Gleichungsordnung jeweils p-maximal ist. Zur Untersuchung der p-Maximalität von $\mathbb{Z}[\rho]$ für andere Primzahlen $p \in \mathbb{P}$ ist das Dedekind-Kriterium hilfreich.

Dedekind-Kriterium 3.1.24 (Pohst/Zassenhaus, [78], 4.5.55). *Sei $f(t) \equiv \prod_{i=1}^{m} f_i(t)^i \bmod p\mathbb{Z}[t]$ eine Kongruenzfaktorisierung von $f(t)$ in normierte Polynome $f_i(t) \in \mathbb{Z}[t]$, die koprim und separabel modulo $p\mathbb{Z}[t]$ sind. Sei $h(t) := \frac{1}{p}\,(f(t) - \prod_{i=1}^{m} f_i(t)^i) \in \mathbb{Z}[t]$. Dann ist die Gleichungsordnung $\mathbb{Z}[\rho]$ genau dann p-maximal, wenn $ggT(h(t), \prod_{i=2}^{m} f_i(t)) = 1$ in $\mathbb{F}_p[t]$ gilt.*

Exemplarisch wird in den folgenden beiden Betrachtungen bzgl. der Primzahlen $p = 7, 11$ untersucht, ob die Gleichungsordnungen $\mathbb{Z}[\rho]$ p-maximal sind.

Betrachtung 1: $p = 7$

Eine Untersuchung und Faktorisierung von $F_5(x)$ modulo 7 ist erst sinnvoll, wenn man die möglichen Fälle $n \equiv 0, 1, 2, \ldots, 6 \bmod 7$ einzeln betrachtet. Dabei ergeben sich mit $n = i + 7\,k$ folgende Faktorisierungen modulo 7:

$$\begin{aligned}
i = 0: &\quad F_5(x) \equiv x^5 + 6\,x^3 + 2\,x^2 + 5\,x + 1,\\
i = 1: &\quad F_5(x) \equiv x^5 + 6\,x^4 + x^3 + x^2 + 5\,x + 1,\\
i = 2: &\quad F_5(x) \equiv (x^2 + 5\,x + 5)\,(x^2 + 2\,x + 2)\,(x + 5),\\
i = 3: &\quad F_5(x) \equiv (x + 2)^2\,(x + 3)^2\,(x + 1),\\
i = 4: &\quad F_5(x) \equiv x^5 + 3\,x^4 + 1 + 5\,x^2 + 5\,x,\\
i = 5: &\quad F_5(x) \equiv (x^2 + 2\,x + 5)\,(x + 4)\,(x^2 + 3\,x + 6),\\
i = 6: &\quad F_5(x) \equiv x^5 + x^4 + 4\,x^3 + 3\,x^2 + 5\,x + 1.
\end{aligned}$$

Das Dedekind-Kriterium 3.1.24 untersucht das Produkt der Faktoren f_i der Kongruenzfaktorisierung von $F_5(x)$, die mindestens quadratisch in dieser Faktorisierung auftreten. Tritt kein Faktor quadratisch oder mit einer höheren Potenz auf, so ist der größte gemeinsame Teiler 1 und die Gleichungsordnung 7-maximal. Damit bleibt in dieser ersten Betrachtung nur der Fall $n = 3+7k$ übrig.

Zur Berechnung des größten gemeinsamen Teilers wird $h(x)$ und $\prod_{i=2}^{m} f_i(x)$ benötigt. Es ist $\prod_{i=2}^{m} f_i(x) = (x + 2)\,(x + 3)$ und $h(x)$ berechnet sich zu $h(x) = \frac{1}{7}\,(F_5(x) - (x + 2)^2\,(x + 3)^2\,(x + 1)) = -(k + 2)\,x^4 + (2\,k - 6)\,x^3 - (k + 14)\,x^2 - 14\,x - 5$. Sei $k = j + 7\,l$ und durchlaufe j die Zahlen $0, \ldots, 6$. Dabei ergibt sich

$$\mathrm{ggT}\,(h(x), \prod_{i=2}^{m} f_i(x)) = 1 \quad \text{für alle } j \neq 4$$

bzw. für $j = 4$

$$\mathrm{ggT}\left(-(7\,l+6)\,x^4+(14\,l+2)\,x^3-(7\,l+18)\,x^2-14\,x-5, (x+2)\,(x+3)\right) = x^2 + 5\,x + 6.$$

Damit wurde gezeigt, dass für $n = 3 + 7\,k = 3 + 7\,(4 + 7\,l) = 31 + 49\,l$, also für $n \equiv 31 \pmod{7^2}$, die Gleichungsordnung $\mathbb{Z}[\rho]$ nicht 7-maximal ist.

Betrachtung 2: $p = 11$

Für $p = 11$ faktorisiert sich $F_5(x)$ mit $n = i + 11\,k$ modulo 11 wie folgt:

$$\begin{aligned}
i = 0: &\quad F_5(x) \equiv (x^2 + x + 8)\,(x^2 + 8\,x + 9)\,(x + 2),\\
i = 1: &\quad F_5(x) \equiv (x^2 + 7\,x + 2)\,(x + 5)\,(x^2 + 9\,x + 10),\\
i = 2: &\quad F_5(x) \equiv x^5 + 9\,x^4 + 3\,x^3 + 9\,x + 1,\\
i = 3: &\quad F_5(x) \equiv (x^2 + 6\,x + 1)\,(x + 8)\,(x^2 + 5\,x + 7),
\end{aligned}$$

$$
\begin{aligned}
i = 4 &: \quad F_5(x) \equiv (x+6)^2\,(x+4)\,(x+1)^2,\\
i = 5 &: \quad F_5(x) \equiv x^5 + 6\,x^4 + 9\,x^3 + 8\,x^2 + 9\,x + 1,\\
i = 6 &: \quad F_5(x) \equiv (x^2 + 7\,x + 5)\,(x^2 + 2\,x + 6)\,(x+7),\\
i = 7 &: \quad F_5(x) \equiv (x+3)^5,\\
i = 8 &: \quad F_5(x) \equiv x^5 + 3\,x^4 + 4\,x^3 + 5\,x^2 + 9\,x + 1,\\
i = 9 &: \quad F_5(x) \equiv x^5 + 2\,x^4 + 6\,x^3 + 4\,x^2 + 9\,x + 1,\\
i = 10 &: \quad F_5(x) \equiv (x^2 + 8\,x + 8)\,(x+9)\,(x^2 + 6\,x + 2).
\end{aligned}
$$

Die Fälle $i = 4, 7$ müssen weiter untersucht werden, da dort in der modularen Faktorisierung Faktoren mit Potenzen größer 1 auftreten. In allen anderen Fällen sind die Gleichungsordnungen $\mathbb{Z}[\rho]$ 11-maximal.

Sei $i = 4$. Dann ist $\prod_{i=2}^{m} f_i(x) = (x+6)\,(x+1)$ und das Polynom $h(x)$ lautet $h(x) = -(k+2)\,x^4 + (2\,k-10)\,x^3 - (k+30)\,x^2 - 34\,x - 13$. Durchläuft nun k die möglichen Zahlen modulo 11, so lässt sich der ggT einfach berechnen: Für $k = j + 11\,l$ erhält man für $j \neq 8$ immer ggT $= 1$. Nur im Fall $j = 8$ ist ggT $= x^2 + 7\,x + 6$. Somit ist die Gleichungsordnung für $n \equiv 92 \bmod 11^2$ nicht 11-maximal.

Sei nun $i = 7$. Wie man in vorstehender Liste sieht, ist $\prod_{i=2}^{m} f_i(x) = x + 3$ und man erhält $h(x) = -(k+2)\,x^4 + (2\,k-7)\,x^3 - (k+25)\,x^2 - 37\,x - 22$. Für $k = j + 11\,l$ mit $j = 0, 1, \ldots, 10$ ergibt sich nur im Fall $j = 1$ ein ggT ungleich 1, und zwar $x^3 + 9\,x^2 + 5\,x + 5$. Die Gleichungsordnung $\mathbb{Z}[\rho]$ ist folglich auch für $n \equiv 18 \bmod 11^2$ nicht 11-maximal.

Weitere analoge Betrachtungen für $p = 13, 17, 19, 29, 41, 43, 47, 53, 61$ führen zur folgenden Aussage zur Maximalität der Gleichungsordnung:

Bemerkung 3.1.25. *Für $F_5(x)$ (mit $b = 1$) ist die durch eine Nullstelle ρ dieses Polynoms erzeugte Gleichungsordnung $\mathbb{Z}[\rho]$ nicht maximal, sofern n eine der folgenden Formen besitzt:*
$n \equiv 31 \bmod 7^2$, $n \equiv 18, 92 \bmod 11^2$, $n \equiv 134 \bmod 13^2$, $n \equiv 88 \bmod 17^2$, $n \equiv 237 \bmod 19^2$, $n \equiv 361 \bmod 29^2$, $n \equiv 98 \bmod 41^2$, $n \equiv 1815 \bmod 43^2$, $n \equiv 94, 330, 1792 \bmod 47^2$, $n \equiv 1339, 2091, 2195 \bmod 52^2$, $n \equiv 897 \bmod 61^2$.

Diese Bemerkung kann durch Betrachtung weiterer Primzahlen erweitert werden. Sinnvoll ist eine genauere Untersuchung von $p = 11$. Eine einfache modulare Rechnung zeigt, dass $d(n) = 4\,n^3 - 28\,n^2 + 24\,n - 47 \equiv 0 \bmod 11$ für $n \equiv 4, 7 \bmod 11$ ist. Also wird $d(n)$ genau dann von 11 geteilt, wenn $n \equiv 4, 7 \bmod 11$ ist. Es gilt sogar, dass $11^2 \mid d(n)$, falls $n \equiv 7 \bmod 11$ ist. Untersucht man nun die Teilbarkeit von $d(n)$ durch 11^2 für $n \bmod 11^2$, so erhält man: $11^2 \mid d(n) \Leftrightarrow n \equiv 7 \bmod 11$ oder $n \equiv 92 \bmod 11^2$.
Für $n = 18 + 11^2\,k$ gilt sogar $11^4 \mid d(n)$.

Nach Bemerkung 3.1.25 ist die Gleichungsordnung $\mathbb{Z}[\rho]$ nicht maximal, wenn $n \equiv 18, 92 \bmod 11^2$ ist. Ist $n \equiv 18 \bmod 11^2$, so ist $n \equiv 7 \bmod 11$ und 11^4 teilt $d(n)$. In den anderen Fällen $n \equiv 7 \bmod 11$ und $n \not\equiv 18 \bmod 11^2$ gilt $11^2 \mid d(n)$, und die Gleichungsordnung ist 11-maximal. Und zuletzt ist $\mathbb{Z}[\rho]$ nicht maximal für $n \equiv 92 \bmod 11^2$, welches der einzige verbliebene Fall ist, in dem $11^2 \mid d(n)$.

Somit ist das folgende Lemma bewiesen:

Lemma 3.1.26. *Für $F_5(x)$ (mit $b = 1$) ist $\mathbb{Z}[\rho]$ nicht maximal, wenn $n \not\equiv 7 \bmod 11$ ist und $d(n) = 4\,n^3 - 28\,n^2 + 24\,n - 47$ von 11^2 geteilt wird.*[15] *Gilt im Fall $n \equiv 7 \bmod 11$, dass $11^3 \not| \, d(n)$, so ist $\mathbb{Z}[\rho]$ 11-maximal.*

Zahlreiche Berechnungen lassen sogar die folgende, weitergehende Aussage vermuten, die auf Grund der parametrisierten Form von $F_5(x)$ und der Tatsache, dass die Diskriminante der Gleichungsordnung $\mathbb{Z}[\rho]$ ein reines Quadrat ist, mit den üblichen Hilfsmitteln nicht allgemein bewiesen werden kann.

Vermutung 3.1.27. *Für $F_5(x)$ (mit $b = 1$) ist die Gleichungsordnung $\mathbb{Z}[\rho]$ genau dann maximal, wenn*

i) $d(n)$ quadratfrei ist oder

ii) im Fall $n \equiv 7 \bmod 11$ die Primzahl 11 mit der exakten Potenz 2 in $d(n)$ aufgeht und $d(n)$ ansonsten quadratfrei ist.

3.1.5 Arithmetik für Zahlkörper vom Grad 6

Analog zu den vorangegangenen Abschnitten 3.1.3 und 3.1.4 befasst sich dieser Abschnitt mit parametrisierten Einheiten der Gleichungsordnung $\mathbb{Z}[\rho]$ für $n \in \mathbb{Z}$.

Die in Abschnitt 3.1.2 ($l = 6$) berechneten Polynome

$$\begin{aligned} F_6(x) \;=\; & x^6 - n\,x^5 + \\ & c\,((2c+3)n - (c+1)(4c+1))x^4 - \\ & c^2(c+1)((c+3)n - 2(c+2)(c+1))x^3 + \\ & c^3(c+1)^2(n - 2(c+3))\,x^2 + \\ & c^4(c+1)^3\,4\,x - c^5(c+1)^4 \end{aligned}$$

[15] Beachte, dass $d(n)$ nicht die Disriminante der Gleichungsordnung ist, sondern deren positive Quadratwurzel.

lassen auf Grund des konstanten Terms $c^5\,(c+1)^4$ nicht hoffen, parametrisierte Einheiten zu finden. Die durch die Transformation $x \mapsto \frac{c\,(c+1)}{x+1}$ gefundene einfachere Form (siehe auch Abschnitt 3.1.2)

$$\begin{aligned}\tilde{F}_6(x) &= x^6 + 2\,x^5 - (n - 2\,c - 1)\,x^4 + \\ &\quad (n - 2\,c)\,(c - 1)\,x^3 + c\,(n - 2\,c - 1)\,x^2 + 2\,c^2\,x - c^3\end{aligned}$$

führt jedoch mit $c = 1$ unmittelbar zu

$$x^6 + 2\,x^5 - (n - 3)\,x^4 + (n - 3)\,x^2 + 2\,x - 1,$$

und man kann ablesen, dass für ganzzahlige n die Nullstellen ρ dieses Polynoms Einheiten in den jeweiligen Gleichungsordnungen $\mathbb{Z}[\rho]$ sind. [16]

Die Möglichkeit $c = -1$ lässt $\tilde{F}_6(x)$ reduzibel werden, so dass im Folgenden $c = 1$ betrachtet wird.

Die Diskriminante von $\tilde{F}_6(x)$ (mit $c = 1$) lautet $64(n - 13)^2(n^2 - 4n + 8)^3$. Bezüglich der Irreduzibilität lässt sich durch Untersuchung der möglichen Zerlegungen (Linearfaktor, quadratisches Polynom, Polynom vom Grad 3) überprüfen, dass $\tilde{F}_6(x)$ nur für $n = 2$ und $n = 13$ reduzibel wird. Somit wird $n \in \mathbb{Z}\backslash\{2, 13\}$ vorausgesetzt, damit die Polynome irreduzibel bleiben.

Satz 3.1.28. *Das Polynom $\tilde{F}_6(x)$ besitzt (mit $c = 1$) die Signatur $(2, 2)$, falls $n < 13$ und die Signatur $(6, 0)$, falls $n > 13$ ist.*

Beweis. Die Diskriminante $64\,(n - 13)^2\,(n^2 - 4\,n + 8)^3$ ist für alle $n \neq 13$ positiv, so dass $\tilde{F}_6(x)$ entweder zwei oder sechs reelle Nullstellen besitzt.

Die Existenz der sechs reellen Nullstellen für $n > 13$ ist leicht durch Vorzeichenwechsel von $\tilde{F}_6(x)$ an bestimmten Stellen gezeigt:
Es ist $\tilde{F}_6(-1) = -4$ und $\tilde{F}_6(-\frac{1}{2}) = \frac{12\,n-167}{64} > 0$ für $n \geq 14$. Weiter ist $\tilde{F}_6(0) = -1$ und $\tilde{F}_6(1) = 4$, so dass für $n \geq 14$ drei reelle Nullstellen existieren, womit zusammen mit der positiven Diskriminante die Signatur $(6, 0)$ folgt.

Für $n < 13$ wird wie im Beweis zu Satz 3.1.17 ein Satz von Sturm (siehe z. B. H. Cohen [6], 4.1.10+4.1.11) angewandt: Durch Polynomdivision werden die Polynome $A_0, A_1, \ldots, A_6$ bestimmt, wobei $A_0 = \tilde{F}_6(x)$ und $A_1 = \tilde{F}_6'(x)$, die formale Ableitung von $\tilde{F}_6(x)$, ist. Die weiteren A_i berechnen sich durch $A_{i-2} = A_{i-1}\,Q_i - A_i$. Betrachtet werden anschließend die führenden Koeffizienten l_i der A_i: Es sind $l_0 = 1$ und $l_1 = 6$, und bis auf positive Faktoren und

[16] Weitere Einheiten in parametrisierter Form wurden nicht gefunden.

quadratische Nenner lauten die anderen Koeffizienten

$$l_2 = 3\,n - 4, \qquad l_3 = (n-3)\,(n^2 - 8\,n + 10),$$

$$l_4 = (n^2 - 4\,n + 8)\,(2\,n^3 - 34\,n^2 + 125\,n - 148)\,(3\,n - 4)^2,$$

$$l_5 = (n - 13)\,(n^2 - 11\,n + 9)\,(n-3)^2\,(n^2 - 8\,n + 10)^2,$$

und

$$l_6 = (n^2 - 4\,n + 8)\,(2\,n^3 - 34\,n^2 + 125\,n - 148)^2\,(3\,n - 4)^2.$$

Sei $\omega(n)$ die Anzahl der Vorzeichenwechsel in der von n abhängigen Sequenz $l_0, -l_1, l_2(n), -l_3(n), l_4(n), -l_5(n), l_6(n)$ und $\nu(n)$ die Anzahl der Vorzeichenwechsel in $l_0, l_1, l_2(n), l_3(n), l_4(n), l_5(n), l_6(n)$, so ist $\omega(n) - \nu(n)$ die Anzahl der reellen Nullstellen von $\tilde{F}_6(x)$. Für jedes $n < 13$ erhält man $\omega(n) = 4$ und $\nu(n) = 2$, so dass die Behauptung folgt. □

Die Galoisgruppe von $\tilde{F}_6(x)$ ist nach Satz 3.1.5 bekannt und ist im Allgemeinen die Diedergruppe mit zwölf Elementen. Die Frage, unter welchen Bedingungen auch C_l als Galoisgruppe auftritt, kann nicht unmittelbar für $\tilde{F}_6(x)$ beantwortet werden, da die Nullstellen laut Satz 3.1.3 nur für $F_6(x)$ bekannt sind. Die Nullstellen werden jedoch benötigt, um mit der Indikatorfunktion Bedingungen herzuleiten. Für $F_6(x)$ wird die Frage im folgenden Abschnitt 3.2 behandelt und es werden Unterfamilien mit zyklischer Galoisgruppe berechnet.

3.2 Zahlkörper mit Galoisgruppe C_l

3.2.1 Allgemeine Situation

Im Anschluss an die Konstruktion der Familien von Polynomen mit Galoisgruppe D_l schließt sich unmittelbar die Frage an, ob Unterfamilien angegeben werden können, die eine Untergruppe der D_l als Galoisgruppe besitzen. Im Folgenden werden die Polynome im Hinblick auf die zyklische Gruppe mit l Elementen untersucht. Auf Grund der Kenntnis der Nullstellen der konstruierten Polynome $F_l(x)$ können mit Indikatorfunktionen Bedingungen aufgestellt werden, wann $F_l(x)$ die Galoisgruppe C_l besitzt.

Lemma 3.2.1 (Geißler [21], 6.4+6.24). *Sei $F_l(x)$ wie in 3.1.1 konstruiert. Seien $x_i := x(P \oplus iA)$ die Nullstellen von $F_l(x)$ mit $1 \le i \le l$. Dann gilt:*

Das Polynom $F_l(x)$ (genauer der Zerfällungskörper dieses Polynoms) besitzt die Galoisgruppe C_l genau dann, wenn der Ausdruck $\mathcal{C}_l := \mathcal{C}_l(x_1, \ldots, x_l)$ schon in $\mathbb{Q}$ liegt. Dabei ist mit $x_{l+k} = x_k$

$$\mathcal{C}_l := \sum_{i=1}^{l} x_i x_{i+1}^2, \quad \textit{falls} \quad 4 \nmid l,$$

und ansonsten mit $j := l/4$

$$\mathcal{C}_l := \sum_{i=1}^{l} x_i x_{i+j}^2.$$

Wie bereits in Abschnitt 3.1.1 angegeben, sind die x_i in den zu untersuchenden Fällen rationale Ausdrücke in x_P, y_P und den Parametern der elliptischen Kurve E_l, von der die Konstruktion 3.1.1 ausgegangen ist. Nutzt man die Kenntnis dieser Funktionen $\mathcal{C}_l = \mathcal{C}_l(x_P, y_P, c)$, (wobei hier c stellvertretend für die Parameter von E_l steht), das Wissen, dass die x_i Nullstellen von $F_l(x)$ sind und den Zusammenhang von x_P und y_P über die elliptische Kurve E_l, so erhält man durch Resultantenbildung ein normiertes, quadratisches Polynom in $\mathcal{C}_l$ mit Koeffizienten in $\mathbb{Q}(n, c)$.

Sei $\mathcal{C}_l^2 + \alpha_l(n,c)\,\mathcal{C}_l + \beta_l(n,c)$ das quadratische Polynom, das nach Eliminierung von x_P, y_P mit $F_l(x), E_l$ aus $\mathcal{C}_l$ entsteht. Die nach Lemma 3.2.1 notwendige Bedingung, dass $\mathcal{C}_l$ in $\mathbb{Q}$ liegt, bedeutet, dass dieses quadratische Polynom über $\mathbb{Q}$ zerfällt, anders ausgedrückt muss dessen Diskriminante ein Quadrat in $\mathbb{Q}$ sein.

3.2.2 Indikatorfunktionen

Über die in Abschnitt 3.2.1 beschriebenen Indikatorfunktionen berechnet man folgende zugehörige quadratische Polynome:

	Polynom $\mathcal{C}_l^2 + \alpha_l\,\mathcal{C}_l + \beta_l$
$l = 3$	$\alpha_3 = -a_3\,(a_1\,n + 3\,a_3)$ $\beta_3 = {a_3}^2\,({a_1}^3\,a_3 + 6\,a_3\,a_1\,n + 9\,{a_3}^2 - n^3)$
$l = 4$	$\alpha_4 = -b\,(4b - n)$ $\beta_4 = -b^2\,(n^3 - 4b\,n^2 + 6b\,n - b\,(20b - 1))$
$l = 5$	$\alpha_5 = -b\,((b-1)\,n + 5b)$ $\beta_5 = -b^2\,(n^3 - 7b\,n^2 - 6b\,(b^2 - b - 1)\,n - b\,(b^4 - b^3 - 10b^2 + 29b - 1))$
$l = 6$	$\alpha_6 = -c\,(c+1)\,((c-1)\,n + 6c\,(c+1))$ $\beta_6 = -c^2\,(c+1)^2\,(n^3 - c\,(7\,c + 10)\,n^2 + 6\,c\,(c+1)\,(4\,c+1)\,n$ $\quad -c\,(36c - 1)\,(c+1)^2)$

	Polynom $\mathcal{C}_l^2 + \alpha_l \mathcal{C}_l + \beta_l$
$l = 7$	$\alpha_7 = -(d-1)\,d^2\,((d^2-d-1)\,n + 7d^2\,(d-1))$ $\beta_7 = -d^4\,(d-1)^2\,(\,n^3 - d\,(7d+6)\,(d-1)\,n^2 -$ $6d\,(d-1)\,(d^5 - 2d^4 - 7d^3 + 9d^2 - 3d + 1)\,n -$ $d\,(d-1)\,(d^9 - 2d^8 - 34d^7 + 153d^6 - 229d^5 + 199d^4 -$ $111d^3 + 28d^2 - 7d + 1)\,)$
$l = 8$	$\alpha_8 = -d^2\,(d-1)\,(2d-1)\,(\,2n^2 - (d-1)\,(8d^3 + 22d^2 - 14d + 1)\,n +$ $4\,d\,(d-1)\,(2d-1)\,(8d^4 - 2d^3 - 10d^2 + 6d - 1)\,)$ $\beta_8 = d^4\,(d-1)^2\,(2d-1)^2\,(\,n^4 - d\,(d-1)\,(12d^2 + 14d - 9)\,n^3 +$ $d\,(d-1)\,(80d^6 - 24d^5 + 9d^4 - 183d^3 + 161d^2 - 41d + 2)\,n^2 -$ $2\,d\,(2d-1)\,(d-1)^2\,(320d^7 - 672d^6 + 756d^5 - 616d^4 +$ $274d^3 - 40d^2 - 7d + 2)\,n + d\,(d-1)^2\,(2\,d-1)^2 \cdot$ $(1280d^9 - 4736d^8 + 8080d^7 - 8416d^6 + 5664d^5 - 2368d^4 +$ $552d^3 - 48d^2 - 5d + 1)\,)$

Die Diskriminanten dieser Polynome in $\mathcal{C}_l$ enthalten jeweils quadratische Faktoren. Sollen diese Diskriminanten insgesamt ein Quadrat in $\mathbb{Q}$ sein, so ist jeweils ein Polynom vom Grad 3 in n zu untersuchen. Da jedes dieser Polynome keine mehrfachen Nullstellen besitzt, werden rationale Punkte auf elliptischen Kurven $z^2 = 4n^3 + (\ldots)n^2 + (\ldots)n + (\ldots)$ gesucht. Konkret geht es um die folgenden Kurvenscharen:

	zu untersuchende elliptische Kurvenschar
$l = 3$	$z^2 = 4\,n^3 + {a_1}^2\,n^2 - 18\,a_1\,a_3\,n - a_3\,(27\,a_3 + 4\,{a_1}^3)$
$l = 4$	$z^2 = 4\,n^3 - (16b-1)\,n^2 + 16b\,n - 4b\,(16b-1)$
$l = 5$	$z^2 = 4\,n^3 + (b^2 - 30b + 1)\,n^2 - 2b\,(3b+1)\,(4b-7)\,n -$ $b\,(4b^4 - 4b^3 - 40b^2 + 91b - 4)$
$l = 6$	$z^2 = 4\,n^3 - (27c^2 + 42c - 1)\,n^2 + 12c\,(c+1)\,(9c+1)\,n -$ $4c\,(27c-1)\,(c+1)^2$
$l = 7$	$z^2 = 4\,n^3 + (d^4 - 30d^3 + 3d^2 + 26d + 1)\,n^2 -$ $2d\,(d-1)\,(12d^5 - 24d^4 - 91d^3 + 115d^2 - 29d + 12)\,n -$ $d\,(d-1)\,(4d^9 - 8d^8 - 136d^7 + 612d^6 - 916d^5 + 747d^4 -$ $395d^3 + 112d^2 - 28d + 4)$
$l = 8$	$z^2 = 4\,n^3 - (64d^4 - 32d^3 - 64d^2 + 32d - 1)\,n^2 +$ $8d\,(d-1)\,(2d-1)\,(64d^4 - 80d^3 + 8d^2 + 12d - 3)\,n -$ $4\,(64d^4 - 96d^3 + 32d^2 - 1)\,d\,(d-1)\,(2d-1)^4$

Im nächsten Abschnitt wird mit Hilfe von Formeln von Vélu [93] gezeigt, dass es sich bei diesen Kurven um Quotientenkurven $E_l/\langle A \rangle$ handelt, wobei E_l wieder die Kubert-Kurve aus Abschnitt 1.3.1 und $A = (0,0)$ der Torsionspunkt von E_l der Ordnung l ist.

3.2.3 Quotientenkurven nach Vélu

Allgemeine Konstruktion nach Vélu

Sei E eine elliptische Kurve über einem perfekten Körper K. Sei Γ eine endliche Untergruppe von $E(\bar{K})$, die (als Gruppe) invariant ist unter den Automorphismen $Gal(\bar{K}/K)$. Dann gibt es eine elliptische Kurve E^* und eine Isogenie $\varphi : E \to E^*$, die über K definiert ist und deren Kern Γ ist. Das Paar (E^*, φ) ist eindeutig bis auf K-Isomorphie und E^* wird mit E/Γ bezeichnet. (Siehe auch Satz 1.2.3 und die daran anschließende Bemerkung.)

Ist nun E in der (langen) Weierstraß-Form gegeben und sind die Koordinaten aller Punkte aus einer endlichen Untergruppe Γ bekannt, so kann das Paar $(E/\Gamma, \varphi)$ durch folgende Formeln von Vélu (siehe [93]) berechnet werden.

Sei die elliptische Kurve E gegeben durch

$$E \quad : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (a_i \in K).$$

Dann definiert man $g^x, g^y \in K(E)$ durch

$$g^x = 3x^2 + 2a_2x + a_4 - a_1y, \quad g^y = -2y - a_1x - a_3.$$

Zu einem Punkt $R \neq \mathcal{O}$ von E berechnet man weiter

$$t_R = \begin{cases} {g^x}_R & \text{falls } 2R = \mathcal{O}, \\ 2{g^x}_R - a_1{g^y}_R & \text{sonst}, \end{cases}$$

$$u_R = ({g^y}_R)^2.$$

Sei S ein Repräsentantensystem von $(\Gamma - \mathcal{O})/\pm 1$. Setze

$$t = \sum_{R \in S} t_R, \qquad w = \sum_{R \in S} (u_R + x_R t_R).$$

Diese beiden Ausdrücke t und w liegen in K und sind nicht abhängig von der Wahl der Repräsentanten in S. Seien weiter

$$A_1 = a_1, A_3 = a_3, A_2 = a_2, A_4 = a_4 - 5t, A_6 = a_6 - (a_1^2 + 4a_2)t - 7w,$$

dann gilt:

$$E/\Gamma \ : \ Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,$$

und $\varphi \ : \ E \to E/\Gamma$ ist gegeben durch

$$X = x + \sum_{R \in S} \left(\frac{t_R}{x - x_R} + \frac{u_R}{(x - x_R)^2} \right),$$
$$Y = y - \sum_{R \in S} \left(u_R \frac{2y + a_1x + a_3}{(x - x_R)^3} + t_R \frac{a_1(x - x_R) + y - y_R}{(x - x_R)^2} + \frac{a_1u_R - {g^x}_R \, {g^y}_R}{(x - x_R)^2} \right).$$

Berechnung der Quotientenkurven

Mit den Formeln von Vélu lassen sich Gleichungen der Quotientenkurven $E_l/\langle A \rangle$ berechnen, wobei stets $A = (0, 0)$ gilt. (Für Details der Berechnung siehe Anhang A.)

In der folgenden Tabelle finden sich entsprechende Gleichungen von $E_l/\langle A \rangle$ in Weierstraßform $Y^2 = f_l(X)$ für $3 \leq l \leq 8$. Die Fälle $l = 9, 10, 12$ finden sich in Anhang B.

l	$f_l(X)$
3	$4\,X^3 + a_1^2\,X^2 - 18\,a_1\,a_3\,X - a_3\,(27\,a_3 + 4\,a_1^3)$
4	$4\,X^3 - (4\,b - 1)\,X^2 - 2\,b\,(10\,b - 9)\,X - b\,(b + 4)\,(12\,b - 1)$
5	$4\,X^3 + (b^2 - 6\,b + 1)\,X^2 - 2\,b\,(10\,b^2 + 19\,b - 9)\,X -$ $b\,(4\,b^4 + 40\,b^3 - 20\,b^2 + 59\,b - 4)$
6	$4\,X^3 - (3\,c^2 + 6\,c - 1)\,X^2 - 2\,c\,(30\,c^3 + 39\,c^2 + 10\,c - 9)\,X -$ $c\,(4\,c^3 + 4\,c^2 + c + 4)\,(19\,c^2 + 14\,c - 1)$

l	$f_l(X)$
7	$4\,X^3 + (d^4 - 6\,d^3 + 3\,d^2 + 2\,d + 1)\,X^2 -$ $2\,d\,(d-1)\,(10\,d^5 + 10\,d^4 - 61\,d^3 + 81\,d^2 - 59\,d + 10)\,X -$ $d\,(d-1)\,(4\,d^9 + 36\,d^8 - 148\,d^7 + 280\,d^6 - 528\,d^5 + 843\,d^4 -$ $727\,d^3 + 304\,d^2 - 72\,d + 4)$
8	$4\,X^3 - (4\,d^4 + 4\,d^3 - 16\,d^2 + 8\,d - 1)\,X^2 -$ $2d\,(d-1)\,(170d^6 - 514d^5 + 600d^4 - 336d^3 + 51d^2 + 30d - 10)\,X -$ $d\,(d-1)\,(44\,d^4 - 84\,d^3 + 48\,d^2 - 8\,d - 1)\cdot$ $(25\,d^6 - 85\,d^5 + 116\,d^4 - 80\,d^3 + 44\,d^2 - 20\,d + 4)$

Diese Kurven sind isomorph zu den Kurven, die mittels der Indikatorfunktion bestimmt wurden. Geeignete Transformationen finden sich in Anhang A.

3.2.4 Punkte auf Quotientenkurven

Allgemeine Konstruktion

Wie in den vorangegangenen Abschnitten deutlich wurde, ist die Frage, bei welcher Parameterwahl (n, c)[17] die Polynomfamilie $F_l(x)$ die Galoisgruppe C_l besitzt, äquivalent dazu, dass rationale Punkte auf bestimmten elliptischen Kurven gefunden werden, und zwar den Quotientenkurven

$$E_l/\langle A \rangle \quad : \quad z^2 \;=\; 4\,n^3 + (\ldots)\,n^2 + (\ldots)\,n + (\ldots).$$

Laut Abschnitt 3.2.3 ist nicht nur die Kurve $E_l/\langle A \rangle$ bekannt, sondern auch die Isogenie φ, so dass sich kanonisch folgende exakte Sequenz ergibt:

$$\mathcal{O} \quad \longrightarrow \quad \langle A \rangle \quad \longrightarrow \quad E_l \quad \xrightarrow{\varphi} \quad E_l/\langle A \rangle \quad \longrightarrow \quad \mathcal{O}.$$

Somit ist es leicht möglich, rationale Punkte auf der Quotientenkurve anzugeben, wenn man rationale Punkte auf E_l kennt, da φ explizit gegeben ist.

Rationale Punkte, die von E_l kommen, führen jedoch zur vollständigen Zerlegung von $F_l(x)$. (Siehe dazu Bemerkung 3.1.4.) Es müssen also rationale Punkte auf $E_l/\langle A \rangle$ gefunden werden, die *nicht* von rationalen Punkten von

[17] c steht hier wieder stellvertretend für die verschiedenen auftretenden Parameter (a_1, a_3), b, c, d.

E_l kommen. Deren Existenz wird im folgenden Abschnitt für $l \in \{3,4,5,6\}$ konstruktiv gezeigt. Diese Punkte besitzen im Allgemeinen unendliche Ordnung.

Die oben angegebene exakte Sequenz führt unmittelbar nach Silverman (siehe [86], B.2.3) zu einer langen exakten Sequenz von Kohomologiegruppen: mit der Bezeichnung $G := Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ gilt

$$\begin{aligned} \mathcal{O} \quad &\longrightarrow \quad H^0(G,\langle A\rangle) \quad \longrightarrow \quad H^0(G,E_l) \quad \longrightarrow \quad H^0(G,E_l/\langle A\rangle) \\ &\xrightarrow{\delta} \quad H^1(G,\langle A\rangle) \quad \longrightarrow \quad H^1(G,E_l) \quad \longrightarrow \quad H^1(G,E_l/\langle A\rangle). \end{aligned}$$

(Die Beschreibung des Homomorphismus δ findet sich ebenfalls bei Silverman [86], B.2.3.)

Da $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ trivial auf $\langle A\rangle$ operiert, folgt (siehe Silverman [86], B.2.2), dass $H^0(G,\langle A\rangle) = \langle A\rangle$ und $H^1(G,\langle A\rangle) = \mathrm{Hom}(G,\langle A\rangle)$ gilt. Nach Definition ist $H^0(G,E_l) = E_l(\mathbb{Q})$ und $H^0(G,E_l/\langle A\rangle) = E_l/\langle A\rangle(\mathbb{Q})$. Somit lautet dieser Teil der exakten Sequenz:

$$\ldots \longrightarrow \quad E_l(\mathbb{Q}) \quad \xrightarrow{\varphi} \quad E_l/\langle A\rangle(\mathbb{Q}) \quad \xrightarrow{\delta} \quad \mathrm{Hom}(G,\langle A\rangle) \quad \xrightarrow{\psi} \ldots \quad .$$

Hieraus lassen sich einige äquivalente Aussagen folgern: Die Ungleichung $\mathrm{Ker}\,\psi \neq \{0\}$ ist äquivalent dazu, dass δ nicht die 0-Abbildung ist, also dass

$$\mathrm{Ker}\,\delta \neq E_l/\langle A\rangle(\mathbb{Q})$$

gilt. Auf Grund der Exaktheit ist $\mathrm{Ker}\,\delta = \mathrm{Im}\,\varphi$, womit die Äquivalenz zur Nicht-Surjektivität von φ folgt, was bedeutet, dass es rationale Punkte auf $E_l/\langle A\rangle(\mathbb{Q})$ gibt, die nicht von $E_l(\mathbb{Q})$ kommen.[18] Da letzteres gilt, ist $\mathrm{Ker}\,\psi \neq \{0\}$, so dass insbesondere $\mathrm{Hom}\,(G,\langle A\rangle)$ nicht nur die 0 enthält.

Die Idee, wie man entsprechende rationale Punkte von $E_l/\langle A\rangle$ – möglichst in parametrisierter Form – erhält, basiert auf der spezifischen Form der Punkte in $\varphi(E_l)$: Deren Koordinaten (n,z) sind rationale Ausdrücke, deren Zähler und Nenner Polynome in (den Kurvenparametern) c sind. Dabei sind die auftretenden Nenner im Allgemeinen nicht 1. Nimmt man diese nun aber als 1 an und setzt $n = \ Polynom(c)$ und findet (parametrisierte) Punkte auf $E_l/\langle\, A\,\rangle$, so ist es sehr wahrscheinlich, dass diese nicht in $\varphi(E_l)$ liegen.

[18] Diese Kette von Äquivalenzen kann weitergeführt werden: Die Existenz von rationalen Punkten auf $E_l/\langle A\rangle(\mathbb{Q})$, die nicht von $E_l(\mathbb{Q})$ mittels φ kommen, ist äquivalent dazu, dass die zu $E_l/\mathbb{Q}$ und φ gehörende Selmergruppe $S^{(\varphi)}(E_l/\mathbb{Q})$ nicht isomorph zum Kern $Ш(E_l/\mathbb{Q})[\varphi]$ von φ bzgl. der zugehörigen Tate-Shafarevich-Gruppe ist. (Vgl. Silverman [86], X.4.2.)

Die Konstruktion basiert also darauf, dass die Kurvenkoordinate n durch ein Polynom in c ersetzt wird. Sofern der Grad dieses Polynoms größer 1 ist, wird das Problem scheinbar schwieriger, denn in der Quotientenkurve $z^2 = 4n^3 + (\ldots)n^2 + \ldots$ wird der Grad in c der rechten Seite deutlich erhöht. Ergibt sich damit jedoch eine Form

$$z^2 \;=\; A(c)\,G^2(c),$$

bei der $A(c)$ und $G(c)$ Polynome in c sind und der Grad von $A(c)$ entweder 0, 1 oder 2 ist, so ist die weitere Parametrisierung einfach. Um diese Gestalt zu erreichen, berechnet man die Diskriminante der rechten Seite bezüglich c und setzt diese gleich 0, was einen quadratischen Faktor $G^2(c)$ garantiert.

Mit diesem Verfahren können relativ einfach parametrisierte Punkte auf elliptischen Kurven (hier Quotientenkurven) gefunden werden. Es bleibt jedoch die Frage, ob $F_l(x)$ über $\mathbb{Q}$ zerfällt.

Konstruktion von Polynomfamilien mit Galoisgruppe C_l

Die im vorangegangenen Abschnitt ausgeführte Methode führt bei den vier Fällen $l = 3, 4, 5, 6$ zu parametrisierten Zahlkörperfamilien mit Galoisgruppe C_l. Die Polynome $F_l(x)$, von denen ausgegangen wird, wurden in Abschnitt 3.1.2 konstruiert. Für die Berechnungen wurde MAPLE ([53]) benutzt.

1. Fall: $l = 3$

In diesem Fall werden parametrisierte Punkte auf

$$z^2 = f_3(n) := 4\,n^3 + {a_1}^2\,n^2 - 18\,a_1\,a_3\,n - a_3\,(27\,a_3 + 4\,{a_1}^3)$$

gesucht. Wie im vorangegangenen Abschnitt beschrieben, wird versucht, die rechte Seite als ein $f_3 = A(a_1, a_3)\cdot G^2(a_1, a_3)$ zu schreiben, wobei der Faktor A Grad 0, 1 oder 2 in a_1 oder in a_3 hat. Um zu dieser Gestalt zu kommen, ersetzt man n durch $va_1 + wa_3 + u$, was aber im Folgenden in fünf Fälle auf Grund der dann übersichtlicheren Rechnung aufgeteilt wird. Es werden außerdem nur die Fälle angesprochen, die zu einem positiven Ergebnis führen. (Die systematische Suche ergab zahlreiche Male auch keine Lösung, was entweder daran lag, dass das betrachtete Polynom $F_l(x)$ nicht mehr irreduzibel blieb oder ein Ausdruck zu komplex war.)

Fall 1.1: $n = u$

Diskriminantenbildung von $f_3(u)$ nach u ergibt $16a_3(a_1^3 - 27a_3)^3$, welche für $a_3 = \frac{a_1^3}{27}$ Null wird. f_3 wird für $n = \frac{3t^2+5a_1^2}{12}$ ein Quadrat. Damit erhält man die Polynomfamilie $x^3 - \left(\frac{1}{4}t^2 + \frac{5}{12}a_1^2\right)x^2 + \frac{1}{27}a_1^4 x + \frac{1}{729}a_1^6$, welche sich in

$$G_{3,1}(x) = x^3 - k\,x^2 - 9\,x + k$$

transformieren läßt. Es gilt $\mathrm{disc}(G_{3,1}(x)) = 4\,(k^2+27)^2$.

Fall 1.2: $n = a_1 + u$

Diskriminantenbildung von $f_3(a_1 + u)$ nach dem Parameter a_1 ergibt den Ausdruck $-256\,a_3\,(1 + a_3 - u)\,(27\,a_3^2 - 27\,(u-1)\,a_3 + u^3)^3$, der zum Beispiel für $a_3 = 1$ und $u = 3$ Null wird. Mit dieser Wahl wird f_3 ein Quadrat und man erhält die Familie von Shanks (siehe [85])

$$G_{3,2} = x^3 - k\,x^2 - 3\,x^2 + k\,x + 1$$

mit Diskriminante $(k^2 + 3\,k + 9)^2$.

Die Diskriminante von f_3 wird auch Null bei Paaren (a_3, u) aus der Menge $\{(-64,-36),(-27,-18),(-8,-6),(-1,0),(0,0),(1,-6),(8,-18),(27,-36),(64,-60)\}$. Alle Paare liefern unterschiedliche Familien. Beispielhaft seien drei Paare herausgegriffen:
Das Paar $(1,-6)$ führt mit $a_1 = -\frac{12\,(t+2)}{t^2-1} - 9$ dazu, dass f_3 ein Quadrat wird. Man erhält nach Transformation die Polynomfamilie

$$G_{3,3} = x^3 + 3\,(5\,t^2+4\,t+3)\,x^2 + -3\,(t-1)\,(t+1)\,(3\,t^2+4\,t+5)\,x + (t-1)^3\,(t+1)^3$$

mit Diskriminante $5184\,(t-1)^2\,(t+1)^2\,(t^2+4\,t+1)^2\,(t^2+t+1)^2$.
Für $(8,-18)$ wird f_3 mit $a_1 = -\frac{28\,(3\,t+4)}{t^2-1} - 30$ ein Quadrat; mit Transformation ergibt sich

$$G_{3,4} = x^3 + (12\,t^2+21\,t+16)\,x^2 - (t-1)\,(t+1)\,(15\,t^2+42\,t+41)\,x + (t-1)^3\,(t+1)^3$$

mit $\mathrm{disc}(G_{3,4}(x)) = 49\,(t-1)^2\,(t+1)^2\,(9\,t^2+21\,t+19)^2\,(3\,t^2+8\,t+3)^2$.
Bei $(-64,-36)$ wird f_3 mit $a_1 = -\frac{52\,(6\,t-7)}{t^2-1} - 100$ ein Quadrat und Transformation führt zur Polynomfamilie

$$\begin{aligned} G_{3,5} \;=\; & x^3 - (16\,t^2 - 78\,t + 75)\,x^2 - \\ & 16\,(t-1)\,(t+1)\,(25\,t^2 - 78\,t + 66)\,x + 64\,(t-1)^3\,(t+1)^3, \end{aligned}$$

deren Diskriminante $43264\,(t-1)^2\,(t+1)^2\,(3\,t^2 - 7\,t + 3)^2\,(28\,t^2 - 78\,t + 63)^2$ lautet.

Fall 1.3: $n = a_3 + u$

In diesem Fall führt die Diskriminantenberechnung von $f_3(a_3 + u)$ nach a_3 zu $16\,(a_1+1-u)\,(a_1^3+9\,a_1^2+27\,u)^3$. Diese wird Null für $u = -4$ und $a_1 = 3$, und f_3 wird mit $a_3 = t^2 + 28$ ein Quadrat. Nach Transformation erhält man die Polynomfamilie

$$G_{3,6} = x^3 + (-t^2+18)\,x^2 - 25\,t^2\,x + t^2\,(t^2-98)$$

mit Diskriminante $4\,t^2\,(t^2+28)^2\,(t^2+27)^2$.

Fall 1.4: $n = wa_3 + u$ [19]

Diskriminantenbildung von $f_3(n)$ nach a_3 führt zu $-16\,(v^2\,u - v\,a_1 - 1)\,(v\,a_1^3 + 9\,a_1^2 + 27\,u)^3$, was für $u = -\frac{1}{27}\,v\,a_1^3 - \frac{1}{3}\,a_1^2$ Null wird. Mit $a_3 = \frac{1}{108\,v^3}\,(486\,v\,a_1 + 81\,a_1^2\,v^2 + 729 + 4\,a_1^3\,v^3 + 3\,t^2)$ wird f_3 ein Quadrat. Insgesamt führt dies nach Transformation zur Familie

$$G_{3,7} = x^3 + (1-t)\,x^2 + (-t-2\,t^2)\,x + t^3$$

mit Diskriminante $t^2\,(1+t+7\,t^2)^2$.

In diesem Fall wird die Diskriminante auch bei $v = -\frac{9(a_1^2+3\,u)}{a_1^3}$ Null und mit $a_3 = \frac{(4\,u^3\,a_1^4 + a_1^6\,u^2 - t^2)}{4\,(27\,a_1^2\,u^2 + 27\,u^3 + a_1^6 + 9\,a_1^4\,u)\,a_1}$ wird f_3 ebenfalls zum Quadrat. Hiermit berechnet man nach Transformation die Familie

$$\begin{aligned} G_{3,8} \;=\;& x^3 - 2\,(a_1+3\,t)\,x^2 + (a_1^2\,(1-t^2) + 8\,t\,a_1 - 3\,(5\,t^2+3))\,x + \\ & 8\,a_1\,(1-t^2) - 8\,t\,(t^2-9), \end{aligned}$$

und es gilt $\mathrm{disc}(G_{3,8}(x)) = 4\,(27+a_1^2)^2\,(a_1\,t^3 - 9\,t^2 - t\,a_1 + 1)^2$.

Fall 1.5: $n = va_1 + wa_3 + u$

Die Diskriminante von f_3 nach a_3 lautet $-16\,(w^2\,a_1\,v - w\,a_1 + u\,w^2 - 1)\,(27\,v\,a_1 + a_1^3\,w + 9\,a_1^2 + 27\,u)^3$ und wird bei $w = -\frac{9\,(3\,v\,a_1 + a_1^2 + 3\,u)}{a_1^3}$ Null.

Mit $a_3 = \frac{(2\,v\,a_1^7\,u + 4\,u^3\,a_1^4 + 12\,v\,a_1^5\,u^2 + 12\,v^2\,a_1^6\,u + 4\,v^3\,a_1^7 + v^2\,a_1^8 + a_1^6\,u^2 - t^2)}{4\,a_1\,(3\,v\,a_1 + a_1^2 + 3\,u)^3}$ wird f_3 ein Quadrat und man erhält die Polynomfamilie

$$\begin{aligned} G_{3,9} \;=\;& x^3 - (9\,t^2 + 19\,a_1^2 + 34\,a_1 + 15)\,x^2 + \\ & 4\,(4\,a_1+3)\,(4 + 13\,a_1 + 14\,a_1^2 + 5\,a_1^3 - a_1\,t^2)\,x + \\ & 4\,(4 + 13\,a_1 + 14\,a_1^2 + 5\,a_1^3 - a_1\,t^2)^2, \end{aligned}$$

[19] Die in LPS1 [48], Seite 404 ausgeführte Variante von parametrisierten Punkten auf $E_3/\langle A \rangle$ bleibt hier unerwähnt, da das Polynom $F_3(x)$ mit diesen Punkten zerfällt.

deren Diskriminante $16\,(81+198\,a_1+121\,a_1^2+27\,t^2)^2\,t^2\,(4+13\,a_1+14\,a_1^2+5\,a_1^3-a_1\,t^2)^2$ lautet.

2. Fall: $l=4$

Im Fall $l=4$[20] werden Punkte auf $z^2=f_4$ gesucht mit

$$\begin{aligned} f_4 &:= 4\,n^3-(16\,b-1)\,n^2+b\,(16\,n-64\,b+4)\\ &= (4\,b+n^2)\,(-16\,b+4\,n+1). \end{aligned}$$

Naheliegend ist es, die Zerlegung von f_4 auszunutzen, um die rechte Seite zu einem Quadrat zu machen. (Siehe LPS1 [48], Seite 406.) Damit können parametrisierbare Punkte auf $E_4/\langle A\rangle$ gefunden werden. Alle gefundenen Punkte (siehe LPS1 [48], Seite 406) haben jedoch zur Folge, dass $F_4(x)$ zerfällt. Die im Fall $l=3$ angewandten Methoden führen aber zum Erfolg.

Fall 2.1: $n=u$

Die Diskriminante von f_4 nach u lautet $-16\,b\,(16\,b+1)^4$ und wird durch $b=-\frac{1}{16}$ Null. f_4 wird mit $u=\frac{1}{2}+t^2$ zu einem vollständigen Quadrat. Die resultierende Polynomfamilie mit zyklischer Galoisgruppe lautet nach Transformation

$$G_{4,1}=x^4-2\,(t^2+2)\,x^3-(t^2-2)\,x^2+4\,x+1$$

mit $\operatorname{disc}(G_{4,1}(x))=16\,t^4\,(t^2+4)^3$.

Fall 2.2: $n=b+u$

Mit $n=b+u$ nimmt die Diskriminante von f_4 nach b den Wert $16\,(u+1)\,(7+16\,u)^4$ an und wird für $u=-\frac{7}{16}$ Null. f_4 wird damit zu $-\frac{3}{1024}\,(16\,b+49)\,(16\,b+1)^2$ und mit $b=-\frac{49}{16}-\frac{1}{48}\,t^2$ ein Quadrat. Mit Transformation erhält man insgesamt die Polynomfamilie

$$\begin{aligned} G_{4,2} &= x^4+6\,t^2\,x^3+\\ &\quad (36\,t^4+237\,t^2+588)\,x^2+72\,t^2\,(t^2+7)\,x+\\ &\quad 9\,(192\,t^6+2100\,t^4+7693\,t^2+9604), \end{aligned}$$

die zyklische Galoisgruppe und Diskriminante $11664\,t^4\,(t^2+4)^3\,(12\,t^2+49)^6$ besitzt.

[20] Die Berechnungen in LPS1 [48], Seite 406 beruhen auf der Gleichung der Quotientenkurve $E_4/\langle A\rangle\ :\ y^2=(x+c)(4x^2+x+c)$, welche nicht reproduziert werden konnte.

Fall 2.3: $n = v\,b + u$

Auch mit $n = v\,b + u$ erhält man nach Diskriminantenbildung (nach b) mit $v = 8 + 16\,u$ und mit $b = \frac{t^2 - u^2\,(4\,u+1)}{4\,(4\,u^2+4\,u+1)\,(4\,u+1)}$ eine Familie mit Galoisgruppe C_4, die nach Transformation die Form

$$\begin{aligned} G_{4,3} \;=\; & x^4 - 4\,u\,(u\,t^2 - t^2 - 1 + 2\,u)\,x^3 - \\ & 2\,u\,(2\,u - t^2 - 1)\,(-2\,u^2 + t^2\,u^2 - u + 1 - 2\,u\,t^2 + t^2)\,x^2 + \\ & 4\,u^2\,(2\,u - 1)\,(u - 1)\,(2\,u - t^2 - 1)^2\,x + \\ & u^2\,(2\,u - 1)\,(u - 1)^2\,(2\,u - t^2 - 1)^3 \end{aligned}$$

mit

$$\mathrm{disc}(G_{4,3}(x)) = 256\,(t^2+1-2\,u\,t^2-4\,u+t^2\,u^2+4\,u^2)^3\,u^6\,t^4\,(2\,u-1)^2\,(u-1)^4\,(2\,u-1-t^2)^6$$

besitzt.

Fall 2.4:

Durch geschickte Transformation und Spezialisierung von n und b durch rationale Ausdrücke in u (siehe LPS1 [48], S. 408–409) erhält man von $F_4(x)$ ausgehend auch die Familie von Gras (siehe [23]):

$$G_{4,4} = x^4 - u\,x^3 - 6\,x^2 + u\,x + 1.$$

3. Fall: $l = 5$

$F_5(x) = x^5 - n\,x^4 + b\,(2\,n + b^2 - b - 1)\,x^3 - b^2\,(n + b - 3)\,x^2 + b^3\,(b - 3)\,x + b^4$ besitzt die Galoisgruppe C_5, falls es (parametrisierte) Punkte auf $z^2 = f_5$ gibt, wobei

$$f_5 := 4\,n^3 + (b^2 - 30\,b + 1)\,n^2 - 2\,b\,(3\,b + 1)\,(4\,b - 7)\,n - b\,(4\,b^4 - 4\,b^3 - 40\,b^2 + 91\,b - 4)$$

ist.

Fall 3.1: $n = v\,b + u$

Setzt man $n = v\,b + u$, so berechnet sich die Diskriminante von $f_5(n)$ nach b zu $256\,(u\,v^5 + (1 - 11\,u)\,v^4 + (29\,u - u^2 - 10)\,v^3 + (12\,u + 39\,u^2 + 20)\,v^2 + (-12\,u^2 + 25 + 75\,u)\,v + 67 - 72\,u - 27\,u^3 + 55\,u^2)\,(v^2 + (-11\,u - 5)\,v - u^2 - 35\,u - 25)^5$.

Sie wird Null für $u = -1$ und $v = -3$ und f_5 wird durch $b = -\frac{3}{4} - \frac{1}{4}\,t^2$ ein vollständiges Quadrat. Nach Transformation erhält man aus $F_5(x)$ die

Polynomfamilie

$$x^5+(t^2+15)\,x^4-8\,(t^2-5)\,x^3-(t^4+34\,t^2+45)\,x^2-64\,(3\,t^2+5)\,x+256\,(t^2+3),$$

deren Galoisgruppe zyklisch ist. [21]

Fall 3.2: $n = b^2 + v\,b + u$

Nimmt man $n = b^2 + v\,b + u$, so erhält man die Diskriminante von f_5 nach b in der Form[22] $-4096\cdot(\ldots)\cdot(v^2+(-11\,u+6)\,v-u^2-158\,u-116)^5$, welche für $(u, v) = (-2, -14)$ Null wird. Damit wird f_5 zu $(5\,b^2-144\,b-28)\,(b^2-11\,b-1)^2$ und wird offensichtlich ein vollständiges Quadrat für $b = -22\,(k+7)/(k^2-5)$. Die resultierende Polynomfamilie mit zyklischer Galoisgruppe lautet damit:

$$\begin{aligned}&x^5+(4\,k^2+22\,k+134)x^4-(9\,k^4+330\,k^3+2704\,k^2+5126\,k+12391)x^3-\\&(k^2-5)\,(27\,k^4+770\,k^3+6572\,k^2+16478\,k+44873)\,x^2-\\&(13\,k^4+352\,k^3+2818\,k^2+5016\,k+11721)\,(k^2-5)^2\,x+\\&(k^2+22\,k+149)\,(k^2-5)^4.\end{aligned}$$

Fall 3.3: $n = w\,b^2 + v\,b + u$

Nutzt man die allgemeinere Form $n = w\,b^2 + v\,b + u$, so ergibt sich die Diskriminante von F_5 nach b zu[23]

$$-4096\cdot(\ldots)\cdot\left(v^2+(11w-5-11u)\,v-u(u+123w+35)-w(w+90)-25\right)^5$$

und wird Null bei $(v, w) = (8+11\,u, -1-u)$. Damit wird f_5 zu $(b^2-11\,b-1)^2\cdot(-(4\,u+3)\,(1+u)^2\,b^2+2\,(2\,u+1)\,(11\,u^2+11\,u+2)\,b+u^2\,(4\,u+1))$. Es gibt nun zwei verschiedene Möglichkeiten, f_5 zu einem Quadrat zu machen: Entweder man eliminiert den Koeffizient vor b^2, erhält einen linearen Ausdruck in b, der einfach zu parametrisieren ist, oder man versucht, f_5 insgesamt zu parametrisieren.
Wählt man bei der ersten Variante zum Eliminieren des Koeffizienten von b^2 den Parameter $u = -1$, so erhält man die erste der obigen Familien. Wählt man $u = -\frac{3}{4}$, so wird f_5 mit $b = 2\,(9+8\,t^2)$ ein Quadrat und die resultierende

[21] Dies ist die erste der drei Familien in LPS1 [48], Seite 404. Dort ist jedoch ein Tippfehler, die Ausführungen hier sind exakt.

[22] Die drei Punkte $(\ldots)$ stehen für ein Polynom vom Grad 6 in v und vom Grad 4 in u.

[23] Die drei Punkte $(\ldots)$ stehen hier für ein Polynom vom Grad 6 in v und vom Grad 4 in u und w.

Polynomfamilie

$$x^5 + (2\,t^2 + 30)\,x^4 + (t^4 + 33\,t^2 + 285)\,x^3 + 4\,(t^4 + 33\,t^2 + 265)\,x^2 + 4\,(t^4 + 37\,t^2 + 345)\,x + 32\,(t^2 + 18)$$

besitzt die Galoisgruppe C_5.[24]
Bei der zweiten Variante wird der konstante Term von f_5 ein Quadrat, wenn $u = \frac{t^2-1}{4}$ gesetzt wird. Damit erfüllt der Punkt $(b, z) = (0, u\,t)$ die Gleichung $z^2 = -(4\,u+3)\,(1+u)^2\,b^2 + 2\,(2\,u+1)\,(11\,u^2+11\,u+2)\,b + u^2\,(4\,u+1)$. Eine Parametrisierung findet man dann durch $z = k \cdot b + t\,u$, denn

$$\begin{aligned} z^2 &= (k\,b)^2 + 2\,k\,b\,t\,u + (t\,u)^2 \\ &= -(4\,u+3)\,(1+u)^2\,b^2 + 2\,(2\,u+1)\,(11\,u^2+11\,u+2)\,b + u^2\,(4\,u+1) \end{aligned}$$

führt nach Vereinfachen unter der Annahme $b \neq 0$ zu der in b linearen Gleichung $k^2\,b + 2\,k\,t\,u = -(4\,u+3)\,(1+u)^2\,b + 2\,(2\,u+1)\,(11\,u^2+11\,u+2)$, welche sich wie oben leicht nach $b = \frac{11\,t^6+33\,t^4-8\,k\,t^3+21\,t^2+8\,k\,t-1}{t^6+8\,t^4+21\,t^2+18+16\,k^2}$ auflösen lässt. Mit Parametrisierung von u und b wie angegeben erhält man auch in diesem Fall eine Polynomfamilie mit Galoisgruppe C_5. [25]

4. Fall: $l = 6$

Im Fall $l = 6$ setzt man

$$\begin{aligned} f_6 \;:=\; & 4n^3 - (27c^2+42c-1)n^2 + 12c(c+1)(9c+1)n - 4c(27c-1)(c+1)^2 \\ & (4\,n - (c+1)\,(27\,c-1))\,(n^2 - 4\,c\,n + 4\,c\,(c+1)). \end{aligned}$$

Somit werden parametrisierte Punkte auf $z^2 = f_6$ gesucht. Analog zum Fall $l = 4$ erhält man durch Ausnutzen der Produktdarstellung von f_6 parametrisierte Punkte, die auch hier wieder dazu führen, dass das betrachtete Polynom

$$\begin{aligned} F_6(x) \;=\; & x^6 - n\,x^5 + \\ & c\,((2c+3)n - (c+1)(4c+1))x^4 - \\ & c^2(c+1)((c+3)n - 2(c+2)(c+1))x^3 + \\ & c^3(c+1)^2(n - 2(c+3))\,x^2 + \\ & c^4(c+1)^3\,4\,x - c^5(c+1)^4 \end{aligned}$$

[24] Dies ist die zweite der Familien in LPS1 [48], Seite 404.
[25] Dies ist die dritte Familie aus LPS1 [48], Seite 404.

zerfällt. [26]

Fall 4.1: $n = n$

Berechnet man ohne Substitution von n die Diskriminante von f_6 nach n, so erhält man $-16c(c+1)^2(9c+1)^6$, welche für $c = -\frac{1}{9}$ Null wird. Mit $n = \frac{4}{9}+\frac{1}{9}\,t^2$ wird f_6 zu einem Quadrat und man erhält aus $F_6(x)$ die Polynomfamilie

$$x^6 - 6\,x^5 - 3\,(3\,t^2-1)\,x^4 + 10\,(3\,t^2+2)\,x^3 - 3\,(3\,t^2-1)\,x^2 - 6\,x + 1,$$

die C_6 als Galoisgruppe besitzt.

Fall 4.2: $n = v\,c + u$

Eine weitere Polynomfamilie mit zyklischer Galoisgruppe erhält man durch Wahl von $n = v\,c + u$. Die Diskriminante von $f_6(n)$ nach c lautet $256\,(v^2 - 13\,v + 27\,u + 49)\,(u\,v - 2\,u + 1)\,(v - 9\,u - 8)^6\,(v-u)^2$. Diese wird Null durch $v = 9\,u + 8$. Mit $u = -\frac{2}{3}$ und $c = -\frac{5}{9} - \frac{3}{4}\,t^2$ erhält man (wieder nach Transformation) die Polynomfamilie

$$x^6+2\,(3\,t^2+4)\,x^3+9\,(3\,t^2+4)\,x^2+6\,(3\,t^2+2)(3\,t^2+4)\,x+(3\,t^2+4)(9\,t^4+15\,t^2+8).$$

Eine weniger kompakte Polynomfamilie, deren Galoisgruppe C_6 ist, ergibt sich durch $v = u$ (damit wird die obige Diskriminante Null), und mit $u = \frac{1}{4}\,t^2 - \frac{1}{4}$ und $c = -\frac{t^6-45\,t^4-8\,k\,t^3+135\,t^2+8\,k\,t-27}{27\,t^4-486\,t^2+16\,k^2+2187}$ (damit wird f_6 ein Quadrat).

Bei den weiteren Fällen treten mit dieser Methode bei der Berechnung und Faktorisierung der Diskriminante nach Ersetzen von n durch ein Polynom in c mit MAPLE [53] Speicherprobleme auf.

Zyklische Zahlkörper in den Fällen $l = 7, 8, 9, 10, 12$

Bei diesen Fällen gibt es eine weitere Möglichkeit, eine Familie von Polynomen zu erzeugen, deren Galoisgruppe die zyklische Gruppe der Ordnung l ist:

Da die Suche *parametrisierter* rationaler Punkte auf $E_l/\langle A\rangle \setminus \varphi(E_l)$ nicht zum Erfolg führt, erhält man eine gesuchte Polynomfamilie durch die Bestimmung *einer* Kurve (nach Spezifizierung des Parameters d), deren Rang

[26] Entsprechende Punkte werden in LPS1 [48], Seite 405 hergeleitet. Dort wird jedoch die Kurve in der unmittelbar aus den Vélu-Formeln folgenden Form untersucht und nicht die hier verwendete Form, die aus der Indikatorfunktion folgt.

größer 0 ist. Betrachtet man einen Punkt $P = (n, z)$ unendlicher Ordnung auf der gewählten Kurve, so liefern die unendlich vielen Punkte $2P, 3P, 4P, \ldots$ unendlich viele n-Koordinaten $n(P), n(2P), n(3P) \ldots$, die jeweils zusammen mit dem gewählten d ein Polynom $F_l(x) \in \mathbb{Q}[x]$ ergeben, welches einen zyklischen Zahlkörper erzeugt (sofern $F_l(x)$ irreduzibel bleibt).

Im Fall $l = 7$ besitzt die zu untersuchende Kurve den Rang 1 z. B. für $d \in \{\frac{2}{7}, \frac{4}{7}, \frac{1}{8}, \frac{5}{8}, \frac{7}{8}, \frac{7}{9}, \frac{11}{12}\}$. Eine Parameteränderung $\vartheta : d \mapsto -\frac{1}{d-1}$ liefert eine isomorphe Kurve mit Isomorphismus[27] $n \mapsto n + 28\,d\,(d-1)$. Jedes genannte d führt durch die Abbildung ϑ zu zwei weiteren Werten $\vartheta(d)$ und $\vartheta^2(d)$, die dieselbe Kurve (in anderen Gleichungen) ergeben; ein weiterer Wert ergibt sich aus d nicht, da $\vartheta^3 = id$ gilt.[28]

Für $l = 8$ liefert $d \in \{4, 9, 10, 14, 17, 21\}$ Rang 1. Die Parametervariation $d \mapsto -d + 1$ liefert eine isomorphe Kurve, wobei der Isomorphismus durch $n \mapsto n + 32\,d\,(2\,d-1)\,(d-1)$ beschrieben wird.

Für die gefundenen Parameter gilt jedoch, dass $F_l(x)$ zerfällt: $F_7(x)$ in allen untersuchten Fällen in Linearfaktoren, $F_8(x)$ mal in zwei Faktoren vom Grad vier, mal in vier quadratische Faktoren, mal in Linearfaktoren und auch mal in ein Produkt von Faktoren vom Grad 1, 2 und 4; auch für Torsionspunkte der entsprechenden elliptischen Kurven zerfallen die Polynome $F_l(x)$.

3.3 Zahlkörper mit Galoisgruppe $D_{l/2}$

Da die in Abschnitt 3.1.1 konstruierten Polynomfamilien $F_l(x)$ die Galoisgruppe D_l besitzen und diese Gruppe $D_{l/2}$ als transitive Untergruppe besitzt, falls $l \equiv 0 \pmod 2$ ist, so schließt sich wie in Abschnitt 3.2 die Frage nach Unterfamilien an, die diese Galoisgruppe haben.

Analog zu den dort vorgestellten Methoden werden auch hier wieder Indikatorfunktionen genutzt, um Bedingungen für die Konstruktion solcher Familien mit Galoisgruppe $D_{l/2}$ aufzustellen. Die Indikatorfunktionen haben in diesen Fällen eine einfachere Gestalt als in Abschnitt 3.2.1:

[27] Der angegebene Isomorphismus liefert eine nennerfreie Gleichung der Kurve. Die durch die Parameteränderung ϑ entstehenden Nenner werden durch $n \mapsto \frac{n}{(d-1)^4}$ eliminiert, was zur selben nennerfreien Gleichung führt.

[28] Im Fall $l = 7$ wurden nur drei ganzzahlige d gefunden, die zu einem Rang 1 führen: $d = -7, 8, 12$.

Lemma 3.3.1 (Geißler [21], 6.4+6.24). *Sei $F_l(x)$ wie in 3.1.1 konstruiert. Seien $x_i := x(P \oplus iA)$ die Nullstellen von $F_l(x)$ mit $1 \le i \le l$ und $l \equiv 0 \pmod 2$. Dann gilt:*

Das Polynom $F_l(x)$ besitzt die Galoisgruppe $D_{l/2}$ genau dann, wenn der Ausdruck $\mathcal{D}_l := \mathcal{D}_l(x_1, \ldots, x_l)$ in $\mathbb{Q}$ liegt:

$$\mathcal{D}_l := \sum_{i=1}^{l/2} x_{2i-1}\, x_{2i}.$$

Wie in Abschnitt 3.2 erhält man auch hier durch Resultantenbildung normierte quadratische Polynome in $\mathcal{D}_l$ mit Koeffizienten in $\mathbb{Q}(n, c)$.[29]

Sei $\mathcal{D}_l^2 + \alpha_l(n,c)\,\mathcal{D}_l + \beta_l(n,c)$ das quadratische Polynom, das nach Eliminierung von x_P, y_P mit $F_l(x)$ und E_l aus $\mathcal{D}_l$ entsteht. Die nach 3.3.1 notwendige Bedingung, dass $\mathcal{D}_l$ in $\mathbb{Q}$ liegt, bedeutet auch hier, dass dieses quadratische Polynom über $\mathbb{Q}$ zerfällt, anders ausgedrückt: dessen Diskriminante muss ein Quadrat in $\mathbb{Q}$ sein.

Im Unterschied zur Bedingung im zyklischen Fall entstehen bei diesen Betrachtungen keine elliptischen Kurven. Die Bedingungen sind immer linear in n und können damit sehr einfach parametrisiert werden.

Konkrete Konstruktion

Die aus den Indikatorfunktionen entstehenden normierten, quadratischen Polynome in $\mathcal{D}_l$ sind in der folgenden Tabelle zusammengefasst. Da die Rechnungen nicht so umfangreich sind wie in Abschnitt 3.2, sind hier alle Fälle zusammen aufgeführt.

	Polynom $\mathcal{D}_l^2 + \alpha_l\,\mathcal{D}_l + \beta_l$
$l = 4$	$\alpha_4 = b$ $\beta_4 = b^2\,(4\,b - n)$
$l = 6$	$\alpha_6 = -c\,(c+1)\,(3\,c-1)$ $\beta_6 = -c^2\,(c+1)^2\,(n - c\,(9\,c+5))$
$l = 8$	$\alpha_8 = -d^3\,(2\,d-1)\,(d-1)\,(8\,d^2 - 12\,d + 3)$ $\beta_8 = -d^6\,(2\,d-1)^2\,(d-1)^2\,(n - 2\,(4\,d-1)\,(d-1)\,(2\,d-1)^2)$

[29] Der Parameter c steht wieder stellvertretend für die Parameter von E_l.

	Polynom $\mathcal{D}_l^2 + \alpha_l \mathcal{D}_l + \beta_l$
$l = 10$	$\alpha_{10} = d^3 (d-1) (2\,d-1) (d^2 - 3\,d + 1) (8\,d^3 - 6\,d^2 - 6\,d + 3)$ $\beta_{10} = -d^6 (d-1)^2 (2d-1)^2 (d^2 - 3d + 1)^2 \cdot$ $(n - (d-1) (16d^5 + 8d^4 - 29d^3 + 10d^2 + 4d - 2))$
$l = 12$	$\alpha_{12} = d (2d-1) (2d^2 - 2d + 1) (3d^2 - 3d + 1) \cdot$ $(36d^4 - 60d^3 + 36d^2 - 6d - 1) (d-1)^5$ $\beta_{12} = -d^2 (2d-1)^2 (2d^2 - 2d + 1)^2 (3d^2 - 3d + 1)^2 (d-1)^{10} \cdot$ $(n - 2\,d (3d^2 - 3d + 1) (18d^3 - 30d^2 + 19d - 4) (2d-1)^2)$

Die Diskriminanten dieser Polynome in $\mathcal{D}_l$ enthalten jeweils quadratische Faktoren. Sollen diese Diskriminanten insgesamt ein Quadrat in $\mathbb{Q}$ sein, so bleibt jeweils ein Polynom vom Grad 1 in n zu untersuchen:

	nicht quadratischer Teil der Diskriminante
$l = 4$	$4\,n + 1 - 16\,b$
$l = 6$	$4\,n + 1 - c\,(27\,c + 26)$
$l = 8$	$4\,n + 1 - 32\,d^2\,(2\,d-1)\,(d-1)$
$l = 10$	$4\,n + 1 - 4\,d\,(d-1)\,(16\,d^3 - 6\,d^2 + 3\,d - 3)$
$l = 12$	$4\,n + 1 - 4\,d\,(d-1)\,(108d^6 - 396d^5 + 636d^4 - 576d^3 + 308d^2 - 92d + 11)$

1. Fall: $l = 4$

Mit $n = 4\,b + t\,(t+1)$ und anschließend $x = \frac{b}{x}$ erhält man die Polynomfamilie

$$H_4(x) = x^4 - 2\,x^3 + (1 - 4\,b - t^2 - t)\,x^2 + (4\,b + t^2 + t)\,x - b,$$

deren Galoisgruppe die Kleinsche Vierergruppe ist.

Die Diskriminante berechnet sich zu

$$\mathrm{disc}(H_4) = b^6\,(2\,t+1)^2\,(4\,b + (t+1)^2)^2\,(4\,b + t^2)^2.$$

2. Fall: $l = 6$

Mit $n = \frac{27}{4}\,c^2 + \frac{13}{2}\,c + t^2 + t$ und den Vereinfachungen $c = 2\,c$ und $x = \frac{c\,(2\,c+1)}{x}$ erhält man die Polynomfamilie

$$\begin{aligned} H_6(x) &= x^6 - 4\,x^5 - (t\,(t+1) + 3\,(3\,c+2)\,(3\,c-1))\,x^4 + \\ &\quad ((2\,c+3)\,t\,(t+1) + 99\,c^2 + 27\,c + 54\,c^3 - 4)\,x^3 - \\ &\quad ((4\,c+3)\,t\,(t+1) + (108\,c^3 + 117\,c^2 + 29\,c1))\,x^2 + \\ &\quad (2\,c+1)\,(c\,(27\,c+13) + t\,(t+1))\,x - 2\,c\,(2\,c+1)^2 \end{aligned}$$

mit Galoisgruppe $D_{6/2}$, wobei die Diskriminante den Wert

$$\begin{aligned} \mathrm{disc}(H_6) &= 64\,c^6\,(2\,t+1)^4\,(2\,c+1)^2\,\cdot \\ &\quad \left(t^2(t+1)^2 + 18\,c(3c+1)\,t\,(t+1) + c(729c^3 + 486c^2 + 81c + 8)\right)^3 \end{aligned}$$

hat.

3. Fall: $l = 8$

In diesem Fall führt $n = 8\,d^2\,(2\,d-1)\,(d-1)+t\,(t+1)$ und die Transformation $x = \frac{(d-1)\,(2\,d-1)\,d^3}{x}$ zur Polynomfamilie

$$\begin{aligned} H_8(x) &= x^8 - 2\,(4\,d-1)\,x^7 - \left(t\,(t+1) + (16\,d^4 - 32\,d^3 - 6\,d^2 + 8\,d - 1)\right)^6 + \\ &\quad \left((2\,d^2 + 4\,d - 1)\,t\,(t+1) + 4\,d^2\,(8\,d^4 - 26\,d^2 + 15\,d - 2)\right)\,x^5 - \\ &\quad d\,\big((d^3 + 8\,d^2 + 3\,d - 2)\,t\,(t+1) + \\ &\qquad 96\,d^6 - 188\,d^5 + 28\,d^4 + 55\,d^3 + 16\,d^7 - 28\,d^2 + 7\,d - 1\big)\,x^4 + \\ &\quad d^2\,\big((4\,d+1)\,(d^2 + 2\,d - 1)\,t\,(t+1) + 2\,d\,(2\,d-1) \\ &\qquad (16\,d^5 + 12\,d^4 - 54\,d^3 + 30\,d^2 - 9\,d + 2)\big)\,x^3 - \\ &\quad d^4\,\big((5d^2+2d-2)\,t\,(t+1) + (20d^4-12d^3-10d^2+2d-1)\,(2d-1)^2\big)\,x^2 + \\ &\quad d^6\,(2\,d-1)\,\left(t\,(t+1) + 8\,d^2\,(2\,d-1)\,(d-1)\right)\,x - (d-1)\,(2\,d-1)^2\,d^9 \end{aligned}$$

mit Galoisgruppe $D_{8/2}$. Die Diskriminante lautet

$$\begin{aligned} \mathrm{disc}(H_8) &= d^{26}\,(2\,t+1)^6\,(2\,d-1)^4\,(d-1)^{26}\,(t^2 + 4\,d\,(d-1)\,(2\,d-1)^2)^4\,\cdot \\ &\quad ((t+1)^2 + 4\,d\,(d-1)\,(2\,d-1)^2)^4. \end{aligned}$$

4. Fall: $l = 10$

Mit $n = t\,(t+1) + d\,(d-1)\,(16\,d^3 - 6\,d^2 + 3\,d - 3)$ und der Transformation $x = \frac{d^3\,(d^2-3\,d+1)\,(2\,d-1)\,(d-1)}{x}$ erhält man die Polynomfamilie

$$
\begin{aligned}
H_{10}(x) = {} & x^{10} - 4\,(d+1)\,(d^2-3\,d+1)\,x^9 + \\
& \left(-t\,(t+1) + 4\,d^6 - 36\,d^5 + 26\,d^4 + 49\,d^3 + 6\,d^2 - 27\,d + 6\right) x^8 + \\
& \left((2\,d^3 - 6\,d^2 - 6\,d + 3)\,t\,(t+1) + (2\,d-1)\,(16\,d^7 - 60\,d^6 - 34\,d^5 + 100\,d^4 + 45\,d^3 + 10\,d^2 - 25\,d + 4)\right) x^7 - \\
& \left((d^6 - 6\,d^5 - 7\,d^4 + 54\,d^3 - 14\,d^2 - 10\,d + 3)\,t\,(t+1) + \right. \\
& \quad \left. (16\,d^{11} - 172\,d^{10} + 408\,d^9 + 23\,d^8 - 292\,d^7 - 402\,d^6 + 416\,d^5 - 115\,d^4 + 109\,d^3 - 78\,d^2 + 18\,d - 1)\right) x^6 - \\
& \left((12d^7 - 75d^6 + 98d^5 + 87d^4 - 118d^3 + 30d^2 + 2d - 1)\,t\,(t+1) + \right. \\
& \quad \left. d\,(48d^{12} - 288d^{11} + 228d^{10} + 1052d^9 - 1499d^8 + 484d^7 - 676d^6 + 1000d^5 - 567d^4 + 264d^3 - 141d^2 + 44d - 5)\right) x^5 + \\
& d\,(d^2-3\,d+1)\left((2d^7 - 12d^6 - 20d^5 + 138d^4 - 67d^3 - 19d^2 + 15d - 2)\,t\,(t+1) + \right. \\
& \quad \left. (16d^{13} - 128d^{12} + 212d^{11} + 72d^{10} + 329d^9 - 1089d^8 + 744d^7 - 427d^6 + 394d^5 - 189d^4 + 57d^3 - 27d^2 + 9d - 1)\right) x^4 + \\
& d^2\,(d^2-3\,d+1)^2\left((12\,d^5 - 40\,d^4 - 20\,d^3 + 38\,d^2 - 12\,d + 1)\,t\,(t+1) + \right. \\
& \quad \left. d\,(64d^{10} - 288d^9 + 240d^8 - 184d^7 + 456d^6 - 394d^5 + 186d^4 - 110d^3 + 41d^2 - 2d - 1)\right) x^3 - \\
& d^4\,(d^2-3\,d+1)^3\left((d^4 - 3\,d^3 - 15\,d^2 + 12\,d - 2)\,t\,(t+1) + \right. \\
& \quad \left. 16d^9 - 144d^8 + 200d^7 - 123d^6 + 124d^5 - 102d^4 + 41d^3 - 17d^2 + 7d - 1\right) x^2 - \\
& d^6\,(2d-1)\,(d^2-3d+1)^4\left(t\,(t+1) + d\,(d-1)\,(16d^3 - 6d^2 + 3d - 3)\right) x + \\
& d^9\,(d-1)\,(2\,d-1)^2\,(d^2-3\,d+1)^5,
\end{aligned}
$$

deren Galoisgruppe die $D_{10/2}$ ist, mit Diskriminante

$$
\begin{aligned}
\operatorname{disc}(H_{10}) = {} & d^{32}\,(2\,t+1)^8\,(2\,d-1)^{14}\,(d^2-3\,d+1)^{20}\,(d-1)^{68}\,(t^2\,(t+1)^2 + \\
& 2\,t\,(t+1)\,d\,(d-1)\,(2\,d^4 + 18\,d^3 - 32\,d^2 + 23\,d - 7) + d\,(d-1)\cdot \\
& (128\,d^9 - 256\,d^8 + 64\,d^7 + 144\,d^6 - 56\,d^5 - 39\,d^4 + 21\,d^3 - 9\,d^2 + 11\,d - 4))^5.
\end{aligned}
$$

5. Fall: $l = 12$

Man setzt

$$
n = t\,(t+1) + d\,(d-1)\,(108\,d^6 - 396\,d^5 + 636\,d^4 - 576\,d^3 + 308\,d^2 - 92\,d + 11).
$$

Zur Vereinfachung der dadurch erhaltenen Polynomfamilie mit Galoisgruppe $D_{12/2}$ wird $x = \frac{d\,(d-1)^5\,(2\,d-1)\,(3\,d^2-3\,d+1)\,(2\,d^2-2\,d+1)}{x}$ transformiert. Die resultierende Familie $H_{12}(x)$, deren Diskriminante sich zu

$$
\begin{aligned}
\operatorname{disc}(H_{12}) \;=\; & d^{140}\,(2\,t+1)^{10}\,(2\,d^2 - 2\,d + 1)^{12}\,(3\,d^2 - 3\,d + 1)^{12}\,(2\,d-1)^{34}\cdot \\
& (d-1)^{140}\,((t+d)^2 + 4\,d\,(d-1)\,(3\,d^2 - 3\,d + 1)^3))^6\cdot \\
& ((t-d+1)^2 + 4\,d\,(d-1)\,(3\,d^2 - 3\,d + 1)^3))^6
\end{aligned}
$$

berechnet, ist im Anhang B.3 zu finden.

3.4 Zahlkörper mit großem l-Rang

Sei K ein Zahlkörper, Cl_K die Idealklassengruppe von K und l eine Primzahl. Der l-Rang $r_l(Cl_K)$ von Cl_K ist die Dimension von $Cl_K/l\,Cl_K$ über $\mathbb{F}_l$, die Anzahl der unabhängigen Erzeuger der Ordnung l von Cl_K. Es ist bekannt, dass der 2-Rang nicht beschränkt ist, wenn K alle quadratischen Zahlkörper durchläuft (siehe z. B. Belabas [2]). Für $l \geq 3$ ist unbekannt, ob $r_l(Cl_K)$ beschränkt ist oder nicht, es gibt auch kein Beispiel für einen Zahlkörper K mit $r_l(Cl_K) > 6$. Andererseits hat Yamamoto [96] 1970 bewiesen, dass zu jedem l unendlich viele imaginärquadratische Zahlkörper existieren, deren l-Rang mindestens 2 ist. Craig [7] zeigte 1977, dass für unendlich viele imaginärquadratische Zahlkörper $r_3(Cl_K) \geq 4$ gilt, und Mestre [63] hat am 07.02.2005 im *Séminaire de théorie des nombres de Chevaleret* gezeigt, dass es unendlich viele imaginärquadratische Zahlkörper mit $r_3(Cl_K) \geq 5$ gibt. Von letzteren ist $\mathbb{Q}(\sqrt{-5393946914743})$ der kleinste[30], was Belabas [2] 2004 bewiesen hat. Bekannt sind außerdem drei Beispiele[31] mit $r_3(Cl_K) = 6$ (siehe Quer [81]). Mestre [62] bewies 1992, dass es unendlich viele imaginärquadratische Zahlkörper gibt, deren 5-Rang mindestens 3 beträgt, von denen Schoof [84] schon im Jahre 1983 Beispiele angegeben hat. Für $r_5(Cl_K) = 4$ und $r_7(Cl_K) = 3$ ist bisher jeweils ein imaginärquadratischer Zahlkörper K publiziert:[32] Schoof [84] veröffentlichte $\mathbb{Q}(\sqrt{-258559351511807})$ mit 5-Rang 4 und Solderitsch [88] $\mathbb{Q}(\sqrt{-480544612303251864826851053 6})$ mit 7-Rang 3. Für größere l sind aktuell nur Beispiele von Leprévost [42] mit $r_{11}(Cl_K) = 3$ bekannt.

Die Konstruktionen der genannten Autoren basieren in der Regel auf elliptischen Kurven (Mestre: Kubert-Kurve E_{10}, Schoof: $X_0(11)$) oder hyperelliptischen Kurven (Yamamoto: $y^2 = 4x^l + d$, Solderitsch: $y^2 = x^{2l} - 6x^l + 1$, Leprévost: $X_0(23), X_0(46)$). Yamamoto konnte bei den Zahlkörpern $K = \mathbb{Q}(\sqrt{y^2 - 4x^l})$ idealtheoretisch zeigen, dass unendlich viele dieser Körper den Rang $r_l(Cl_K) \geq 2$ besitzen. Der theoretische Hintergrund der meisten anderen Arbeiten liegt in der algebraischen Geometrie und gründet sich auf

[30] „Kleinste“ bezieht sich auf den absoluten Wert der Diskriminante des Zahlkörpers.

[31] Die Diskriminanten dieser drei imaginärquadratischen Zahlkörper sind -408368221541174183, -3082320147153282331 und -3161659186633662283.

[32] Weitere imaginärquadratische Zahlkörper mit $r_5(Cl_K) = 4$ und $r_7(Cl_K) = 3$ wurden von Llorente und Quer gefunden; diese sind jedoch nicht veröffentlicht. (Siehe z.B. Leprévost [42].)

Gruppenschemata[33] und Néron-Modelle[34] der betrachteten Kurven.

Ausgangspunkt ist jeweils eine exakte Sequenz (vgl. auch 3.2.4)

$$\mathcal{O} \longrightarrow \langle [D] \rangle \longrightarrow J_{\mathcal{C}} \longrightarrow \overline{J_{\mathcal{C}}} \longrightarrow \mathcal{O},$$

wobei $\mathcal{C}$ eine algebraische Kurve, $J_{\mathcal{C}}$ ihre Jacobische Varietät, $[D]$ eine Divisorenklasse der Ordnung l von $J_{\mathcal{C}}$ und $\overline{J_{\mathcal{C}}}$ die abelsche Varietät $J_{\mathcal{C}}/\langle [D] \rangle$ ist. Durch Anwendung algebraisch-geometrischer Argumente, deren Wiedergabe deutlich über den Rahmen dieses Abschnittes hinausgeht, erhält man schließlich für einen imaginärquadratischen Zahlkörper eine Injektion

$$J'_{\mathcal{C}}(O_K)/C(O_K) \longrightarrow {}_lCl_K.$$

Dabei ist C/O_K das Néron-Modell über O_K der zu $\overline{J_{\mathcal{C}}}$ dualen Varietät, die sich aus obiger exakten Sequenz durch Dualität herleitet, und $J'_{\mathcal{C}}/O_K$ ist ein gewisses Gruppenschema über O_K. (Details hierzu finden sich bei Leprévost [42] und Mestre [60].) Finden sich nun in $J'_{\mathcal{C}}(O_K)/C(O_K)$ zwei unabhängige Elemente, so existieren auch in ${}_lCl_K$, dem l-Teil der Idealklassengruppe, zwei unabhängige Elemente, so dass $r_l(Cl_K) \geq 2$ gilt.

Die folgenden Ausführungen beziehen sich auf Artikel [42] von Leprévost. Während in diesem Artikel eine hyperelliptische Kurve $\mathcal{C} : y^2 = f(x)$ untersucht wird, stehen hier unendlich viele Kurven aus den Familien[35] $\mathcal{C}_{a,b,5}, \mathcal{C}_{b,d,1,5}$ und $\mathcal{C}_{u,v,d,7}$ (siehe Abschnitt 2.2.3) zur Verfügung. Nach ganzzahliger Wahl der Kurvenparameter werden die Kurven auf Anzahl und Größe der Primfaktoren der Diskriminanten[36] im Hinblick auf schlechte Reduktion untersucht. Die Parameter werden jeweils aus der Menge $\{-100, \ldots, 100\}$ gewählt. Für $l = 5$ wurden 54, für $l = 7$ wurden 17 geeignete Kurven gefunden, die bei maximal zwei ungeraden Primzahlen (≤ 200) schlechte Reduktion haben.

[33] Die Theorie von Schemata geht auf einen einzigen Wissenschaftler, Grothendieck, zurück und hat die Verallgemeinerung von Varietäten (inklusive ihrer Zariski-Topologien) in rein algebraischen Ausdrücken zum Ziel. (Siehe dazu Hindry/Silverman [27], A.9.1.)

[34] Eine beliebige Varietät besitzt im Allgemeinen an bestimmten Primstellen p schlechte Reduktion, das heißt, bei der Reduktion modulo p entsteht eine singuläre Varietät. Aus diesem Grund soll die Varietät so vergrößert werden, dass die Reduktion auch an diesem p nicht-singulär ist. Diese Vergrößerung ist ein Gruppenschema und heißt Néron-Modell; sie ist bis auf Isomorphie eindeutig und existiert zu jeder abelschen Varietät, was von Néron selbst bewiesen wurde. (Siehe dazu Hindry/Silverman [27], A.9.4.)

[35] Die Familie $\mathcal{C}_{p,q,7}$ mit einem Torsionspunkt der Ordnung 7 wurde auf Grund der großen Koeffizienten nicht weiter untersucht.

[36] Es wird immer die Diskriminante von $f(x)$ angegeben. Diese unterscheidet sich von der Kurvendiskriminante, sofern die Kurve in der Form $y^2 = f(x)$ gegeben ist, nur durch den Faktor 2^{4g}, wobei g das Geschlecht der Kurve ist.

Eine davon ist

$$\mathcal{C}_{1,4,5} \; : \qquad y^2 \;=\; (x^3 + x^2 + 8\,x + 4)\,(x^3 - x^2 + 7\,x - 11),$$

an der beispielhaft die sich jeweils anschließenden Berechnungen im Folgenden ausgeführt werden.

Diese Kurve $\mathcal{C}_{1,4,5}$ hat (in obiger Gleichung) überall gute Reduktion außer bei 7 und 29. Bei 7 ergibt sich

$$y^2 \;\equiv\; (x^2 + 2\,x + 3)\,(x + 4)^2\,(x + 5)\,(x + 6) \mod 7.$$

Um den modulo 7 singulären Punkt $(-4, 0)$ zu eliminieren, wird $x = -4 + 7\,t$ in $\mathcal{C}_{1,4,5}$ gesetzt. Dabei erhält man die Kurvengleichung

$$y^2 \;=\; 7\,(-76 + 336\,t - 539\,t^2 + 343\,t^3)\,(-17 + 63\,t - 91\,t^2 + 49\,t^3) \;=:\; f_{-4}(t),$$

für die formal

$$\frac{f_{-4}(t)}{7} \equiv 4 \mod 7$$

gilt. Weiter liegt bei 29 schlechte Reduktion vor, und für $y^2 = f_{-4}(t)$ gilt

$$y^2 \;\equiv\; 25\,(t + 3)\,(t + 2)^2\,(t + 19)\,(t + 6)^2 \mod 29.$$

Um die Singularitäten modulo 29 zu eliminieren, wird $t = -2 + 29\,u$ in $y^2 = f_{-4}(t)$ ersetzt. Es ergibt sich

$$y^2 \;=\; f_{(-4,-2)}(u)$$

mit

$$\begin{aligned} f_{(-4,-2)}(u) \;:=\; & 203\,(-5648 + 191632\,u - 2184077\,u^2 + 8365427\,u^3) \\ & (-31 + 1015\,u - 11165\,u^2 + 41209\,u^3). \end{aligned}$$

Formal erhält man

$$\frac{f_{(-4,-2)}(u)}{29} \equiv 18 \mod 29,$$

so dass auf diese Art und Weise beide singulären Punkte modulo 29 gleichzeitig beseitigt werden können. Die erhaltene Gleichung $y^2 = f_{(-4,-2)}(u)$ ist der Ausgangspunkt für die weiteren Berechnungen.

Im nächsten Schritt werden die reellen Nullstellen von $f_{(-4,-2)}(u)$ bestimmt, die bei $0,08612752835$ und bei $0,09576717402$ liegen und zwischen denen

$f_{(-4,-2)}(u)$ negative Werte annimmt. Sei nun B eine ganzzahlige Schranke[37] und sei $u = \frac{i}{j}$ mit $1 \leq j \leq B$ derart, dass j prim zu 7 und 29 ist und dass $u = \frac{i}{j}$ zwischen den beiden Nullstellen von $f_{(-4,-2)}(u)$ liegt. Dann ist der 5-Rang $r_5(Cl_K)$ für den imaginärquadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{f_{(-4,-2)}(u)})$ mindestens 1.

Die konkrete Berechnung erfolgt ausgehend von den folgenden spezialisierten Kurven.[38] Zuerst alle Kurven mit einem Punkt der Ordnung 5:

$\mathcal{C}_{a,b,5}$	a	b	Diskrim. von $f(x)$
	1	1	$23 \cdot 83$
	1	2	$2^6 \cdot 53 \cdot 131$
	1	4	$2^{14} \cdot 7 \cdot 29^2$
	2	-4	$2^{13} \cdot 197$
	2	-1	$-5^5 \cdot 7$
	2	1	$3 \cdot 23$
	2	2	$2^6 \cdot 19 \cdot 109$
	2	4	$2^{15} \cdot 3 \cdot 5^4$
	3	-4	$-2^{16} \cdot 17 \cdot 43$
	3	2	$2^6 \cdot 43$
	3	4	$2^{13} \cdot 3^2 \cdot 19^2$
	4	3	$3^4 \cdot 109$
	4	4	$2^{13} \cdot 5 \cdot 11^2$
	6	4	$-2^{14} \cdot 3 \cdot 11^2$
	6	6	$2^6 \cdot 3^6 \cdot 139$
	7	8	$2^{17} \cdot 13 \cdot 59$

$\mathcal{C}_{b,d,1,5}$	d	b	Diskrim. von $f(x)$
	1	-31	$2^{44} \cdot 17 \cdot 101$
	1	-15	$2^{36} \cdot 3 \cdot 37$
	1	-7	$2^{30} \cdot 5 \cdot 31$
	1	-5	$2^{18} \cdot 3^6 \cdot 11^2$
	1	-1	$2^{18} \cdot 19 \cdot 67$
	1	2	$2^{12} \cdot 31^2$
	1	5	$2^{24} \cdot 43 \cdot 67$
	2	-14	$2^{40} \cdot 7 \cdot 23$
	2	4	$2^{25} \cdot 41 \cdot 137$
	3	4	$2^{12} \cdot 3^{10} \cdot 83$
	14	16	$-2^{25} \cdot 7^{10} \cdot 137$

Unter diesen 27 Kurven sind vier Kurven mit negativer Diskriminante, also besitzt $f(x)$ jeweils vier reelle Nullstellen. In diesen Fällen werden beide

[37] Praktisch wurde meist $B = 15000$ gewählt.

[38] Die Hälfte der anfangs erwähnten 54 Kurven wurden nicht weiter untersucht, weil bei der Elimination der Singularitäten die Koeffizienten teilweise sehr groß wurden oder die Nullstellen zu dicht zusammen lagen, was sehr große Körperdiskriminanten zur Folge hat. Analoges gilt für die Kurven mit einem Punkt der Ordnung 7.

Intervalle untersucht, in denen $f(x)$ negative Werte annimmt, sofern die Intervalle nicht zu klein sind, denn dies hätte sehr große Körperdiskriminanten zur Folge. (Dies trifft auch für die beiden betrachteten Kurven mit einem Punkt der Ordnung 7 zu. Siehe folgende Tabelle.)

Bei den Kurven mit einem Punkt der Ordnung 7 wird der Nenner $w_{u,v} = 3\,v^2 - u - d$ der Koeffizienten (siehe Abschnitt 2.2.3) durch Setzen von $u = u_1 := 3\,v^2 - d - 1$ bzw. von $u = u_{-1} := 3\,v^2 - d + 1$ eliminiert, um Kurven mit ganzzahligen Koeffizienten zu erhalten.

$\mathcal{C}_{u_1,v,d,7}$	v	d	Diskrim. von $f(x)$
	1	1	$2^{24} \cdot 5^2 \cdot 53$
	1	2	$2^{23} \cdot 103$
	1	4	$-2^{28} \cdot 19$
	1	5	$2^{24} \cdot 5^5 \cdot 61$
	1	6	$2^{23} \cdot 3^{14} \cdot 5^2$
	1	9	$2^{24} \cdot 3^{20} \cdot 101$
	1	12	$2^{28} \cdot 3^{22} \cdot 71$

$\mathcal{C}_{u_{-1},v,d,7}$	v	d	Diskrim. von $f(x)$
	1	6	$-2^{24} \cdot 3^5 \cdot 43$

Die Ergebnisse der Untersuchung sind in den folgenden Tabellen zusammengefasst. Zuerst die Zahlkörper mit $r_5(Cl_K) = 3$:

$-\Delta(K)$	Kurve	Cl_K
1237158817307463655	$\mathcal{C}_{-5,1,1,5}$	$435000 \times 20 \times 10 \times 2 \times 2 \times 2$
128236180881027624051	$\mathcal{C}_{2,1,1,5}$	$2388000 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2$
187264536191983840695	$\mathcal{C}_{2,1,5}$	$7888500 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2$
627067952237612355135	$\mathcal{C}_{2,4,5}$	$78050500 \times 10 \times 10 \times 2$
725337966757867340559	$\mathcal{C}_{6,4,5}$	$29079000 \times 20 \times 10 \times 2 \times 2$
1969656765315632780191	$\mathcal{C}_{2,-4,5}$	$36047500 \times 20 \times 10 \times 2 \times 2$
2554995310733425950915	$\mathcal{C}_{2,4,5}$	$26314000 \times 10 \times 10 \times 2 \times 2$
2927734242780096140927	$\mathcal{C}_{3,4,5}$	$104439500 \times 10 \times 10 \times 2 \times 2$
3253368489499420878615	$\mathcal{C}_{2,4,5}$	$104943750 \times 10 \times 10 \times 2 \times 2$
4362013615130038177131	$\mathcal{C}_{4,3,1,5}$	$61513000 \times 20 \times 10 \times 2$
7877039817092440928187	$\mathcal{C}_{4,3,1,5}$	$25678000 \times 10 \times 10 \times 2 \times 2$
10777868000847235430439	$\mathcal{C}_{6,4,5}$	$408168750 \times 10 \times 10 \times 2$
13503402682025812161203	$\mathcal{C}_{2,1,1,5}$	$125301500 \times 10 \times 10 \times 2$
18098278981575412478159	$\mathcal{C}_{2,-1,5}$	$458787500 \times 10 \times 10 \times 2 \times 2$

$-\Delta(K)$	Kurve	Cl_K
32793059398336805135739	$\mathcal{C}_{2,1,1,5}$	$137985750 \times 10 \times 10 \times 2 \times 2$
33778404599053432529535	$\mathcal{C}_{2,4,5}$	$280401250 \times 10 \times 10 \times 2 \times 2$
35253291884155495552763	$\mathcal{C}_{2,1,1,5}$	$187722000 \times 10 \times 10 \times 2$
69884925442885595503527	$\mathcal{C}_{6,4,5}$	$213803750 \times 10 \times 10 \times 2 \times 2 \times 2$
109086505971168036991159	$\mathcal{C}_{3,4,5}$	$2039898000 \times 10 \times 10$
118561426837906477764531	$\mathcal{C}_{4,3,1,5}$	$2411277500 \times 10 \times 5$
125538546985034149902603	$\mathcal{C}_{2,1,1,5}$	$33963900 \times 50 \times 10 \times 2 \times 2$
259191856749839800455339	$\mathcal{C}_{6,4,5}$	$351021750 \times 10 \times 10 \times 2 \times 2$
300898750825133265918795	$\mathcal{C}_{6,4,5}$	$145082500 \times 10 \times 10 \times 2 \times 2 \times 2$
313722695854056260630859	$\mathcal{C}_{6,4,5}$	$111270000 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2$
334080419323489720395135	$\mathcal{C}_{2,4,5}$	$1105222000 \times 10 \times 10 \times 2 \times 2$
727161503030460136578747	$\mathcal{C}_{2,1,1,5}$	$198844500 \times 10 \times 10 \times 2 \times 2 \times 2$
798968818235953536458871	$\mathcal{C}_{4,3,1,5}$	$4143861000 \times 10 \times 10 \times 2$
820522838548466418765767	$\mathcal{C}_{2,1,1,5}$	$303485500 \times 20 \times 10 \times 2 \times 2 \times 2 \times 2$
838954490591219789810859	$\mathcal{C}_{6,4,5}$	$92735250 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2 \times 2$
113275277326591709766 3015	$\mathcal{C}_{2,4,5}$	$1939612250 \times 10 \times 10 \times 2 \times 2$
116109190095036642075 0107	$\mathcal{C}_{2,1,1,5}$	$1278334500 \times 10 \times 10 \times 2$
166587184753148166616 5415	$\mathcal{C}_{3,4,5}$	$850883000 \times 10 \times 10 \times 2 \times 2 \times 2$
215404488184842445032 1535	$\mathcal{C}_{4,4,5}$	$11241016500 \times 10 \times 10$
227762585530500204264 6311	$\mathcal{C}_{2,-4,5}$	$2232549250 \times 10 \times 10 \times 2 \times 2 \times 2$
231614541443566642799 2335	$\mathcal{C}_{2,4,5}$	$570962250 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2$
260944724060025220660 7687	$\mathcal{C}_{2,1,1,5}$	$1618760250 \times 10 \times 10 \times 2 \times 2 \times 2$
310337019653679746949 5339	$\mathcal{C}_{1,4,5}$	$3764411750 \times 10 \times 10 \times 2$
313686843619019249933 9335	$\mathcal{C}_{4,4,5}$	$2091523000 \times 20 \times 10 \times 2$
382075325060104296937 3479	$\mathcal{C}_{6,4,5}$	$833007000 \times 20 \times 10 \times 2 \times 2 \times 2$
431059042189254224698 2939	$\mathcal{C}_{4,3,1,5}$	$1124278500 \times 10 \times 10 \times 2 \times 2$
447839656198066430941 9335	$\mathcal{C}_{2,4,5}$	$6375263000 \times 10 \times 10 \times 2$
722716955996526831711 1539	$\mathcal{C}_{4,3,1,5}$	$955607000 \times 40 \times 10 \times 2$
754803605034305785944 1599	$\mathcal{C}_{6,4,5}$	$790070000 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2 \times 2$
117928136257808940866 86935	$\mathcal{C}_{2,4,5}$	$1923149500 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2$
197603194208159032096 38135	$\mathcal{C}_{2,4,5}$	$2002069500 \times 10 \times 10 \times 2 \times 2 \times 2 \times 2$
316894952680558163992 93767	$\mathcal{C}_{6,4,5}$	$9332210750 \times 10 \times 10 \times 2 \times 2$
358995200694986536899 55131	$\mathcal{C}_{4,3,1,5}$	$5847144500 \times 10 \times 10 \times 2$
373262383612985300076 30339	$\mathcal{C}_{4,3,1,5}$	$10118884500 \times 10 \times 10 \times 2$
724914624089715724139 47879	$\mathcal{C}_{2,2,5}$	$3880756250 \times 10 \times 10 \times 2 \times 2 \times 2$

Und die gefundenen imaginärquadratischen Zahlkörper mit $r_7(Cl_K) = 2$:

$-\Delta(K)$	Kurve	Cl_K
175687836012054155	$\mathcal{C}_{u_1,1,4,7}$	$816340 \times 14 \times 2 \times 2 \times 2 \times 2$
360749648242621195	$\mathcal{C}_{u_1,1,4,7}$	$1162084 \times 28 \times 2 \times 2$
616805120532435755	$\mathcal{C}_{u_1,1,9,7}$	$4850020 \times 14 \times 2 \times 2$
1162893606848063587	$\mathcal{C}_{u_1,1,4,7}$	$734706 \times 14 \times 2 \times 2 \times 2 \times 2$
1204866585378245779	$\mathcal{C}_{u_1,1,9,7}$	$1843968 \times 28 \times 2 \times 2$
2868282309926099611	$\mathcal{C}_{u_1,1,4,7}$	$3932838 \times 14 \times 2 \times 2 \times 2$
6766934584288884627	$\mathcal{C}_{u_1,1,4,7}$	$5205368 \times 14 \times 2 \times 2 \times 2$
28134314940177667003	$\mathcal{C}_{u_1,1,4,7}$	$7808052 \times 14 \times 2 \times 2 \times 2$
37070531147262312227	$\mathcal{C}_{u_1,1,4,7}$	$7260624 \times 14 \times 2 \times 2 \times 2 \times 2$
38448880695555460739	$\mathcal{C}_{u_1,1,4,7}$	$5056506 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
38870100890120553455	$\mathcal{C}_{u_1,1,6,7}$	$117159196 \times 14 \times 2 \times 2$
41116118869352457795	$\mathcal{C}_{u_1,1,4,7}$	$4802000 \times 14 \times 2 \times 2 \times 2 \times 2$
61478529174488116019	$\mathcal{C}_{u_1,1,4,7}$	$29772400 \times 14 \times 2 \times 2 \times 2$
65643881666136195939	$\mathcal{C}_{u_1,1,9,7}$	$6482700 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
70513304812500732803	$\mathcal{C}_{u_1,1,4,7}$	$5551112 \times 28 \times 2 \times 2 \times 2 \times 2$
145921815935209797383	$\mathcal{C}_{u_1,1,4,7}$	$60298714 \times 14 \times 2 \times 2 \times 2 \times 2$
163481769799804117955	$\mathcal{C}_{u_1,1,4,7}$	$1495480 \times 98 \times 2 \times 2 \times 2 \times 2 \times 2$
179039241255149734835	$\mathcal{C}_{u_1,1,4,7}$	$101442250 \times 14 \times 2 \times 2$
458450139170355475715	$\mathcal{C}_{u_1,1,4,7}$	$37772532 \times 14 \times 2 \times 2 \times 2 \times 2$
526072250433357801971	$\mathcal{C}_{u_1,1,4,7}$	$89888638 \times 14 \times 2 \times 2 \times 2$
827488871726615170435	$\mathcal{C}_{u_1,1,4,7}$	$45446128 \times 14 \times 2 \times 2 \times 2$
1074813082604330302987	$\mathcal{C}_{u_1,1,4,7}$	$7193396 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
1229139405492827863107	$\mathcal{C}_{u_1,1,4,7}$	$14319564 \times 28 \times 2 \times 2 \times 2 \times 2$
1364943970422372325843	$\mathcal{C}_{u_1,1,9,7}$	$4417840 \times 28 \times 2 \times 2 \times 2 \times 2 \times 2$
1458895792053390800235	$\mathcal{C}_{u_1,1,4,7}$	$32951324 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
2049421256849800707131	$\mathcal{C}_{u_1,1,9,7}$	$40115908 \times 28 \times 4 \times 2 \times 2$
2143495478933506762895	$\mathcal{C}_{u_1,1,6,7}$	$838184298 \times 14 \times 2 \times 2 \times 2$
2355562055291966695195	$\mathcal{C}_{u_1,1,4,7}$	$37047430 \times 14 \times 2 \times 2 \times 2 \times 2$
2873331595577871128123	$\mathcal{C}_{u_1,1,4,7}$	$115003098 \times 14 \times 2 \times 2 \times 2$
3706322043746962689955	$\mathcal{C}_{u_1,1,5,7}$	$207139072 \times 28 \times 2$
4033273868960090916131	$\mathcal{C}_{u_1,1,4,7}$	$35976584 \times 28 \times 2 \times 2 \times 2 \times 2 \times 2$
5787357001170556761915	$\mathcal{C}_{u_1,1,4,7}$	$13704908 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
5893840457582092136803	$\mathcal{C}_{u_1,1,4,7}$	$47587820 \times 28 \times 2 \times 2 \times 2$
11978721097010039824707	$\mathcal{C}_{u_1,1,9,7}$	$107862524 \times 14 \times 2 \times 2 \times 2 \times 2$
14616529802415355073299	$\mathcal{C}_{u_1,1,4,7}$	$154931728 \times 14 \times 2 \times 2 \times 2 \times 2$
15841404756140419829947	$\mathcal{C}_{u_1,1,4,7}$	$100640316 \times 14 \times 2 \times 2 \times 2 \times 2$

$-\Delta(K)$	Kurve	Cl_K
18606482705644680397407	$\mathcal{C}_{u_{-1},1,6,7}$	$4019394050 \times 14 \times 2$
19033631360080682315947	$\mathcal{C}_{u_1,1,9,7}$	$242121642 \times 14 \times 2 \times 2$
22554278750716806455043	$\mathcal{C}_{u_1,1,4,7}$	$140357658 \times 14 \times 2 \times 2 \times 2 \times 2$
26527900923085209913355	$\mathcal{C}_{u_1,1,4,7}$	$77081704 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
3100475611558342367379 5	$\mathcal{C}_{u_1,1,5,7}$	$849742712 \times 28 \times 2$
32544297374946013072667	$\mathcal{C}_{u_1,1,4,7}$	$132852132 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
44609762969841645125403	$\mathcal{C}_{u_1,1,4,7}$	$211388842 \times 14 \times 2 \times 2 \times 2 \times 2$
48553166773754105153915	$\mathcal{C}_{u_1,1,4,7}$	$22353310 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
59698145159257722641507	$\mathcal{C}_{u_1,1,9,7}$	$189054740 \times 14 \times 2 \times 2 \times 2 \times 2$
61631921058912091250827	$\mathcal{C}_{u_1,1,4,7}$	$80808056 \times 28 \times 2 \times 2 \times 2 \times 2$
71435278808357709112819	$\mathcal{C}_{u_1,1,4,7}$	$138105520 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
73440398276511781681059	$\mathcal{C}_{u_1,1,4,7}$	$325993374 \times 14 \times 2 \times 2 \times 2 \times 2$
12450889038641512678339 1	$\mathcal{C}_{u_1,1,5,7}$	$11472741518 \times 14 \times 2$
15346669511845261931418 7	$\mathcal{C}_{u_1,1,4,7}$	$257939430 \times 14 \times 2 \times 2 \times 2 \times 2$
15876809484144526833731 9	$\mathcal{C}_{u_1,1,4,7}$	$515590740 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
16162655195113408110119 5	$\mathcal{C}_{u_1,1,5,7}$	$266530208 \times 28 \times 2 \times 2 \times 2$
17382239715951405440362 7	$\mathcal{C}_{u_1,1,4,7}$	$239504552 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
20033183542172456830479 5	$\mathcal{C}_{u_1,1,4,7}$	$385456540 \times 28 \times 2 \times 2 \times 2 \times 2$
21225522761552592702505 1	$\mathcal{C}_{u_1,1,4,7}$	$2129739822 \times 14 \times 2 \times 2 \times 2$
32865617699979074915129 9	$\mathcal{C}_{u_1,1,4,7}$	$2861550216 \times 14 \times 2 \times 2 \times 2$
38909724130398290321023 5	$\mathcal{C}_{u_1,1,4,7}$	$387353330 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
50152478886370466940409 9	$\mathcal{C}_{u_1,1,9,7}$	$1310825950 \times 14 \times 2 \times 2 \times 2$
84098272002437093012495 5	$\mathcal{C}_{u_1,1,9,7}$	$145851146 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
98643287598371732677861 9	$\mathcal{C}_{u_1,1,4,7}$	$630919688 \times 98 \times 2 \times 2$
10335338881230886740946 03	$\mathcal{C}_{u_1,1,9,7}$	$691199880 \times 28 \times 4 \times 2$
19105913511510313364724 03	$\mathcal{C}_{u_1,1,9,7}$	$277949364 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
38567845918590246203453 95	$\mathcal{C}_{u_1,1,9,7}$	$1584381484 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2$
58645274220465392951818 51	$\mathcal{C}_{u_1,1,9,7}$	$10589380004 \times 14 \times 2 \times 2$
17527441607316623693030 115	$\mathcal{C}_{u_1,1,9,7}$	$2235427040 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
24667380390324428635077 043	$\mathcal{C}_{u_1,1,9,7}$	$874429794 \times 14 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
53674971877598595807132 547	$\mathcal{C}_{u_1,1,9,7}$	$163978696 \times 28 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

Anhang A

Quotientenkurvenberechnung nach Vélu

Die Formeln von Vélu aus Abschnitt 3.2.3 ermöglichen eine Berechnung der Gleichungen von Quotientenkurven $E_l/\langle A \rangle$, wobei E_l die Kubert-Kurve mit einem Punkt $A = (0, 0)$ der Ordnung l ist.

Im Folgenden wird diese Berechnung für die Fälle $3 \leq l \leq 8$ ausgeführt. Die Ergebnisse dieser Berechnung finden sich auch in der Tabelle in Abschnitt 3.2.3. Die Fälle $l = 9, 10, 12$ folgen im Anhang B.

1. Fall $l = 3$:

Wählt man z. B. $S = \{A\}$, so berechnen sich t und w zu $t = a_1\, a_3$ und $w = {a_3}^2$, und eine Gleichung der Quotientenkurve lautet:

$$E_3/\langle A \rangle \;:\; Y^2 + a_1\, XY + a_3\, Y \;=\; X^3 - 5\, a_1\, a_3\, X - a_3\, ({a_1}^3 + 7\, a_3).$$

Der Isomorphismus $Y \mapsto \frac{1}{2}\,(Y - (a_1\, X + a_3)\,)$ führt zur (langen) Weierstraß-Form

$$Y^2 \;=\; 4\, X^3 + a_1^2\, X^2 - 18\, a_1\, a_3\, X - a_3\, (27\, a_3 + 4\, a_1^3),$$

welches genau die in Abschnitt 3.2.2 (Indikatorfunktionen) berechnete Kurvengleichung ist.

2. Fall $l = 4$:

Mit $S = \{A, 2A\}$, wobei $2A = (b, 0)$ ist, berechnet man $t = b(b-1)$ und $w = b^2(b+1)$. Damit lautet die Gleichung von $E/\langle A \rangle$:

$$E_4/\langle A \rangle \; : \; Y^2 + XY - bY \; = \; X^3 - bX^2 - 5b(b-1)X - b(3b^2 + 12b - 1).$$

Die Weierstraß-Form dieser Kurve lautet

$$Y^2 \; = \; 4X^3 - (4b-1)X^2 - 2b(10b-9)X - b(b+4)(12b-1),$$

und mit dem Isomorphismus $X \mapsto X - b$ erhält man die in Abschnitt 3.2.2 gefundene Kurvengleichung, mit der eine Bedingung formuliert wurde, wann F_4 die Galoisgruppe C_4 besitzt:

$$Y^2 \; = \; 4X^3 - (16b-1)X^2 + 16bX - 4b(16b-1).$$

3. Fall $l = 5$:

Ein mögliches Repräsentantensystem $S = \{A, 3A\}$ mit $3A = (b, 0)$ liefert $t = b(b^2 + 2b - 1)$ und $w = b^2(2b^2 + b + 1)$, so dass sich die Gleichung der Quotientenkurve $E_5/\langle A \rangle$ zu

$$Y^2 + (1-b)XY - bY = X^3 - bX^2 - 5b(b^2+2b-1)X - b(b^4+10b^3-5b^2+15b-1)$$

bzw. zu

$$Y^2 \; = \; 4X^3 + (b^2-6b+1)X^2 - 2b(10b^2+19b-9)X - b(4b^4+40b^3-20b^2+59b-4)$$

berechnet.[1] Daraus folgt die in Abschnitt 3.2.2 bestimmte Gleichung durch den Isomorphismus $X \mapsto X - 2b$:

$$Y^2 = 4X^3 + (b^2-30b+1)X^2 - 2b(3b+1)(4b-7)X - b(4b^4-4b^3-40b^2+91b-4).$$

[1] In LPS1 [48] wird auf Seite 403 die schon transformierte Kurve als Vélu-Kurve bezeichnet.

4. Fall $l = 6$:

Das System $S = \{A,\, 3A,\, 4A\}$ mit $3A = (c, c^2)$ und $4A = (\, c(c+1), 0\,)$ führt zu $t = c(3c^3 + 4c^2 + c - 1)$ und $w = c^2(4c^4 + 9c^3 + 6c^2 + 3c + 1)$ und zu der Gleichung

$$\begin{aligned} Y^2 + (1-c)\,XY - c(c+1)\,Y \;=\; & X^3 - c(c+1)\,X^2 - 5c\,(3c^3 + 4c^2 + c - 1)\,X \\ & - c\,(19c^5 + 33c^4 + 18c^3 + 22c^2 + 14c - 1) \end{aligned}$$

von $E_6/\langle\, A\,\rangle$, deren Weierstraß-Form

$$\begin{aligned} Y^2 \;=\; & 4\,X^3 - (3c^2 + 6c - 1)\,X^2 - 2c\,(30c^3 + 39c^2 + 10c - 9)\,X - \\ & c\,(4\,c^3 + 4\,c^2 + c + 4)\,(19\,c^2 + 14\,c - 1) \end{aligned}$$

lautet. Mit dem Isomorphismus $X \mapsto X - c(2\,c + 3)$ kommt man zu der in Abschnitt 3.2.2 gefundenen Gleichung:

$$Y^2 = 4\,X^3 - (27\,c^2 + 42\,c - 1)\,X^2 + (12\,c(c+1)(9c+1))\,X - 4c(27c-1)(c+1)^2.$$

5. Fall $l = 7$:

Ein Repräsentantensystem $S = \{A,\, 3A,\, 5A\}$ von $\langle\, A\,\rangle$ mit den Punkten $3A = (d(d-1), d(d^2-2d+1))$ und $5A = (d^2(d-1), 0)$, ergibt $t = d(d-1)(d^2-d+1)\cdot$ $\cdot(d^3 + 2d^2 - 5d + 1)$ und $w = d^2\,(d-1)^2\,(2d^6 - 2d^5 + d^4 - 8d^3 + 15d^2 - 9d + 2)$, und eine Gleichung der Quotientenkurve lautet

$$\begin{aligned} & Y^2 - (d^2 - d - 1)\,XY - d^2\,(d-1)\,Y = X^3 - d^2\,(d-1)\,X^2 - \\ & \quad 5d\,(d-1)(d^2 - d + 1)(d^3 + 2d^2 - 5d + 1)\,X - \\ & \quad d\,(d-1)(d^9 + 9d^8 - 37d^7 + 70d^6 - 132d^5 + 211d^4 - 182d^3 + 76d^2 - 18d + 1) \end{aligned}$$

und in Weierstraß-Form

$$\begin{aligned} Y^2 \;=\; & 4\,X^3 + (d^4 - 6d^3 + 3d^2 + 2d + 1)\,X^2 - \\ & 2d\,(d-1)\,(10\,d^5 + 10\,d^4 - 61\,d^3 + 81\,d^2 - 59\,d + 10)\,X - \\ & d\,(d-1)\,(4\,d^9 + 36\,d^8 - 148\,d^7 + 280\,d^6 - 528\,d^5 + 843\,d^4 - 727\,d^3 + \\ & \qquad 304\,d^2 - 72\,d + 4), \end{aligned}$$

welche durch $X \mapsto X - 2\,d\,(d^2 - 1)$ isomorph zur Kurve aus 3.2.2 ist:

$$\begin{aligned} Y^2 \;=\; & 4\,X^3 + (d^4 - 30\,d^3 + 3\,d^2 + 26\,d + 1)\,X^2 - \\ & 2\,d\,(d-1)\,(12d^5 - 24d^4 - 91d^3 + 115d^2 - 29d + 12)\,X - \\ & d\,(d-1)\,(4d^9 - 8d^8 - 136d^7 + 612d^6 - 916d^5 + 747d^4 - 395d^3 + \\ & \qquad 112d^2 - 28d + 4). \end{aligned}$$

6. Fall $l = 8$:

Aus $S = \{A,\, 3A,\, 4A,\, 6A\}$ mit

$$\begin{aligned} 3A &= \left(d(2d-1)(d-1), d^2(2d-1)(d-1)^2 \right), \\ 4A &= \left(d^3(d-1), d^4(d-1)^2 \right), \\ 6A &= \left(d^2(2d-1)(d-1), 0 \right) \end{aligned}$$

berechnet man

$$\begin{aligned} t &= d\,(d-1)\,(17d^6 - 51d^5 + 59d^4 - 33d^3 + 5d^2 + 3d - 1) \quad \text{und} \\ w &= d^2\,(d-1)^2\,(49d^8 - 179d^7 + 267d^6 - 209d^5 + 111d^4 - 65d^3 + 39d^2 - 14d + 2). \end{aligned}$$

Eine Gleichung der Quotientenkurven $E_8/\langle\, A \,\rangle$ lautet

$$\begin{aligned} &Y^2 - (2d^2 - 4d + 1)\,XY - d^3\,(2d-1)(d-1)\,Y = \\ &\quad X^3 - d^2(2d-1)(d-1)\,X^2 - \\ &\quad 5\,d\,(d-1)\,(17\,d^6 - 51\,d^5 + 59\,d^4 - 33\,d^3 + 5\,d^2 + 3\,d - 1)\,X - \\ &\quad d(d-1)\,(275\,d^{10} - 1460\,d^9 + 3362\,d^8 - 4388\,d^7 + 3721\,d^6 - 2315\,d^5 + \\ &\quad 1123\,d^4 - 392\,d^3 + 77\,d^2 - 3\,d - 1) \end{aligned}$$

bzw. in Weierstraß-Form

$$\begin{aligned} Y^2 = {} & 4\,X^3 - (4d^4 + 4d^3 - 16d^2 + 8d - 1)\,X^2 - \\ & 2d\,(d-1)\,(170d^6 - 514d^5 + 600d^4 - 336d^3 + 51d^2 + 30d - 10)\,X - \\ & d\,(d-1)\,(44d^4 - 84d^3 + 48d^2 - 8d - 1)\,\cdot \\ & (25d^6 - 85d^5 + 116d^4 - 80d^3 + 44d^2 - 20d + 4), \end{aligned}$$

und die isomorphe Abbildung $X \mapsto X - d\,(5d^3 - 3d^2 - 4d + 2)$ führt zur selben Gleichung wie die Indikatorfunktion in Abschnitt 3.2.2:

$$\begin{aligned} Y^2 = {} & 4\,X^3 - (64\,d^4 - 32\,d^3 - 64\,d^2 + 32\,d - 1)\,X^2 + \\ & 8\,d\,(d-1)\,(2\,d-1)\,(64\,d^4 - 80\,d^3 + 8\,d^2 + 12\,d - 3)\,X - \\ & 4\,d\,(d-1)\,(64\,d^4 - 96\,d^3 + 32\,d^2 - 1)\,(2\,d-1)^4. \end{aligned}$$

Anhang B

D_l und C_l mit $l = 9, 10, 12$

Die Berechnungen der Polynome mit Galoisgruppe D_l bzw. C_l in den Abschnitten 3.1 und 3.2 in den drei Fällen $l = 9, 10, 12$ führen zu großen und unhandlichen Ausdrücken. Aus diesem Grund sind diese drei Fälle einzeln kompakt zusammengefasst. Die Bezeichnungen und Abfolge der Ergebnisse orientieren sich dabei an den Ausführungen der Kapitel 3.1 und 3.2.

B.1 Fall $l = 9$

Die Konstruktion einer Polynomfamilie mit Galoisgruppe D_9 basiert auf der über $\mathbb{Q}$ definierten elliptischen Kurve

$$E_l \quad : \quad y^2 + (1-c)\,xy - b\,y \;=\; x^3 - b\,x^2,$$

mit $c = d^2(d-1)$ und $b = d^2(d-1)(d^2-d+1)$, die einen Punkt der Ordnung 9 hat: $A = (0, 0)$.

Konstruktion des Polynoms

In diesem Fall sind alle folgenden Resultate jeweils durch $\alpha := d - 1$ und $\beta := d^2 - d + 1$ verkürzt.

Die Punktberechnung ergibt:

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{y_P\, d^2\, \alpha\, \beta}{{x_P}^2}$
$P \oplus 2A$	$\frac{d^2\, \alpha\, \beta\, (-d^2\, \alpha\, y_P + {x_P}^2 + d^2\, \alpha\, (d-2)\, (d^2+1)\, x_P + d^4\, \beta\, \alpha^2)}{(d^2\, \alpha\, \beta - x_P)^2}$
$P \oplus 3A$	$\frac{d^2\, \alpha\, (d\, \alpha^2\, y_P + (d\, \alpha - x_P)\, (d^2\, \alpha\, \beta - x_P))}{(x_P - d^2\, \alpha)^2}$
$P \oplus 4A$	$\frac{d\, \alpha\, \beta\, (-\alpha^3\, y_P + {x_P}^2 + \alpha\, \beta\, (d^3 - 3\, d^2 + d - 1)\, x_P + d^2\, \alpha^2\, \beta^2)}{(x_P - d\, \alpha\, \beta)^2}$
$P \oplus 5A$	$\frac{d\, \alpha\, \beta\, (\alpha^3\, y_P + {x_P}^2 - d^2\, \alpha\, (d^2 - 2\, d + 3)\, x_P + d^3\, \beta\, \alpha^2)}{(x_P - d\, \alpha\, \beta)^2}$
$P \oplus 6A$	$\frac{d^2\, \alpha\, (-d\, \alpha^2\, y_P + {x_P}^2 + d^2\, \alpha\, (d^3 - 3\, d^2 + 2\, d - 2)\, x_P + d^4\, \beta\, \alpha^2)}{(x_P - d^2\, \alpha)^2}$
$P \oplus 7A$	$\frac{d^2\, \alpha\, \beta\, (d^2\, \alpha\, y_P + x_P\, (x_P - d^2\, \alpha\, \beta))}{(x_P - d^2\, \alpha\, \beta)^2}$
$P \oplus 8A$	$\frac{d^2\, \alpha\, \beta\, (-y_P + (d^3 - d^2 - 1)\, x_P + d^2\, \alpha\, \beta)}{{x_P}^2}$

Damit berechnet man:

$$n_9 = \big({x_P}^9 + d\,\alpha\,\beta\,(d^7 - 2\,d^6 - 6\,d^5 + 11\,d^4 - 22\,d^3 + 21\,d^2 - 5\,d + 1)\,{x_P}^7 - d^3\,\alpha^2\,\beta\,(4\,d^8 - 20\,d^7 + 45\,d^6 - 109\,d^5 + 149\,d^4 - 141\,d^3 + 79\,d^2 - 17\,d + 3)\,{x_P}^6 + d^4\,\alpha^3\,\beta^2\,(d^9 - 5\,d^8 + 23\,d^7 - 83\,d^6 + 119\,d^5 - 134\,d^4 + 74\,d^3 - 17\,d^2 + 2\,d - 1)\,{x_P}^5 - d^6\,\alpha^4\,\beta^3\,(4\,d^7 - 17\,d^6 + 24\,d^5 - 42\,d^4 + 17\,d^3 - 12\,d^2 - 4\,d - 5)\,{x_P}^4 + d^8\,\alpha^5\,\beta^3\,(d^8 - 4\,d^7 + 5\,d^6 - 7\,d^5 - 4\,d^4 - 2\,d^3 - 14\,d^2 - 10)\,{x_P}^3 - d^{10}\,\alpha^6\,\beta^4\,(d^3 - 3\,d^2 - 5)\,(d^2 + 2)\,{x_P}^2 + d^{12}\,\alpha^7\,\beta^5\,(d^3 - 3\,d^2 - 5)\,x_P + d^{14}\,\alpha^8\,\beta^6\big) / \big({x_P}^2\,(d^2\,\alpha\,\beta - x_P)^2\,(d^2\,\alpha - x_P)^2\,(d\,\alpha\,\beta - x_P)^2\big).$$

Das zugehörige Polynom mit Galoisgruppe D_9 lautet

$$\begin{aligned}
F_9(x) \;=\;& x^9 - n\,x^8 + \\
& d\,\alpha\,\big(2\,(d^3+d+1)\,n + \beta\,(d^7 - 2\,d^6 - 6\,d^5 + 11\,d^4 - 22\,d^3 + 21\,d^2 - 5\,d + 1)\big)\,x^7 - \\
& d^2\,\alpha^2\,\big((d^6 + 2\,d^5 + 8\,d^3 - 3\,d^2 + 6\,d + 1)\,n + \\
& \qquad d\,\beta\,(4\,d^8 - 20\,d^7 + 45\,d^6 - 109\,d^5 + 149\,d^4 - 141\,d^3 + 79\,d^2 - 17\,d + 3)\big)\,x^6 + \\
& d^4\,\alpha^3\,\beta\,\big((2\,d^5 + 6\,d + 8\,d^3 + 4)\,n + \\
& \qquad \beta\,(d^9 - 5\,d^8 + 23\,d^7 - 83\,d^6 + 119\,d^5 - 134\,d^4 + 74\,d^3 - 17\,d^2 + 2\,d - 1)\big)\,x^5 - \\
& d^6\,\alpha^4\,\beta^2\,\big((2\,d^3 + d^4 + 2\,d + 4\,d^2 + 6)\,n + \\
& \qquad \beta\,(4\,d^7 - 17\,d^6 + 24\,d^5 - 42\,d^4 + 17\,d^3 - 12\,d^2 - 4\,d - 5)\big)\,x^4 + \\
& d^8\,\alpha^5\,\beta^3\,\big(2\,(d^2+2)\,n + d^8 - 4\,d^7 + 5\,d^6 - 7\,d^5 - 4\,d^4 - 2\,d^3 - 14\,d^2 - 10\big)\,x^3 - \\
& d^{10}\,\alpha^6\,\beta^4\,\big(n + (d^3 - 3\,d^2 - 5)\,(d^2+2)\big)\,x^2 + \\
& d^{12}\,\alpha^7\,\beta^5\,(d^3 - 3\,d^2 - 5)\,x + \\
& d^{14}\,\alpha^8\,\beta^6.
\end{aligned}$$

Das zur Indikatorfunktion gehörende quadratische Polynom von $F_9(x)$ berechnet sich zu

$$\begin{aligned}
&\mathcal{C}_9^2 - d^2\,\alpha\beta\left(2n^2 + d\,\alpha\,(d^4 - 5d^3 - 4d^2 - 5d - 8)\,n - \right.\\
&\left. d\,\alpha\beta\,(8d^6 - 36d^5 + 55d^4 - 99d^3 + 84d^2 - 20d + 4)\right)\mathcal{C}_9 + \\
&d^4\,\alpha^2\beta^2\,\left(n^4 - d\,\alpha\,(4d^3 + 4d^2 + 5d + 8)\,n^3 + d\,\alpha\cdot\right.\\
&(5d^9 - 17d^8 + 64d^7 - 104d^6 + 203d^5 - 240d^4 + 201d^3 - 112d^2 + 8d - 4)\,n^2 + \\
&2d^2\,\alpha^2\beta\,(3d^{11} - 11d^{10} + 7d^9 - 2d^8 - 27d^7 + 8d^6 - 68d^5 + 60d^4 - 111d^3 + \\
&147d^2 - 35d + 8)\,n + d^2\,\alpha^2\beta^2\,(d^{15} - 2d^{14} - 34d^{13} + 198d^{12} - 627d^{11} + \\
&1621d^{10} - 3132d^9 + 4567d^8 - 5258d^7 + 5456d^6 - 4854d^5 + 2875d^4 - \\
&\left.1039d^3 + 268d^2 - 40d + 4)\right),
\end{aligned}$$

welches über die Diskriminantenberechnung in $\mathcal{C}_9$ zur elliptischen Kurve

$$\begin{aligned}
z^2 \;=\;& 4\,n^3 + (d^6 - 30d^5 + 33d^4 - 34d^3 + 6d^2 + 24d + 1)\,n^2 - \\
& 6\,d\,\alpha\beta\,(4d^7 - 8d^6 - 24d^5 + 41d^4 - 85d^3 + 84d^2 - 17d + 4)\,n - \\
& d\,\alpha\beta^2\,(4d^{11} - 4d^{10} - 140d^9 + 588d^8 - 1344d^7 + 2964d^6 - 4020d^5 + \\
& 2751d^4 - 1023d^3 + 256d^2 - 40d + 4)
\end{aligned}$$

führt. Die Quotientenkurve $E_9/\langle A \rangle$ lautet mit

$$\begin{aligned}
t \;=\;& d\,(d-1)\,(d^9 - 8\,d^7 + 25\,d^6 - 47\,d^5 + 61\,d^4 - 53\,d^3 + 28\,d^2 - 9\,d + 1), \\
w \;=\;& d^2\,(d-1)^2\,(2\,d^{12} - 6\,d^{11} + 10\,d^{10} - 19\,d^9 + 56\,d^8 - 141\,d^7 + 241\,d^6 - \\
& 285\,d^5 + 245\,d^4 - 153\,d^3 + 66\,d^2 - 17\,d + 2)
\end{aligned}$$

nach den Formeln von Vélu (siehe 3.2.3)

$$\begin{aligned}
&Y^2 - (d^3 - d^2 - 1)\,X\,Y - d^2\,\alpha\beta\,Y = X^3 - d^2\,\alpha\beta\,X^2 - \\
&\quad 5\,d\,\alpha\,(d^9 - 8d^7 + 25d^6 - 47d^5 + 61d^4 - 53d^3 + 28d^2 - 9d + 1)\,X - \\
&\quad d\,\alpha\,(d^{15} + 8\,d^{14} - 55\,d^{13} + 175\,d^{12} - 466\,d^{11} + 1173\,d^{10} - 2518\,d^9 + \\
&\quad 4189d^8 - 5236d^7 + 4938d^6 - 3518d^5 + 1861d^4 - 698d^3 + 167d^2 - 23d + 1)
\end{aligned}$$

bzw. in Weierstraß-Form

$$\begin{aligned} Y^2 &= 4\,X^3 + (d^6 - 6\,d^5 + 9\,d^4 - 10\,d^3 + 6\,d^2 + 1)\,X^2 - \\ &\quad 2\,d\,\alpha\,(10\,d^9 - 80\,d^7 + 249\,d^6 - 468\,d^5 + 608\,d^4 - 528\,d^3 + \\ &\quad 279\,d^2 - 89\,d + 10)\,X - d\,\alpha\,(4\,d^{15} + 32\,d^{14} - 220\,d^{13} + \\ &\quad 700\,d^{12} - 1864\,d^{11} + 4692\,d^{10} - 10072\,d^9 + 16755\,d^8 - 20941\,d^7 + \\ &\quad 19747\,d^6 - 14067\,d^5 + 7441\,d^4 - 2791\,d^3 + 668\,d^2 - 92\,d + 4), \end{aligned}$$

und ist durch $X = X - 2\,d\,(d-1)\,(d^3+d+1)$ isomorph zur obigen elliptischen Kurve in n und z.

Abschließend zum Fall $l = 9$ auch hier die Bemerkung, dass man durch die Transformation $x \mapsto \frac{d^2(d-1)(d^2-d+1)}{x}$, angewandt auf die Polynomfamilie $F_9(x)$, eine Familie $\tilde{F}_9(x)$ erhält, die dieselben Körper wie F_9 erzeugt, deren Gestalt jedoch etwas kompakter ist:

$$\begin{aligned} \tilde{F}_9 &= x^9+(d^3-3d^2-5)\,x^8-(n+(d^3-3d^2-5)\,(d^2+2))\,x^7 + \\ &\quad (2\,(d^2+2)\,n+d^8-4d^7+5d^6-7d^5-4d^4-2d^3-14d^2-10)\,x^6 - \\ &\quad ((d^4+2d^3+4d^2+2d+6)\,n+\beta\,(4d^7-17d^6+24d^5-42d^4+17d^3-12d^2-4d-5))\,x^5 + \\ &\quad ((2d^5+8d^3+6d+4)\,n+\beta\,(d^9-5d^8+23d^7-83d^6+119d^5-134d^4+74d^3-17d^2+2d-1))\,x^4 - \\ &\quad ((d^6+2d^5+8d^3-3d^2+6d+1)\,n+d\,\beta\,(4d^8-20d^7+45d^6-109d^5+149d^4-141d^3+79d^2-17d+3))\,x^3 + \\ &\quad d\,\beta\,((2d^3+2d+2)\,n+\beta\,(d^7-2d^6-6d^5+11d^4-22d^3+21d^2-5d+1))\,x^2 - \\ &\quad n\,d^2\,\beta^2\,x + d^4\,\alpha\beta^3. \end{aligned}$$

Die Diskriminanten der beiden Polynome lauten:

$$\begin{aligned} \mathrm{disc}(F_9) &= d^{100}\,\alpha^{100}\,\beta^{30}\,(-4\,n^3-(d^6-30\,d^5+33\,d^4-34\,d^3+6\,d^2+24\,d+1)\,n^2+ \\ &\quad 6\,d\,(d-1)\,(d^2-d+1)\,(4\,d^7-8\,d^6-24\,d^5+41\,d^4-85\,d^3+84\,d^2-17\,d+4)\,n+ \\ &\quad d\,(d-1)\,(d^2-d+1)^2\,(4\,d^{11}-4\,d^{10}-140\,d^9+588\,d^8-1344\,d^7+2964\,d^6-4020\,d^5+2751\,d^4- \\ &\quad 1023\,d^3+256\,d^2-40\,d+4))^4, \\ \mathrm{disc}(\tilde{F}_9) &= d^{20}\,\alpha^{44}\,\beta^6\,(-4\,n^3-(d^6-30\,d^5+33\,d^4-34\,d^3+6\,d^2+24\,d+1)\,n^2+ \\ &\quad 6\,d\,(d-1)\,(d^2-d+1)\,(4\,d^7-8\,d^6-24\,d^5+41\,d^4-85\,d^3+84\,d^2-17\,d+4)\,n+ \\ &\quad d\,(d-1)\,(d^2-d+1)^2\,(4\,d^{11}-4\,d^{10}-140\,d^9+588\,d^8-1344\,d^7+2964\,d^6-4020\,d^5+2751\,d^4- \\ &\quad 1023\,d^3+256\,d^2-40\,d+4))^4. \end{aligned}$$

B.2 Fall $l = 10$

Die diesem Fall zugrunde liegende elliptische Kurve (siehe auch 1.3.1) lautet

$$E_{10}: \quad y^2 + (\alpha - \beta)\, xy - \alpha\beta d^2\, y \;=\; x^3 - d^2\beta,$$

wobei $\alpha = -(d^2 - 3d + 1)$ und $\beta = d(d-1)(2d-1)$ ist. Der Punkt $A = (0, 0)$ hat die Ordnung 10.

Konstruktion des Polynoms

Die x-Koordinaten der Punkte $P, P \oplus A, P \oplus 2A, \ldots, P \oplus 9A$ lauten:

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{y_P\,\alpha\beta\,d^2}{{x_P}^2}$
$P \oplus 2A$	$\frac{d^2\,\beta\,(-\beta\,y_P+{x_P}^2+\beta\,(2\,d^3-3\,d^2-2\,d+1)\,x_P+d^2\,\alpha\beta^2)}{(x_P-d^2\,\beta)^2}$
$P \oplus 3A$	$\frac{\alpha\beta\,((2\,d-1)\,(d-1)^2\,y_P-(x_P-(2\,d-1)\,(d-1)\,\alpha)\,(d^2\,\beta-x_P))}{(x_P-\alpha\beta)^2}$
$P \oplus 4A$	$\frac{d\,\beta\,(-(d-1)^3\,y_P+{x_P}^2-2\,d^3\,(d-1)\,\alpha\,x_P+d^4\,(d-1)\,\alpha\beta)}{(x_P-d\,\beta)^2}$
$P \oplus 5A$	$\frac{d^3\,(d-1)\,\alpha\,(x_P-d\,\beta)}{(x_P-d^3\,(d-1)\,\alpha)}$
$P \oplus 6A$	$\frac{d\,\beta\,((d-1)^3\,y_P+{x_P}^2-(2\,d-1)\,(d-1)\,(d^2+2\,d-1)\,x_P+d\,\alpha\,\beta^2)}{(x_P-d\,\beta)^2}$
$P \oplus 7A$	$\frac{\alpha\beta\,(-(2\,d-1)\,(d-1)^2\,y_P+{x_P}^2+d\,\beta\,(2\,d^2-5\,d+1)\,x_P+d^2\,\alpha\,\beta^2)}{(x_P+\alpha\beta)^2}$
$P \oplus 8A$	$\frac{d^2\,\beta\,(\beta\,y_P-x_P\,(d^2\,\beta-x_P))}{(x_P-d^2\,\beta)^2}$
$P \oplus 9A$	$\frac{d^2\,\alpha\beta\,(-y_P+(2\,d^3-2\,d^2-2\,d+1)\,x_P+d^2\,\alpha\beta)}{{x_P}^2}$

Es ergibt sich daraus

$$n_{10}=\big({x_P}^{10}-\alpha\beta\,(37\,d^5-53\,d^4+28\,d^3-18\,d^2+8\,d-1)\,{x_P}^8-2\,d\,\alpha\beta(16\,d^7-64\,d^6+22\,d^5+32\,d^4-15\,d^3+13\,d^2-10\,d+2)\,{x_P}^7-d^2(d-1)\,\alpha\beta^2\,(16\,d^{11}-112\,d^{10}+96\,d^9+510\,d^8-765\,d^7+316\,d^6-39\,d^5-27\,d^4+69\,d^3-47\,d^2+12\,d-1)\,{x_P}^6+2\,d^4(d-1)\,\alpha\beta^3\,(24\,d^{10}-168\,d^9+318\,d^8-15\,d^7-357\,d^6+403\,d^5-295\,d^4+171\,d^3-65\,d^2+13\,d-1)\,{x_P}^5+d^5\,(d-1)\,\alpha^2\beta^4\,(54\,d^8-217\,d^7+230\,d^6-237\,d^5+119\,d^4-25\,d^3+11\,d^2-6\,d+1)\,{x_P}^4-2\,d^7\,(d-1)\alpha^3\beta^5\,(2\,d^5-25\,d^4-17\,d^3+8\,d^2+6\,d-2)\,{x_P}^3+2\,d^9(d-1)\,\alpha^4\beta^6\,(d+1)(2\,d^3-6\,d^2-6\,d+3)\,{x_P}^2+4\,d^{11}\,(d-1)\,(d+1)\,\alpha^5\beta^7\,x_P-d^{13}\,(d-1)\alpha^5\beta^8\big)/\big({x_P}^2\,(d^2\,\beta-x_P)^2\,(x_P-\alpha\beta)^2\,(d\,\beta-x_P)^2\,(x_P-d^3\,(d-1)\,\alpha)\big).$$

Das zugehörige Polynom mit Galoisgruppe D_{10} hat die Form

$$
\begin{aligned}
F_{10}(x) \;=\;& x^{10} - n\,x^9 + \\
& d\,(d-1)\,\alpha\,\big(\,(d^4-3\,d^3-15\,d^2+12\,d-2)\,n-(2\,d-1)\,(37\,d^5-53\,d^4+28\,d^3-18\,d^2+8\,d-1)\,\big)\;x^8 + \\
& d(d-1)\,\beta\,\big(\,(12\,d^5-40\,d^4-20\,d^3+38\,d^2-12\,d+1)\,n- \\
& \qquad 2\,d\,(2\,d-1)\,\alpha\,(16\,d^7-64\,d^6+22\,d^5+32\,d^4-15\,d^3+13\,d^2-10\,d+2)\,\big)\;x^7 + \\
& d^2\,(d-1)\,\beta^2\,\big(\,(2\,d^7-12\,d^6-20\,d^5+138\,d^4-67\,d^3-19\,d^2+15\,d-2)\,n- \\
& \qquad \alpha\,(16\,d^{11}-112\,d^{10}+96\,d^9+510\,d^8-765\,d^7+316\,d^6-39\,d^5-27\,d^4+69\,d^3-47\,d^2+12\,d-1)\,\big)\;x^6 - \\
& d^3\,(d-1)\,\beta^3\,\big(\,(12\,d^7-75\,d^6+98\,d^5+87\,d^4-118\,d^3+30\,d^2+2\,d-1)\,n- \\
& \qquad 2d\,\alpha(24\,d^{10}-168\,d^9+318\,d^8-15\,d^7-357\,d^6+403\,d^5-295\,d^4+171\,d^3-65\,d^2+13\,d-1)\,\big)\;x^5 - \\
& d^5\,(d-1)\,\alpha\beta^4\,\big(\,(-d^6+6\,d^5+7\,d^4-54\,d^3+14\,d^2+10\,d-3)\,n- \\
& \qquad \alpha\,(54\,d^8-217\,d^7+230\,d^6-237\,d^5+119\,d^4-25\,d^3+11\,d^2-6\,d+1\,)\;x^4 + \\
& d^7\,(d-1)\,\alpha^2\beta^5\,\big(\,(2\,d^3-6\,d^2-6\,d+3)\,n-2\,\alpha\,(2\,d^5-25\,d^4-17\,d^3+8\,d^2+6\,d-2)\big)\;x^3 + \\
& d^9\,(d-1)\,\alpha^3\beta^6\,\big(\,n+2\,(d+1)\,\alpha\,(2\,d^3-6\,d^2-6\,d+3)\,\big)\;x^2 - \\
& d^{11}\,(d-1)\,\alpha^5\beta^7\,4(d+1)\;x - \\
& d^{13}\,(d-1)\,\alpha^5\beta^8.
\end{aligned}
$$

Die Indikatorfunktion läßt sich hier auf Grund der Größe der Ausdrücke nicht mehr anwenden, aber die Formeln von Vélu (siehe 3.2.3) ergeben die Werte

$$
\begin{aligned}
t \;&=\; d\,(d-1)\,(d^{10}-7\,d^9+83\,d^8-346\,d^7+739\,d^6-935\,d^5+729\,d^4- \\
&\quad\; 352\,d^3+102\,d^2-16\,d+1), \\
w \;&=\; -d^2\,(d-1)^2\,(d^{14}-10\,d^{13}-23\,d^{12}+422\,d^{11}-2268\,d^{10}+7094\,d^9- \\
&\quad\; 14207\,d^8+19086\,d^7-17709\,d^6+11498\,d^5-5207\,d^4+1609\,d^3- \\
&\quad\; 323\,d^2+38\,d-2)
\end{aligned}
$$

und damit die Quotientenkurve $E_{10}/\langle A \rangle$ in der Gestalt

$$
\begin{aligned}
& Y^2+(2\,d^2+2\,d-1-2\,d^3)\,X\,Y+(d^2-3\,d+1)\,(2\,d-1)\,d^3\,(d-1)\,Y = \\
& \quad X^3-(2\,d-1)\,d^3\,(d-1)\,X^2-5\,d\,(d-1)\,(d^{10}-7\,d^9+83\,d^8-346\,d^7+ \\
& \quad 739\,d^6-935\,d^5+729\,d^4-352\,d^3+102\,d^2-16\,d+1)\,X+d\,(d-1) \\
& \quad (3\,d^{16}-33\,d^{15}-543\,d^{14}+5875\,d^{13}-27930\,d^{12}+83206\,d^{11}-170156\,d^{10}+ \\
& \quad 248030\,d^9-263424\,d^8+206431\,d^7-119674\,d^6+50891\,d^5-15541\,d^4+ \\
& \quad 3279\,d^3-446\,d^2+34\,d-1)
\end{aligned}
$$

bzw. in Weierstraß-Form

$$\begin{aligned} Y^2 \;=\;& 4\,X^3 + (4\,d^6 - 16\,d^5 + 8\,d^4 + 8\,d^3 - 4\,d + 1)\,X^2 - 2\,d\,(d-1)\cdot \\ & (10\,d^{10} - 70\,d^9 + 834\,d^8 - 3478\,d^7 + 7410\,d^6 - 9346\,d^5 + 7275\,d^4 - \\ & 3513\,d^3 + 1019\,d^2 - 160\,d + 10)\,X + d\,(d-1)\,(4\,d^6 + 48\,d^5 - \\ & 136\,d^4 + 144\,d^3 - 80\,d^2 + 20\,d - 1)\,(3\,d^{10} - 69\,d^9 + 387\,d^8 - 1223\,d^7 + \\ & 2449\,d^6 - 3099\,d^5 + 2436\,d^4 - 1180\,d^3 + 344\,d^2 - 56\,d + 4). \end{aligned}$$

Zwischen dieser Kurve $E_{10}/\langle A \rangle$ und der entsprechenden Kurve E_{Ind}, die aus der Indikatorfunktion berechnet werden kann, existiert analog zu den Fällen $3 \le l \le 9$ vermutlich ein Isomorphismus

$$\phi \;:\; E_{10}/\langle A \rangle \quad \to \quad E_{Ind}.$$

Da die Indikatorfunktion auf Grund der Größe der Ausdrücke kein Ergebnis liefert, kann weder E_{Ind} noch der Isomorphismus ϕ angegeben werden. Wäre dieser bekannt, könnten Punkte unendlicher Ordnung der Quotientenkurve nach den Ausführungen in Abschnitt 3.2.4 zu Familien zyklischer Zahlkörper führen. Die Quotientenkurve $E_{10}/\langle A \rangle$ besitzt z. B. für $d \in \{-5, -2, -\frac{3}{4}, 9\}$ laut MAGMA [52] den Rang $r = 1$. Erzeuger des unendlichen Teils der Mordell-Weil-Gruppe für $d = 9$ (dieser Kurve in Weierstraß-Form) ist der Punkt $P = (10120095, -31066629000)$. Jedoch erst das Bild $\phi(P) = (n_P, z_P)$ liefert für d und n_P einen zyklischen Zahlkörper (sofern das erzeugende Polynom F_{10} nicht zerfällt).

Zu F_{10} führt $x \mapsto \frac{d^3(d-1)(d^2-3d+1)(2d-1)}{x}$ zu der kompakteren Familie $\tilde{F}_{10}$:

$$\begin{aligned} \tilde{F}_{10} \;=\;& x^{10} + 4\,(d+1)\,\alpha\,x^9 + \left(-n - 2\,(d+1)\,\alpha\,(2d^3 - 6d^2 - 6d + 3)\right)\,x^8 + \\ & \left((2d^3 - 6d^2 - 6d + 3)\,n - 2\,\alpha\,(2d^5 - 25d^4 - 17d^3 + 8d^2 + 6d - 2)\right)\,x^7 + \\ & \left((-d^6 + 6d^5 + 7d^4 - 54d^3 + 14d^2 + 10d - 3)\,n - \alpha\,(54d^8 - 217d^7 + 230d^6 - 237d^5 + 119d^4 - 25d^3 + 11d^2 - 6d + 1)\right)\,x^6 - \\ & \Big((12d^7 - 75d^6 + 98d^5 + 87d^4 - 118d^3 + 30d^2 + 2d - 1)\,n - \\ & \qquad 2\,d\,\alpha\,(24d^{10} - 168d^9 + 318d^8 - 15d^7 - 357d^6 + 403d^5 - 295d^4 + 171d^3 - 65d^2 + 13d - 1)\Big)\,x^5 - \\ & d\,\alpha\,\Big((2d^7 - 12d^6 - 20d^5 + 138d^4 - 67d^3 - 19d^2 + 15d - 2)\,n - \\ & \qquad \alpha\,(16d^{11} - 112d^{10} + 96d^9 + 510d^8 - 765d^7 + 316d^6 - 39d^5 - 27d^4 + 69d^3 - 47d^2 + 12d - 1)\Big)\,x^4 + \\ & d^2\,\alpha^2\left((12d^5 - 40d^4 - 20d^3 + 38d^2 - 12d + 1)\,n - 2\,d\,(2\,d-1)\,\alpha\,(16d^7 - 64d^6 + 22d^5 + 32d^4 - 15d^3 + 13d^2 - 10d + 2)\right)x^3 - \\ & d^4\,\alpha^3\left((-d^4 + 3d^3 + 15d^2 - 12d + 2)\,n - \alpha\,(2\,d-1)\,(37d^5 - 53d^4 + 28d^3 - 18d^2 + 8d - 1)\right)x^2 - \\ & d^6\,n\,(2\,d-1)\,\alpha^4\,x - d^8\,(2\,d-1)\,\alpha^5\beta. \end{aligned}$$

Die Diskriminanten der Polynome $F_{10}(x)$ und $\tilde{F}_{10}(x)$ lauten dazu:

$$\begin{aligned}\mathrm{disc}(F_{10}) &= \alpha^{20}\beta^{68}\,d^{72}\,(d-1)^{72}\,(4\,n-(2\,d-1)\,(32\,d^4-28\,d^3+4\,d^2-10\,d+1))^4\\ &\quad (n^2-4\,\alpha\,d\,(d-1)\,(d^2+4\,d-2)\,n+4\,\alpha^2\beta\,(8\,d^4-9\,d^3+4\,d^2-3\,d+1))^5,\\ \mathrm{disc}(\tilde{F}_{10}) &= \alpha^{20}\beta^{14}\,d^{18}\,(d-1)^{54}\,(4\,n-(2\,d-1)\,(32\,d^4-28\,d^3+4\,d^2-10\,d+1))^4\\ &\quad (n^2-4\,\alpha\,d\,(d-1)\,(d^2+4\,d-2)\,n+4\,\alpha^2\beta\,(8\,d^4-9\,d^3+4\,d^2-3\,d+1))^5.\end{aligned}$$

B.3 Fall $l = 12$

Bei der Konstruktion der Polynomfamilie mit Galoisgruppe D_{12} wird von der allgemeinen Form einer über $\mathbb{Q}$ definierten elliptischen Kurve mit einem Punkt der Ordnung 12 (siehe auch 1.3.1)

$$E_{12} \quad : \quad y^2 + (\alpha^3+\beta)\,xy - \alpha^5\beta\gamma\,y \;=\; x^3 - \alpha^2\beta\gamma\,x^2$$

ausgegangen. Dabei ist $\alpha = (d-1)$ und $\beta = d(2d-1)(3d^2-3d+1)$ und $\gamma = (2d^2-2d+1)$. Der Punkt $A = (0,0)$ hat die Ordnung 12.

Konstruktion des Polynoms

Im Sinne von 3.1.1 ergibt sich:

Punkt	x-Koordinate
P	x_P
$P \oplus A$	$\frac{y_P\,\alpha^5\beta\,\gamma}{{x_P}^2}$
$P \oplus 2A$	$\frac{\alpha^2\beta\,\gamma\,(\beta\,y_P+{x_P}^2+\beta\,(4\,d^4-2\,d^3-5\,d^2+6\,d-2)\,x_P-\alpha^5\beta^2\,\gamma)}{(\alpha^2\beta\,\gamma-x_P)^2}$
$P \oplus 3A$	$\frac{\alpha^3\beta\,(d^2\,(2\,d-1)^2\,y_P-(x_P+d\,(2\,d-1)\,\alpha^5)\,(x_P-\beta\,\gamma\,\alpha^2))}{(\alpha^3\beta+x_P)^2}$
$P \oplus 4A$	$\frac{-\alpha^4\,\gamma\,d\,(2\,d-1)\,(d^3\,(2\,d-1)\,y_P+{x_P}^2+\gamma\,d\,(2\,d-1)\,(d^4+6\,d^3-12\,d^2+8\,d-2)\,x_P-d\,(2\,d-1)\,\alpha^5\beta\,\gamma^2)}{(d\,(2\,d-1)\alpha^4\,\gamma-x_P)^2}$
$P \oplus 5A$	$\frac{\alpha\,\beta\,\gamma\,(d^4\,y_P-(x_P+\alpha^3\beta)\,(x_P-d\,\alpha^3(3\,d^2-3\,d+1)\,\gamma))}{(x_P+\alpha\beta\,\gamma)^2}$
$P \oplus 6A$	$\frac{\alpha^5\,d\,(3\,d^2-3\,d+1)\,(x_P+\alpha\,\beta\,\gamma)}{(x_P-\alpha^5\,d\,(3\,d^2-3\,d+1))}$
$P \oplus 7A$	$\frac{-\alpha\,\beta\,\gamma\,(d^4\,y_P+{x_P}^2+d\,(2\,d-1)\,\gamma\,(7\,d^3-12\,d^2+8\,d-2)\,x_P-\alpha^5\beta\,d(2\,d-1)\,\gamma^2)}{(x_P+\alpha\beta\,\gamma)^2}$
$P \oplus 8A$	$\frac{\alpha^4 d\,(2\,d-1)\,\gamma\,(-d^3\,(2\,d-1)\,y_P+{x_P}^2-\alpha^2 d\,(2\,d-1)\,(4\,d^4-10\,d^3+13\,d^2-8\,d+2)\,x_P-\alpha^7\beta d(2\,d-1)\,\gamma)}{(\alpha^4 d\,(2\,d-1)\,\gamma-x_P)^2}$
$P \oplus 9A$	$\frac{-\alpha^3\beta\,(d^2\,(2\,d-1)^2\,y_P+{x_P}^2+\beta\,(2\,d^4+3\,d^3-9\,d^2+7\,d-2)\,x_P-\alpha^5\beta^2\,\gamma)}{(x_P+\alpha^3\beta)^2}$

Punkt	x-Koordinate
$P \oplus 10A$	$\frac{-\alpha^2\beta\,\gamma\,(\beta\,y_P - x_P\,(x_P - \alpha^2\beta\,\gamma))}{(x_P - \alpha^2\beta\,\gamma)^2}$
$P \oplus 11A$	$\frac{\alpha^5\beta\,\gamma\,(-y_P + (-2\,d^2 + 8\,d^3 - 6\,d^4 - 2\,d + 1)\,x_P + \alpha^5\beta\,\gamma)}{{x_P}^2}$

Aus diesen x-Koordinaten der Punkte $P \oplus iA$ wird die Funktion $n_{12} \in \mathbb{Q}(E_{12})$ in der folgenden Gestalt berechnet:

$$
\begin{aligned}
n_{12} \;=\; & \Big(x^{12} + \\
& \alpha\beta\gamma\,(210\,d^8 - 1120\,d^7 + 2594\,d^6 - 3402\,d^5 + 2731\,d^4 - 1346\,d^3 + \\
& \quad 381\,d^2 - 50\,d + 1)\,x^{10} - \\
& \alpha^3\beta\gamma\,d\,(2\,d - 1)\,2(672\,d^{12} - 7070\,d^{11} + 30718\,d^{10} - 77033\,d^9 + \\
& \quad 126880\,d^8 - 145992\,d^7 + 120751\,d^6 - 72274\,d^5 + 30898\,d^4 - \\
& \quad 9085\,d^3 + 1696\,d^2 - 168\,d + 5)\,x^9 + \\
& \alpha^4\beta^2\gamma\,d\,(2592\,d^{16} - 44496\,d^{15} + 316476\,d^{14} - 1299912\,d^{13} + \\
& \quad 3545532\,d^{12} - 6918297\,d^{11} + 10088565\,d^{10} - 11283930\,d^9 + \\
& \quad 9819012\,d^8 - 6681445\,d^7 + 3543891\,d^6 - 1447428\,d^5 + 444511\,d^4 - \\
& \quad 98487\,d^3 + 14640\,d^2 - 1268\,d + 45)\,x^8 - \\
& \alpha^7\beta^3\gamma^2\,d\,4(144\,d^{15} - 3504\,d^{14} + 30300\,d^{13} - 139924\,d^{12} + 408690\,d^{11} - \\
& \quad 825344\,d^{10} + 1213027\,d^9 - 1336624\,d^8 + 1121394\,d^7 - 719426\,d^6 + \\
& \quad 350772\,d^5 - 127650\,d^4 + 33490\,d^3 - 5950\,d^2 + 634\,d - 30)\,x^7 + \\
& \alpha^9\beta^3\gamma^3\,d^2\,(2\,d - 1)\,(144\,d^{17} - 7032\,d^{16} + 94296\,d^{15} - 615376\,d^{14} + \\
& \quad 2438108\,d^{13} - 6559704\,d^{12} + 12781976\,d^{11} - 18761370\,d^{10} + \\
& \quad 21250770\,d^9 - 18833186\,d^8 + 13134422\,d^7 - 7197578\,d^6 + \\
& \quad 3070892\,d^5 - 1001113\,d^4 + 241276\,d^3 - 40572\,d^2 + 4256\,d - 210)x^6 + \\
& \alpha^{13}\beta^4\gamma^4\,d^2\,(2\,d - 1)\,2(216\,d^{14} - 5004\,d^{13} + 40344\,d^{12} - 171036\,d^{11} + \\
& \quad 456542\,d^{10} - 841122\,d^9 + 1125636\,d^8 - 1125742\,d^7 + 852744\,d^6 - \\
& \quad 489927\,d^5 + 211179\,d^4 - 66492\,d^3 + 14508\,d^2 - 1970\,d + 126)\,x^5 + \\
& \alpha^{16}\beta^5\gamma^4\,d^2\,(2\,d - 1)\,(936\,d^{14} - 14172\,d^{13} + 86460\,d^{12} - 305378\,d^{11} + \\
& \quad 721198\,d^{10} - 1225100\,d^9 + 1558616\,d^8 - 1517880\,d^7 + 1141748\,d^6 - \\
& \quad 662077\,d^5 + 292006\,d^4 - 95158\,d^3 + 21693\,d^2 - 3101\,d + 210)\,x^4 + \\
& \alpha^{24}\beta^6\gamma^5\,d^2\,(2\,d - 1)\,4(108\,d^7 - 558\,d^6 + 1292\,d^5 - 1723\,d^4 + \\
& \quad 1430\,d^3 - 740\,d^2 + 222\,d - 30)\,x^3 +
\end{aligned}
$$

$$
\begin{aligned}
&\alpha^{25}\beta^{7}\gamma^{6}\,d^{2}\,(2\,d-1)\,(6\,d^{4}-32\,d^{3}+50\,d^{2}-34\,d+9)\cdot\\
&\qquad(12\,d^{3}-24\,d^{2}+18\,d-5)\,x^{2}+\\
&\alpha^{30}\beta^{8}\gamma^{7}\,d^{2}\,(2\,d-1)\,2(12\,d^{3}-24\,d^{2}+18\,d-5)\,x-\\
&\alpha^{35}\beta^{9}\gamma^{8}\,d^{2}\,(2\,d-1)\Big)\\
\Big/\ &\Big(x^{2}\,(x-\alpha^{2}\beta\gamma)^{2}\,(x+\alpha^{3}\beta)^{2}\,(x-\alpha^{4}\gamma\,d\,(2\,d-1))^{2}\,(x+\alpha\beta\gamma)^{2}\cdot\\
&(x-\alpha^{5}\,d\,(3\,d^{2}-3\,d+1))\Big).
\end{aligned}
$$

Das zugehörige Polynom mit Galoisgruppe D_{12} lautet:

$$
\begin{aligned}
F_{12}(x) \;=\;& x^{12}-n\,x^{11}+\\
&\alpha\,\big(\,d\,(35\,d^{6}-171\,d^{5}+329\,d^{4}-340\,d^{3}+201\,d^{2}-65\,d+9)\,n+\\
&\qquad\beta\gamma\,(210\,d^{8}-1120\,d^{7}+2594\,d^{6}-3402\,d^{5}+2731\,d^{4}-1346\,d^{3}+381\,d^{2}-50\,d+1)\,\big)\;x^{10}\;-\\
&\alpha^{2}\,d\,(2\,d-1)\,\big(\,d\,(224\,d^{11}-2282\,d^{10}+9786\,d^{9}-24317\,d^{8}+39724\,d^{7}-45307\,d^{6}+37074\,d^{5}-\\
&\qquad21868\,d^{4}+9144\,d^{3}-2589\,d^{2}+448\,d-36)\,n+\\
&\qquad\alpha\beta\gamma\,2(672\,d^{1}2-7070\,d^{1}1+30718\,d^{1}0-77033\,d^{9}+126880\,d^{8}-145992\,d^{7}+\\
&\qquad120751\,d^{6}-72274\,d^{5}+30898\,d^{4}-9085\,d^{3}+1696\,d^{2}-168\,d+5)\,\big)\;x^{9}\;+\\
&\alpha^{4}\beta\,d\,\big(\,d\,(2\,d-1)\,(216\,d^{13}-3312\,d^{12}+20121\,d^{11}-69177\,d^{10}+155808\,d^{9}-247644\,d^{8}+289203\,d^{7}-\\
&\qquad253221\,d^{6}+167149\,d^{5}-82493\,d^{4}+29687\,d^{3}-7399\,d^{2}+1148\,d-84)\,n+\\
&\qquad\beta\gamma\,(2592\,d^{16}-44496\,d^{15}+316476\,d^{14}-1299912\,d^{13}+3545532\,d^{12}-6918297\,d^{11}+\\
&\qquad10088565\,d^{10}-11283930\,d^{9}+9819012\,d^{8}-6681445\,d^{7}+3543891\,d^{6}-1447428\,d^{5}+\\
&\qquad444511\,d^{4}-98487\,d^{3}+14640\,d^{2}-1268\,d+45)\,\big)\;x^{8}\;-\\
&\alpha^{6}\beta^{2}\gamma\,d\,\big(\,d\,(2\,d-1)\,(48\,d^{13}-1128\,d^{12}+9160\,d^{11}-39012\,d^{10}+104080\,d^{9}-190328\,d^{8}+250562\,d^{7}-\\
&\qquad243603\,d^{6}+176472\,d^{5}-94691\,d^{4}+36764\,d^{3}-9821\,d^{2}+1624\,d-126)\,n+\\
&\qquad4\,\alpha\beta\gamma\,(144\,d^{15}-3504\,d^{14}+30300\,d^{13}-139924\,d^{12}+408690\,d^{11}-825344\,d^{10}+1213027\,d^{9}-\\
&\qquad1336624\,d^{8}+1121394\,d^{7}-719426\,d^{6}+350772\,d^{5}-127650\,d^{4}+33490\,d^{3}-5950\,d^{2}+634\,d-30)\,\big)\;x^{7}+\\
&\alpha^{9}\beta^{3}\gamma^{2}\,d^{2}\,(2\,d-1)\,\big(\,(4\,d^{12}-184\,d^{11}+2086\,d^{10}-10626\,d^{9}+31109\,d^{8}-59068\,d^{7}+77414\,d^{6}-72158\,d^{5}+\\
&\qquad48172\,d^{4}-22694\,d^{3}+7217\,d^{2}-1400\,d+126)\,n+\\
&\qquad\gamma\,(144\,d^{17}-7032\,d^{16}+94296\,d^{15}-615376\,d^{14}+2438108\,d^{13}-6559704\,d^{12}+12781976\,d^{11}-\\
&\qquad18761370\,d^{10}+21250770\,d^{9}-18833186\,d^{8}+13134422\,d^{7}-7197578\,d^{6}+3070892\,d^{5}-1001113\,d^{4}+\\
&\qquad241276\,d^{3}-40572\,d^{2}+4256\,d-210)\,\big)\;x^{6}\;+\\
&\alpha^{12}\beta^{4}\gamma^{3}\,d^{2}\,(2\,d-1)\,\big(\,(12\,d^{10}-256\,d^{9}+1758\,d^{8}-5978\,d^{7}+12099\,d^{6}-15912\,d^{5}+14121\,d^{4}-8484\,d^{3}+\\
&\qquad3339\,d^{2}-784\,d+84)\,n+\\
&\qquad2\,\alpha\gamma\,(216\,d^{14}-5004\,d^{13}+40344\,d^{12}-171036\,d^{11}+456542\,d^{10}-841122\,d^{9}+1125636\,d^{8}-
\end{aligned}
$$

$$1125742\,d^7+852744\,d^6-489927\,d^5+211179\,d^4-66492\,d^3+14508\,d^2 1970\,d+126)\Big)\,x^5+$$
$$\alpha^{16}\beta^5\gamma^4\,d^2\,(2\,d-1)\Big((13\,d^7-147\,d^6+555\,d^5-1027\,d^4+1085\,d^3-677\,d^2+236\,d-36)\,n+$$
$$(936\,d^{14}-14172\,d^{13}+86460\,d^{12}-305378\,d^{11}+721198\,d^{10}-1225100\,d^9+1558616\,d^8-$$
$$1517880\,d^7+1141748\,d^6-662077\,d^5+292006\,d^4-95158\,d^3+21693\,d^2-3101\,d+210)\Big)\,x^4+$$
$$\alpha^{20}\beta^6\gamma^5\,d^2\,(2\,d-1)\Big((6\,d^4-32\,d^3+50\,d^2-34\,d+9)\,n+$$
$$(\alpha^4\,4\,(108\,d^7-558\,d^6+1292\,d^5-1723\,d^4+1430\,d^3-740\,d^2+222\,d-30))\,\alpha^{25}\alpha^{25}\Big)\,x^3+$$
$$\alpha^{25}\beta^7\gamma^6\,d^2\,(2\,d-1)\Big(n+(6\,d^4-32\,d^3+50\,d^2-34\,d+9)\,(12\,d^3-24\,d^2+18\,d-5)\Big)\,x^2+$$
$$\alpha^{30}\beta^8\gamma^7\,d^2\,(2\,d-1)\Big(2(12\,d^3-24\,d^2+18\,d-5)\Big)\,x-$$
$$\alpha^{35}\beta^9\gamma^8\,d^2\,(2\,d-1).$$

Wie im Fall $l = 10$ liefert die Indikatorfunktion kein Ergebnis. Bei der Berechnung der Quotientenkurve nach Vélu erhält man:

$$\begin{aligned} t &= d\,(d-1)\,(777\,d^{14}-5439\,d^{13}+17859\,d^{12}-36447\,d^{11}+51590\,d^{10}-\\ &\quad 53482\,d^9+41663\,d^8-24455\,d^7+10532\,d^6-3044\,d^5+402\,d^4+\\ &\quad 89\,d^3-57\,d^2+12\,d-1) \end{aligned}$$

$$\begin{aligned} w &= (14107\,d^{20}-145732\,d^{19}+721\alpha^{25}425\,d^{18}-2275677\,d^{17}+5129019\,d^{16}-\\ &\quad 8776041\,d^{15}+11824964\,d^{14}-12851151\,d^{13}+11455166\,d^{12}-8480878\,d^{11}+\\ &\quad 5268773\,d^{10}-2771321\,d^9+1243704\,d^8-478685\,d^7+157962\,d^6-\\ &\quad 44246\,d^5+10269\,d^4-1892\,d^3+258\,d^2-23\,d+1)\,(d-1)^2\,d^2. \end{aligned}$$

t und w führen zur Quotientenkurve in der folgenden Gestalt:

$$\begin{aligned} &Y^2+\Big((d-1)^3-(2\,d-1)\,d\,(3\,d-3\,d^2-1)\Big)\,X\,Y-\\ &(d-1)^5\,(2\,d-1)\,d\,(3\,d-3\,d^2-1)\,(2\,d-2\,d^2-1)\,Y=\\ &\quad X^3-(d-1)^2\,(2\,d-1)\,d\,(3\,d-3\,d^2-1)\,(2\,d-2\,d^2-1)\,X^2-\\ &\quad 5\,d\,(d-1)\Big(777\,d^{14}-5439\,d^{13}+17859\,d^{12}-36447\,d^{11}+51590\,d^{10}-\\ &\quad 53482\,d^9+41663\,d^8-24455\,d^7+10532\,d^6-3044\,d^5+402\,d^4+89\,d^3-\\ &\quad 57\,d^2+12\,d-1\Big)\,X-\\ &\quad d\,(d-1)\Big(89425\,d^{22}-960365\,d^{21}+4942039\,d^{20}-16208130\,d^{19}+\\ &\quad 38005032\,d^{18}-67744788\,d^{17}+95312531\,d^{16}-108571313\,d^{15}+\\ &\quad 102098168\,d^{14}-80667699\,d^{13}+54570768\,d^{12}-32296177\,d^{11}+\\ &\quad 17082253\,d^{10}-8176833\,d^9+3520360\,d^8-1326727\,d^7+419773\,d^6-\\ &\quad 105883\,d^5+19892\,d^4-2478\,d^3+147\,d^2+5\,d-1). \end{aligned}$$

Diese besitzt die Weierstraß-Form

$$\begin{aligned} Y^2 \;=\;& 4\,X^3 - (12\,d^8 - 120\,d^7 + 336\,d^6 - 468\,d^5 + 372\,d^4 - 168\,d^3 + 36\,d^2 - 1)\,X^2 - \\ & 2d\,(d-1)\,(7770\,d^{14} - 54318\,d^{13} + 178026\,d^{12} - 362466\,d^{11} + 511650\,d^{10} - \\ & 528894\,d^9 + 411048\,d^8 - 241140\,d^7 + 104275\,d^6 - 30675\,d^5 + 4465\,d^4 + \\ & 646\,d^3 - 495\,d^2 + 107\,d - 9)\,X - d\,(d-1)\,(292\,d^8 - 1192\,d^7 + 2128\,d^6 - \\ & 2172\,d^5 + 1372\,d^4 - 536\,d^3 + 116\,d^2 - 8\,d - 1)\,(1225\,d^{14} - 8155\,d^{13} + \\ & 25481\,d^{12} - 49461\,d^{11} + 66549\,d^{10} - 65595\,d^9 + 49234\,d^8 - 29534\,d^7 + \\ & 15295\,d^6 - 7393\,d^5 + 3301\,d^4 - 1217\,d^3 + 323\,d^2 - 53\,d + 4). \end{aligned}$$

Die Transformation $x \mapsto \frac{d\,(2\,d^2-2\,d+1)\,(3\,d^2-3\,d+1)\,(2\,d-1)\,(d-1)^5}{x}$ vereinfacht F_{12} zu

$$\begin{aligned} \tilde{F}_{12} \;=\;& x^{12} - (24\,d^3-48\,d^2+36\,d-10)\,x^{11} - (n+(6\,d^4-32\,d^3+50\,d^2-34\,d+9)\,(12\,d^3-24\,d^2+18\,d-5))\,x^{10} - \\ & ((6\,d^4-32\,d^3+50\,d^2-34\,d+9)\,n+4\,\alpha^4\,(108\,d^7-558\,d^6+1292\,d^5-1723\,d^4+1430\,d^3-740\,d^2+222\,d-30))\,x^9 \\ & -(d-1)\,((13\,d^7-147\,d^6+555\,d^5-1027\,d^4+1085\,d^3-677\,d^2+236\,d-36)\,n+ \\ & (936\,d^{14}-14172\,d^{13}+86460\,d^{12}-305378\,d^{11}+721198\,d^{10}-1225100\,d^9+ \\ & 1558616\,d^8-1517880\,d^7+1141748\,d^6-662077\,d^5+292006\,d^4-95158\,d^3+21693\,d^2-3101\,d+210))\,x^8 - \\ & \alpha^2\,((12\,d^{10}-256\,d^9+1758\,d^8-5978\,d^7+12099\,d^6-15912\,d^5+14121\,d^4-8484\,d^3+3339\,d^2-784\,d+84)\,n+ \\ & 2\,\alpha\,\gamma\,(216\,d^{14}-5004\,d^{13}+40344\,d^{12}-171036\,d^{11}+ \\ & 456542\,d^{10}-841122\,d^9+1125636\,d^8-1125742\,d^7+852744\,d^6-489927\,d^5+211179\,d^4-66492\,d^3+ \\ & 14508\,d^2-1970\,d+126))\,x^7 - \\ & \alpha^4\,((4\,d^{12}-184\,d^{11}+2086\,d^{10}-10626\,d^9+31109\,d^8-59068\,d^7+77414\,d^6- \\ & 72158\,d^5+48172\,d^4-22694\,d^3+7217\,d^2-1400\,d+126)\,n+\gamma \\ & (144\,d^{17}-7032\,d^{16}+94296\,d^{15}-615376\,d^{14}+2438108\,d^{13}-6559704\,d^{12}+ \\ & 12781976\,d^{11}-18761370\,d^{10}+21250770\,d^9-18833186\,d^8+13134422\,d^7-7197578\,d^6+3070892\,d^5- \\ & 1001113\,d^4+241276\,d^3-40572\,d^2+4256\,d-210))\,x^6 + \\ & \alpha^6\,((48\,d^{13}-1128\,d^{12}+9160\,d^{11}-39012\,d^{10}+104080\,d^9-190328\,d^8+250562\,d^7- \\ & 243603\,d^6+176472\,d^5-94691\,d^4+36764\,d^3-9821\,d^2+1624\,d-126)\,n+4\,\alpha \\ & (144\,d^{15}-3504\,d^{14}+30300\,d^{13}-139924\,d^{12}+408690\,d^{11}-825344\,d^{10}+ \\ & 1213027\,d^9-1336624\,d^8+1121394\,d^7-719426\,d^6+350772\,d^5-127650\,d^4+33490\,d^3- \\ & 5950\,d^2+634\,d-30)\,(3\,d^2-3\,d+1)\,\gamma))\,x^5 - \\ & \alpha^9\,((216\,d^{13}-3312\,d^{12}+20121\,d^{11}-69177\,d^{10}+155808\,d^9-247644\,d^8+289203\,d^7-253221\,d^6+ \\ & 167149\,d^5-82493\,d^4+29687\,d^3-7399\,d^2+1148\,d-84)\,n+\gamma\,(3\,d^2-3\,d+1)\,(2592\,d^{16}-44496\,d^{15}+316476\,d^{14}- \\ & 1299912\,d^{13}+3545532\,d^{12}-6918297\,d^{11}+10088565\,d^{10}-11283930\,d^9+ \end{aligned}$$

$$
\begin{aligned}
&9819012\,d^8-6681445\,d^7+3543891\,d^6-1447428\,d^5+444511\,d^4-98487\,d^3+14640\,d^2-\\
&1268\,d+45))\,x^4+\\
&\alpha^{12}\,\gamma\,((224\,d^{11}-2282\,d^{10}+9786\,d^9-24317\,d^8+39724\,d^7-45307\,d^6+37074\,d^5-\\
&21868\,d^4+9144\,d^3-2589\,d^2+448\,d-36)\,n+2\,\alpha\,(2\,d-1)\,(3\,d^2-3\,d+1)\,(672\,d^{12}-7070\,d^{11}+30718\,d^{10}-77033\,d^9+\\
&126880\,d^8-145992\,d^7+120751\,d^6-72274\,d^5+30898\,d^4-9085\,d^3+1696\,d^2-168\,d+5)\,\gamma)\,x^3-\\
&(3\,d^2-3\,d+1)\,\gamma^2\,\alpha^{16}\,((35\,d^6-171\,d^5+329\,d^4-340\,d^3+\\
&201\,d^2-65\,d+9)\,n+(2\,d-1)\,(3\,d^2-3\,d+1)\,\gamma\,(210\,d^8-1120\,d^7+2594\,d^6-\\
&3402\,d^5+2731\,d^4-1346\,d^3+381\,d^2-50\,d+1))\,x^2+\\
&n\,(2\,d-1)\,(3\,d^2-3\,d+1)^2\,\gamma^3\,\alpha^{20}\,x-\alpha^{25}\beta\gamma^4\,(3\,d^2-3\,d+1)^2\,(2\,d-1).
\end{aligned}
$$

Die Diskriminanten der beiden Polynome berechnen sich zu:

$$
\begin{aligned}
\operatorname{disc}(F_{12}) &= d^{250}\,(2\,d^2-2\,d+1)^{56}\,(3\,d^2-3\,d+1)^{78}\,(2\,d-1)^{122}\,(d-1)^{250}\\
&\quad (4\,n-(2\,d^2-2\,d+1)\,(216\,d^6-792\,d^5+1164\,d^4-864\,d^3+322\,d^2-46\,d-1))^5\\
&\quad (n^2+8\,d\,(d-1)\,(2\,d-1)\,(3\,d^2-3\,d+1)\,(3\,d^2-4\,d+2)\,n+4\,d\,(d-1)\,(2\,d^2-2\,d+1)\\
&\quad (18\,d^4-48\,d^3+47\,d^2-17\,d+1)\,(2\,d-1)^2\,(3\,d^2-3\,d+1)^2)^6,\\
\operatorname{disc}(\tilde{F}_{12}) &= d^{140}\,(3\,d^2-3\,d+1)^{12}\,(2\,d^2-2\,d+1)^{12}\,(2\,d-1)^{34}\,(d-1)^{140}\\
&\quad (4\,n-(2\,d^2-2\,d+1)\,(216\,d^6-792\,d^5+1164\,d^4-864\,d^3+322\,d^2-46\,d-1))^5\\
&\quad (n^2+8\,d\,(d-1)\,(2\,d-1)\,(3\,d^2-4\,d+2)\,(3\,d^2-3\,d+1)\,n+4\,d\,(d-1)\,(2\,d^2-2\,d+1)\\
&\quad (18\,d^4-48\,d^3+47\,d^2-17\,d+1)\,(2\,d-1)^2\,(3\,d^2-3\,d+1)^2)^6.
\end{aligned}
$$

Polynomfamilie $H_{12}(x)$ mit Galoisgruppe $D_{12/2}$

In Abschnitt 3.3 wurden für gerade l auch die Unterfamilien mit Galoisgruppe $D_{l/2}$ berechnet. Die Berechnung liefert für $l = 12$ die folgende Polynomfamilie:

$$
\begin{aligned}
H_{12}(x) = x^{12} &-2\,(12\,d^3-24\,d^2+18\,d-5)\,x^{11}-\\
&(t\,(t+1)+108\,d^8-432\,d^7+504\,d^6+264\,d^5-1330\,d^4+1584\,d^3-975\,d^2+321\,d-45)\,x^{10}-\\
&\big((6\,d^4-32\,d^3+50\,d^2-34\,d+9)\,t\,(t+1)\\
&\quad +(d-1)(648\,d^{11}-5400\,d^{10}+18360\,d^9-34120\,d^8+36992\,d^7-20264\,d^6-2246\,d^5\\
&\quad +13212\,d^4-10934\,d^3+4782\,d^2-1149\,d+120)\big)\,x^9-\\
&(d-1)\,\big((13\,d^7-147\,d^6+555\,d^5-1027\,d^4+1085\,d^3-677\,d^2+236\,d-36)\,t\,(t+1)\\
&\quad +1404\,d^{15}-21492\,d^{14}+133272\,d^{13}-471636\,d^{12}+1091826\,d^{11}-1766430\,d^{10}+2056799\,d^9\\
&\quad -1723052\,d^8+993062\,d^7-325790\,d^6-15969\,d^5+84116\,d^4-49003\,d^3+15389\,d^2-2705\,d+210\big)\,x^8-
\end{aligned}
$$

$$
\begin{aligned}
&(d-1)^2\Big((12\,d^{10}-256\,d^9+1758\,d^8-5978\,d^7+12099\,d^6-15912\,d^5+14121\,d^4-8484\,d^3+3339\,d^2-784\,d+84)\\
&\quad\cdot t\,(t+1)+(d-1)\,(1296\,d^{17}-31536\,d^{16}+277992\,d^{15}-1329696\,d^{14}+4087692\,d^{13}-8813268\,d^{12}\\
&\quad+13996932\,d^{11}-16822904\,d^{10}+15474594\,d^9-10850982\,d^8+5654017\,d^7-2032476\,d^6+378741\,d^5\\
&\quad+55990\,d^4-64167\,d^3+21048\,d^2-3520\,d+252)\Big)\;x^7\;-\\
&(d-1)^4\Big((4\,d^{12}-184\,d^{11}+2086\,d^{10}-10626\,d^9+31109\,d^8-59068\,d^7+77414\,d^6-72158\,d^5+48172\,d^4\\
&\quad-22694\,d^3+7217\,d^2-1400\,d+126)\,t\,(t+1)\\
&\quad+432\,d^{20}-21600\,d^{19}+307800\,d^{18}-2190888\,d^{17}+9668196\,d^{16}-29515536\,d^{15}+66421220\,d^{14}\\
&\quad-114597316\,d^{13}+155373114\,d^{12}-167993344\,d^{11}+145839219\,d^{10}-101586729\,d^9+56245732\,d^8\\
&\quad-24198070\,d^7+7698126\,d^6-1588816\,d^5+99560\,d^4+56945\,d^3-21126\,d^2+3290\,d-210\Big)\;x^6\;+\\
&(d-1)^6\Big((48\,d^{13}-1128\,d^{12}+9160\,d^{11}-39012\,d^{10}+104080\,d^9-190328\,d^8+250562\,d^7-243603\,d^6\\
&\quad+176472\,d^5-94691\,d^4+36764\,d^3-9821\,d^2+1624\,d-126)\,t\,(t+1)\\
&\quad+(d-1)\,(5184\,d^{20}-137376\,d^{19}+1375488\,d^{18}-7683984\,d^{17}+28210032\,d^{16}-74281968\,d^{15}\\
&\quad+147819912\,d^{14}-229769988\,d^{13}+284905724\,d^{12}-285404040\,d^{11}+232381312\,d^{10}-153788696\,d^9\\
&\quad+82179686\,d^8-34919793\,d^7+11455668\,d^6-2733853\,d^5+407352\,d^4-13951\,d^3-8344\,d^2+1750\,d-120)\Big)\;x^5\;-\\
&(d-1)^9\Big((216\,d^{13}-3312\,d^{12}+20121\,d^{11}-69177\,d^{10}+155808\,d^9-247644\,d^8+289203\,d^7-253221\,d^6\\
&\quad+167149\,d^5-82493\,d^4+29687\,d^3-7399\,d^2+1148\,d-84)\,t\,(t+1)\\
&\quad+23328\,d^{21}-451008\,d^{20}+3767148\,d^{19}-18830556\,d^{18}+64562832\,d^{17}-163485864\,d^{16}+319834818\,d^{15}\\
&\quad-497690622\,d^{14}+627896268\,d^{13}-650145042\,d^{12}+556305345\,d^{11}-394270455\,d^{10}+230945544\,d^9\\
&\quad-111005244\,d^8+43189284\,d^7-13288662\,d^6+3104796\,d^5-508638\,d^4+47058\,d^3+195\,d^2-569\,d+45\Big)\;x^4\;+\\
&(d-1)^{12}\,(2\,d^2-2\,d+1)\Big((224\,d^{11}-2282\,d^{10}+9786\,d^9-24317\,d^8+39724\,d^7-45307\,d^6+37074\,d^5-21868\,d^4\\
&\quad+9144\,d^3-2589\,d^2+448\,d-36)\,t\,(t+1)\\
&\quad+(d-1)\,(24192\,d^{18}-319032\,d^{17}+1893024\,d^{16}-6874740\,d^{15}+17326188\,d^{14}-32387400\,d^{13}\\
&\quad+46697784\,d^{12}-53189412\,d^{11}+48527028\,d^{10}-35688849\,d^9+21153438\,d^8-10034499\,d^7\\
&\quad+3751844\,d^6-1075934\,d^5+225550\,d^4-31473\,d^3+2286\,d^2+10\,d-10)\Big)\;x^3\;-\\
&(2\,d^2-2\,d+1)^2\,(3\,d^2-3\,d+1)\,(d-1)^{16}\Big((35\,d^6-171\,d^5+329\,d^4-340\,d^3+201\,d^2-65\,d+9)\,t\,(t+1)\\
&\quad+3780\,d^{14}-33588\,d^{13}+138096\,d^{12}-349560\,d^{11}+609654\,d^{10}-775098\,d^9+739811\,d^8\\
&\quad-536860\,d^7+295967\,d^6-122156\,d^5+36515\,d^4-7409\,d^3+890\,d^2-42\,d-1\Big)\;x^2\;+\\
&(2\,d-1)\,(3\,d^2-3\,d+1)^2\,(2\,d^2-2\,d+1)^3\,(d-1)^{20}\\
&\quad\cdot\Big(t\,(t+1)+108\,d^8-504\,d^7+1032\,d^6-1212\,d^5+884\,d^4-400\,d^3+103\,d^2-11\,d\Big)\;x\;-\\
&d\,(2\,d-1)^2\,(3\,d^2-3\,d+1)^3\,(2\,d^2-2\,d+1)^4\,(d-1)^{25}.
\end{aligned}
$$

Anhang C

Exakte Formeln zur Arithmetik im Grad 5

In Abschnitt 3.1.2 wurde die Polynomfamilie $F_5(x)$ mit Galoisgruppe D_l konstruiert. Die von dieser erzeugte, parametrisierte Zahlkörperfamilie wurde in Abschnitt 3.1.4 im Hinblick auf parametrisierte Fundamentaleinheiten untersucht. Dabei wurde in den Fällen $n < -4$ in Lemma 3.1.22 die Lage der komplexen Nullstellen $\rho^{(2)} = \overline{\rho^{(3)}}$ und $\rho^{(4)} = \overline{\rho^{(5)}}$ von $F_5(x)$ mit Hilfe eines Satzes von Obreschkoff bestimmt. Anstatt

$$F_5(x) = x^5 - n\,x^4 + (2\,n - 1)\,x^3 - (n - 2)\,x^2 - 2\,x + 1$$

wurde nach Substitution $n \mapsto -n$ das Polynom

$$f(x) = x^5 + n\,x^4 - (2\,n + 1)\,x^3 + (n + 2)\,x^2 - 2\,x + 1$$

und dessen Nullstellen $\varrho^{(1)}, \ldots, \varrho^{(5)}$ untersucht. Dabei wurde mit Hilfe der komplexen Zahlen α und $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ ein Kreis C um eine (komplexe) Nullstelle $\varrho^{(i)}$ (für $i = 2, 4$) von $f(x)$ gelegt. Um C wurde ein Quadrat mit den Ecken $E_1, \ldots, E_4$ bzw. $R_1, \ldots, R_4$ konstruiert, die untere und obere Schranken der Nullstellenbeträge lieferten.

Bei dieser Eckenkonstruktion traten umfangreiche parametrisierte Ausdrücke auf, die in Abschnitt 3.1.22 nur verkürzt wiedergegeben wurden. Die folgenden Ausführungen dienen dazu, diese exakt anzugeben.

C.1 Nullstelle $\varrho^{(2)}$

Durch Beispielrechnungen wurde festgestellt, dass die komplexe Zahl

$$\alpha = \frac{1}{2\,n^2} + \frac{1}{\sqrt{n}}\,i$$

dicht bei einer Nullstelle von $f(x)$ liegt. Einsetzen von α in $f(x)$ und $f'(x)$ liefert für den Realteil von $\frac{5f(\alpha)}{f'(\alpha)}$ den Ausdruck

$$\frac{5\,(96\,n^{16}-16\,n^{15}+48\,n^{14}-120\,n^{13}+78\,n^{12}+27\,n^{11}-16\,n^{10}+78\,n^9-20\,n^8-6\,n^7+26\,n^6-2\,n^5-n^4+\frac{49}{16}\,n^3+\frac{5}{32})}{n^2\,(64\,n^{17}+256\,n^{16}+128\,n^{15}+192\,n^{14}+64\,n^{13}+304\,n^{12}+448\,n^{11}-52\,n^{10}+596\,n^9-95\,n^8-32\,n^7+234\,n^6-15\,n^5-\frac{15}{2}\,n^4+30\,n^3+\frac{25}{16})}$$

und als Imaginärteil den Quotienten

$$\frac{5\,(32\,n^{16}+64\,n^{15}+40\,n^{14}+96\,n^{13}-16\,n^{12}+208\,n^{11}-58\,n^{10}+76\,n^9+17\,n^8-4\,n^7+41\,n^6-2\,n^5-n^4+6\,n^3+\frac{5}{16})}{\sqrt{n}\,(64\,n^{17}+256\,n^{16}+128\,n^{15}+192\,n^{14}+64\,n^{13}+304\,n^{12}+448\,n^{11}-52\,n^{10}+596\,n^9-95\,n^8-32\,n^7+234\,n^6-15\,n^5-\frac{15}{2}\,n^4+30\,n^3+\frac{25}{16})}.$$

Der Betrag zum Quadrat $|\frac{5f(\alpha)}{f'(\alpha)}|^2$ dieser Zahl errechnet sich zu

$$\frac{25\,(128\,n^{18}+576\,n^{16}-128\,n^{15}+456\,n^{14}-352\,n^{13}+192\,n^{12}+80\,n^{11}-28\,n^{10}+136\,n^9-26\,n^8-8\,n^7+\frac{65}{2}\,n^6-2\,n^5-n^4+3\,n^3+\frac{1}{8})}{4\,n^4\,(128\,n^{17}+512\,n^{16}+256\,n^{15}+384\,n^{14}+128\,n^{13}+608\,n^{12}+896\,n^{11}-104\,n^{10}+1192\,n^9-190\,n^8-64\,n^7+468\,n^6-30\,n^5-15\,n^4+60\,n^3+\frac{25}{8})}.$$

Der Realteil des neben α zweiten kreisbestimmenden Punktes $\alpha-\frac{5f(\alpha)}{f'(\alpha)}$ lautet

$$\frac{n\,(64\,n^{14}-704\,n^{13}+288\,n^{12}-288\,n^{11}+1264\,n^{10}-476\,n^9+178\,n^8+108\,n^7-184\,n^6+105\,n^5+28\,n^4-26\,n^3+5\,n^2+\frac{5}{2}\,n-\frac{5}{8})}{2\,(64\,n^{17}+256\,n^{16}+128\,n^{15}+192\,n^{14}+64\,n^{13}+304\,n^{12}+448\,n^{11}-52\,n^{10}+596\,n^9-95\,n^8-32\,n^7+234\,n^6-15\,n^5-\frac{15}{2}\,n^4+30\,n^3+\frac{25}{16})}$$

und der Imaginärteil

$$\frac{n^{3,5}\,(64\,n^{13}+96\,n^{12}-192\,n^{11}-8\,n^{10}-416\,n^9+384\,n^8-592\,n^7+238\,n^6+216\,n^5-180\,n^4-12\,n^3+29\,n^2-5\,n-\frac{5}{2})}{64\,n^{17}+256\,n^{16}+128\,n^{15}+192\,n^{14}+64\,n^{13}+304\,n^{12}+448\,n^{11}-52\,n^{10}+596\,n^9-95\,n^8-32\,n^7+234\,n^6-15\,n^5-\frac{15}{2}\,n^4+30\,n^3+\frac{25}{16}}.$$

Aus den beiden Zahlen α und $\alpha-\frac{5f(\alpha)}{f'(\alpha)}$ wurde der Kreis C mit exaktem Durchmesser $\frac{5f(\alpha)}{f'(\alpha)}$ konstruiert. Ausgehend von dessen Mittelpunkt $\alpha-\frac{5f(\alpha)}{2f'(\alpha)}$ wurde über eine obere Abschätzung des Kreisradius durch $\frac{5}{4\sqrt{n}(n+1)}$, die für alle $n>2$ richtig ist, ein den Kreis umfassendes Quadrat gelegt, dessen Ecken durch die folgenden exakten Formeln beschrieben sind:

$$E_1 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\,i \quad \text{mit}$$

$$\begin{aligned} numer_{Re} \;=\; & -5120\,n^{18,5}+2048\,n^{18}-20480\,n^{17,5}-5120\,n^{17}-10240\,n^{16,5}-512\,n^{16}-15360\,n^{15,5}+5120\,n^{15} \\ & -5120\,n^{14,5}+19712\,n^{14}-24320\,n^{13,5}+18496\,n^{13}-35840\,n^{12,5}+7264\,n^{12}+4160\,n^{11,5}+10912\,n^{11} \end{aligned}$$

$$
\begin{aligned}
& -47680\,n^{10,5}+7488\,n^{10}+7600\,n^{9,5}+6752\,n^{9}+2560\,n^{8,5}+96\,n^{8}-18720\,n^{7,5}+3264\,n^{7}+1200\,n^{6,5} \\
& +3168\,n^{6}+600\,n^{5,5}-240\,n^{5}-2400\,n^{4,5}+390\,n^{4}+470\,n^{3}-125\,n^{1,5}+25\,n+25, \\
denom_{Re} &= 4\,n^{2}\,(1024\,n^{18}+5120\,n^{17}+6144\,n^{16}+5120\,n^{15}+4096\,n^{14}+5888\,n^{13}+12032\,n^{12}+6336\,n^{11} \\
& +8704\,n^{10}+8016\,n^{9}-2032\,n^{8}+3232\,n^{7}+3504\,n^{6}-360\,n^{5}+360\,n^{4}+480\,n^{3}+25\,n+25), \\
numer_{Im} &= 4096\,n^{18}+20480\,n^{17}+29696\,n^{16}+14080\,n^{15}+9984\,n^{14}+15872\,n^{13}+41728\,n^{12}+37184\,n^{11} \\
& +27776\,n^{10}+64864\,n^{9}-17808\,n^{8}+4448\,n^{7}+26496\,n^{6}-2160\,n^{5}+40\,n^{4}+3360\,n^{3}+50\,n+175, \\
denom_{Im} &= 4\,\sqrt{n}\,(n+1)\,(1024\,n^{17}+4096\,n^{16}+2048\,n^{15}+3072\,n^{14}+1024\,n^{13}+4864\,n^{12}+7168\,n^{11}-832\,n^{10} \\
& +9536\,n^{9}-1520\,n^{8}-512\,n^{7}+3744\,n^{6}-240\,n^{5}-120\,n^{4}+480\,n^{3}+25).
\end{aligned}
$$

$$E_2 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\,i \quad \text{mit}$$

$$
\begin{aligned}
numer_{Re} &= 5120\,n^{18,5}+2048\,n^{18}+20480\,n^{17,5}-5120\,n^{17}+10240\,n^{16,5}-512\,n^{16}+15360\,n^{15,5}+5120\,n^{15} \\
& +5120\,n^{14,5}+19712\,n^{14}+24320\,n^{13,5}+18496\,n^{13}+35840\,n^{12,5}+7264\,n^{12}-4160\,n^{11,5} \\
& +10912\,n^{11}+47680\,n^{10,5}+7488\,n^{10}-7600\,n^{9,5}+6752\,n^{9}-2560\,n^{8,5}+96\,n^{8}+18720\,n^{7,5}+3264\,n^{7} \\
& -1200\,n^{6,5}+3168\,n^{6}-600\,n^{5,5}-240\,n^{5}+2400\,n^{4,5}+390\,n^{4}+470\,n^{3}+125\,n^{1,5}+25\,n+25, \\
denom_{Re} &= 4\,n^{2}\,(n+1)(1024\,n^{17}+4096\,n^{16}+2048\,n^{15}+3072\,n^{14}+1024\,n^{13}+4864\,n^{12}+7168\,n^{11} \\
& -832\,n^{10}+9536\,n^{9}-1520\,n^{8}-512\,n^{7}+3744\,n^{6}-240\,n^{5}-120\,n^{4}+480\,n^{3}+25), \\
numer_{Im} &= 4096\,n^{18}+20480\,n^{17}+29696\,n^{16}+14080\,n^{15}+9984\,n^{14}+15872\,n^{13}+41728\,n^{12}+37184\,n^{11} \\
& +27776\,n^{10}+64864\,n^{9}-17808\,n^{8}+4448\,n^{7}+26496\,n^{6}-2160\,n^{5}+40\,n^{4}+3360\,n^{3}+50\,n+175, \\
denom_{Im} &= 4\,(n+1)\,\sqrt{n}(1024\,n^{17}+4096\,n^{16}+2048\,n^{15}+3072\,n^{14}+1024\,n^{13}+4864\,n^{12}+7168\,n^{11} \\
& -832\,n^{10}+9536\,n^{9}-1520\,n^{8}-512\,n^{7}+3744\,n^{6}-240\,n^{5}-120\,n^{4}+480\,n^{3}+25).
\end{aligned}
$$

$$E_3 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\,i \quad \text{mit}$$

$$
\begin{aligned}
numer_{Re} &= -5120\,n^{18,5}+2048\,n^{18}-20480\,n^{17,5}-5120\,n^{17}-10240\,n^{16,5}-512\,n^{16}-15360\,n^{15,5} \\
& +5120\,n^{15}-5120\,n^{14,5}+19712\,n^{14}-24320\,n^{13,5}+18496\,n^{13}-35840\,n^{12,5}+7264\,n^{12}+4160\,n^{11,5} \\
& +10912\,n^{11}-47680\,n^{10,5}+7488\,n^{10}+7600\,n^{9,5}+6752\,n^{9}+2560\,n^{8,5}+96\,n^{8}-18720\,n^{7,5}+3264\,n^{7} \\
& +1200\,n^{6,5}+3168\,n^{6}+600\,n^{5,5}-240\,n^{5}-2400\,n^{4,5}+390\,n^{4}+470\,n^{3}-125\,n^{1,5}+25\,n+25, \\
denom_{Re} &= 4\,n^{2}\,(n+1)\,(4096\,n^{17}+16384\,n^{16}+8192\,n^{15}+12288\,n^{14}+4096\,n^{13}+19456\,n^{12}+28672\,n^{11} \\
& -3328\,n^{10}+38144\,n^{9}-6080\,n^{8}-2048\,n^{7}+14976\,n^{6}-960\,n^{5}-480\,n^{4}+1920\,n^{3}+100), \\
numer_{Im} &= 4096\,n^{18}+10240\,n^{17}-11264\,n^{16}-6400\,n^{15}-20736\,n^{14}+5632\,n^{13}-6912\,n^{12}-34496\,n^{11} \\
& +36096\,n^{10}-30496\,n^{9}-2608\,n^{8}+9568\,n^{7}-10944\,n^{6}+240\,n^{5}+1240\,n^{4}-1440\,n^{3}+50\,n-75, \\
denom_{Im} &= 4\,(n+1)\,\sqrt{n}\,(1024\,n^{17}+4096\,n^{16}+2048\,n^{15}+3072\,n^{14}+1024\,n^{13}+4864\,n^{12}+7168\,n^{11} \\
& -832\,n^{10}+9536\,n^{9}-1520\,n^{8}-512\,n^{7}+3744\,n^{6}-240\,n^{5}-120\,n^{4}+480\,n^{3}+25).
\end{aligned}
$$

$$\text{und} \quad E_4 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\, i \quad \text{mit}$$

$$\begin{aligned}
numer_{Re} &= 5120\,n^{18,5}+2048\,n^{18}+20480\,n^{17,5}-5120\,n^{17}+10240\,n^{16,5}-512\,n^{16}+15360\,n^{15,5}+5120\,n^{15}\\
&\quad +5120\,n^{14,5}+19712\,n^{14}+24320\,n^{13,5}+18496\,n^{13}+35840\,n^{12,5}+7264\,n^{12}-4160\,n^{11,5}\\
&\quad +10912\,n^{11}+47680\,n^{10,5}+7488\,n^{10}-7600\,n^{9,5}+6752\,n^{9}-2560\,n^{8,5}+96\,n^{8}+18720\,n^{7,5}\\
&\quad +3264\,n^{7}-1200\,n^{6,5}+3168\,n^{6}-600\,n^{5,5}-240\,n^{5}+2400\,n^{4,5}+390\,n^{4}+470\,n^{3}+125\,n^{1,5}+25\,n+25,\\
denom_{Re} &= 4\,n^2\,(n+1)\,(1024\,n^{17}+4096\,n^{16}+2048\,n^{15}+3072\,n^{14}+1024\,n^{13}+4864\,n^{12}+7168\,n^{11}\\
&\quad -832\,n^{10}+9536\,n^{9}-1520\,n^{8}-512\,n^{7}+3744\,n^{6}-240\,n^{5}-120\,n^{4}+480\,n^{3}+25),\\
numer_{Im} &= 4096\,n^{18}+10240\,n^{17}-11264\,n^{16}-6400\,n^{15}-20736\,n^{14}+5632\,n^{13}-6912\,n^{12}-34496\,n^{11}\\
&\quad +36096\,n^{10}-30496\,n^{9}-2608\,n^{8}+9568\,n^{7}-10944\,n^{6}+240\,n^{5}+1240\,n^{4}-1440\,n^{3}+50\,n-75,\\
denom_{Im} &= 4\,(n+1)\,\sqrt{n}\,(1024\,n^{17}+4096\,n^{16}+2048\,n^{15}+3072\,n^{14}+1024\,n^{13}+4864\,n^{12}+7168\,n^{11}\\
&\quad -832\,n^{10}+9536\,n^{9}-1520\,n^{8}-512\,n^{7}+3744\,n^{6}-240\,n^{5}-120\,n^{4}+480\,n^{3}+25).
\end{aligned}$$

Aus diesen Daten wurde eine Abschätzung des Betrages von $\varrho^{(2)}$ in Abschnitt 3.1.4 berechnet.

C.2 Nullstelle $\varrho^{(4)}$

Analog zum vorangegangenen Abschnitt ergeben Rechnungen, dass auch

$$\alpha = 1 - \frac{1}{n} + \frac{3}{n^2} + \frac{1}{\sqrt{n}}\, i$$

nahe bei einer (weiteren) Nullstelle von $f(x)$ liegt. Es werden wiederum $\frac{5f(\alpha)}{f'(\alpha)}$, dessen Betrag zum Quadrat und $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$ berechnet. Daraus wurde das Quadrat mit den Ecken $R_1, \ldots, R_4$ in Abschnitt 3.1.4 konstruiert.

Es ergeben sich folgende Formeln in n:

Realteil von $\frac{5f(\alpha)}{f'(\alpha)}$: $\frac{numer_{Re}}{denom_{Re}}$

$$\begin{aligned}
numer_{Re} &= 5\,(-2\,n^{17}+99\,n^{16}-269\,n^{15}+1653\,n^{14}-4000\,n^{13}+14112\,n^{12}-27794\,n^{11}+68041\,n^{10}\\
&\quad -120950\,n^{9}+262548\,n^{8}-454788\,n^{7}+787158\,n^{6}-1030806\,n^{5}+1188270\,n^{4}-990711\,n^{3}\\
&\quad +688905\,n^{2}-295245\,n+98415),\\
denom_{Re} &= n^2\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9}\\
&\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2}\\
&\quad -437400\,n+164025).
\end{aligned}$$

Imaginärteil von $\frac{5f(\alpha)}{f'(\alpha)}$: $\frac{numer_{Im}}{denom_{Im}}$

$$\begin{aligned} numer_{Im} &= 5\,(10\,n^{16}+12\,n^{15}+89\,n^{14}-50\,n^{13}+1092\,n^{12}-1186\,n^{11}+4850\,n^{10}-5108\,n^{9}+23462\,n^{8} \\ &\quad -49476\,n^{7}+124650\,n^{6}-189972\,n^{5}+261630\,n^{4}-240084\,n^{3}+189540\,n^{2}-87480\,n+32805), \\ denom_{Re} &= \sqrt{n}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9} \\ &\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2} \\ &\quad -437400\,n+164025). \end{aligned}$$

Betrag zum Quadrat $|\frac{5f(\alpha)}{f'(\alpha)}|^2$: $\frac{numer}{denom}$

$$\begin{aligned} numer &= 25\,(25\,n^{18}-89\,n^{17}+491\,n^{16}-1286\,n^{15}+4809\,n^{14}-11164\,n^{13}+29414\,n^{12}-54224\,n^{11} \\ &\quad +109996\,n^{10}-184962\,n^{9}+345924\,n^{8}-548370\,n^{7}+828873\,n^{6}-987066\,n^{5}+1016955\,n^{4} \\ &\quad -780759\,n^{3}+492075\,n^{2}-196830\,n+59049), \\ denom &= n^{4}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9} \\ &\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2} \\ &\quad -437400\,n+164025). \end{aligned}$$

Realteil von $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$: $\frac{numer_{Re}}{denom_{Re}}$

$$\begin{aligned} numer_{Re} &= n\,(4\,n^{16}+20\,n^{15}+66\,n^{14}-34\,n^{13}+596\,n^{12}-102\,n^{11}+1916\,n^{10}-4964\,n^{9}+18546\,n^{8} \\ &\quad -24537\,n^{7}+8784\,n^{6}+67878\,n^{5}-163134\,n^{4}+226962\,n^{3}-196830\,n^{2}+109350\,n-32805), \\ denom_{Re} &= 4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9} \\ &\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2} \\ &\quad -437400\,n+164025. \end{aligned}$$

Imaginärteil von $\alpha - \frac{5f(\alpha)}{f'(\alpha)}$: $\frac{numer_{Im}}{denom_{Im}}$

$$\begin{aligned} numer_{Im} &= 2\,n^{3,5}\,(2\,n^{13}-13\,n^{12}+4\,n^{11}+6\,n^{10}-123\,n^{9}+418\,n^{8}-2185\,n^{7}+6079\,n^{6} \\ &\quad -13788\,n^{5}+18009\,n^{4}-17955\,n^{3}+7047\,n^{2}-3645), \\ denom_{Re} &= 4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9} \\ &\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2} \\ &\quad -437400\,n+164025. \end{aligned}$$

Der Kreisradius $|\frac{5f(\alpha)}{2f'(\alpha)}|$ konnte in diesem Fall nach oben durch $\frac{25}{4\,n\sqrt{n}}$ abgeschätzt werden.

Man erhält die folgenden Ausdrücke für die Ecken des Quadrates.

$R_1 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\, i$:

$$
\begin{aligned}
numer_{Re} &= 16\,n^{19}+80\,n^{18}-100\,n^{17,5}+244\,n^{17}-600\,n^{16,5}+854\,n^{16}-1700\,n^{15,5}-306\,n^{15}-11425\,n^{14,5}\\
&\quad +16122\,n^{14}+12400\,n^{13,5}-32336\,n^{13}-157400\,n^{12,5}+121264\,n^{12}+257500\,n^{12,5}-203756\,n^{11}\\
&\quad -910200\,n^{10,5}+582262\,n^{10}+1327900\,n^{9,5}-1174364\,n^{9}-3833200\,n^{8,5}+2896992\,n^{8}\\
&\quad +7082250\,n^{7,5}-5200416\,n^{7}-15933600\,n^{6,5}+8779428\,n^{6}+23746500\,n^{5,5}-11095380\,n^{5}\\
&\quad -32521500\,n^{4,5}+12320100\,n^{4}+30010500\,n^{3,5}-10038330\,n^{3}-23692500\,n^{2,5}+6889050\,n^{2}\\
&\quad +10935000\,n^{1,5}-2952450\,n-4100625\,\sqrt{n}+984150,\\
denom_{Re} &= 4\,n^{2}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9}\\
&\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2}\\
&\quad -437400\,n+164025),\\
numer_{Im} &= 16\,n^{18}+96\,n^{17}+752\,n^{16}+2638\,n^{15}+9941\,n^{14}+1864\,n^{13}+128060\,n^{12}-160368\,n^{11}\\
&\quad +748816\,n^{10}-949208\,n^{9}+3194800\,n^{8}-5779374\,n^{7}+14033880\,n^{6}-21159360\,n^{5}\\
&\quad +30120660\,n^{4}-28115100\,n^{3}+22817700\,n^{2}-10606950\,n+4100625,\\
denom_{Im} &= 4\,n^{1,5}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}\\
&\quad -53116\,n^{9}+153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}\\
&\quad +947700\,n^{2}-437400\,n+164025).
\end{aligned}
$$

$R_2 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\, i$:

$$
\begin{aligned}
numer_{Re} &= 16\,n^{19}+80\,n^{18}+100\,n^{17,5}+244\,n^{17}+600\,n^{16,5}+854\,n^{16}+1700\,n^{15,5}-306\,n^{15}+11425\,n^{14,5}\\
&\quad +16122\,n^{14}-12400\,n^{13,5}-32336\,n^{13}+157400\,n^{12,5}+121264\,n^{12}-257500\,n^{11,5}-203756\,n^{11}\\
&\quad +910200\,n^{10,5}+582262\,n^{10}-1327900\,n^{9,5}-1174364\,n^{9}+3833200\,n^{8,5}+2896992\,n^{8}\\
&\quad -7082250\,n^{7,5}-5200416\,n^{7}+15933600\,n^{6,5}+8779428\,n^{6}-23746500\,n^{5,5}-11095380\,n^{5}\\
&\quad +32521500\,n^{4,5}+12320100\,n^{4}-30010500\,n^{3,5}-10038330\,n^{3}+23692500\,n^{2,5}+6889050\,n^{2}\\
&\quad -10935000\,n^{1,5}-2952450\,n+4100625\,\sqrt{n}+984150,\\
denom_{Re} &= 4\,n^{2}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^{9}\\
&\quad +153328\,n^{8}-283290\,n^{7}+637344\,n^{6}-949860\,n^{5}+1300860\,n^{4}-1200420\,n^{3}+947700\,n^{2}\\
&\quad -437400\,n+164025),\\
numer_{Im} &= 16\,n^{18}+96\,n^{17}+752\,n^{16}+2638\,n^{15}+9941\,n^{14}+1864\,n^{13}+128060\,n^{12}-160368\,n^{11}\\
&\quad +748816\,n^{10}-949208\,n^{9}+3194800\,n^{8}-5779374\,n^{7}+14033880\,n^{6}-21159360\,n^{5}\\
&\quad +30120660\,n^{4}-28115100\,n^{3}+22817700\,n^{2}-10606950\,n+4100625,\\
denom_{Im} &= 4\,n^{1,5}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}
\end{aligned}
$$

$$-53116\,n^9+153328\,n^8-283290\,n^7+637344\,n^6-949860\,n^5+1300860\,n^4-1200420\,n^3$$
$$+947700\,n^2-437400\,n+164025).$$

$R_3 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\,i$:

$$\begin{aligned}
numer_{Re} &= 16\,n^{19}+80\,n^{18}-100\,n^{17,5}+244\,n^{17}-600\,n^{16,5}+854\,n^{16}-1700\,n^{15,5}-306\,n^{15}-11425\,n^{14,5}\\
&\quad +16122\,n^{14}+12400\,n^{13,5}-32336\,n^{13}-157400\,n^{12,5}+121264\,n^{12}+257500\,n^{11,5}-203756\,n^{11}\\
&\quad -910200\,n^{10,5}+582262\,n^{10}+1327900\,n^{9,5}-1174364\,n^9-3833200\,n^{8,5}+2896992\,n^8\\
&\quad +7082250\,n^{7,5}-5200416\,n^7-15933600\,n^{6,5}+8779428\,n^6+23746500\,n^{5,5}-11095380\,n^5\\
&\quad -32521500\,n^{4,5}+12320100\,n^4+30010500\,n^{3,5}-10038330\,n^3-23692500\,n^{2,5}+6889050\,n^2\\
&\quad +10935000\,n^{1,5}-2952450\,n-4100625\,\sqrt{n}+984150,\\
denom_{Re} &= 4\,n^2\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}-53116\,n^9\\
&\quad +153328\,n^8-283290\,n^7+637344\,n^6-949860\,n^5+1300860\,n^4-1200420\,n^3+947700\,n^2\\
&\quad -437400\,n+164025),\\
numer_{Im} &= 16\,n^{18}-104\,n^{17}-448\,n^{16}-762\,n^{15}-12909\,n^{14}+26664\,n^{13}-186740\,n^{12}+354632\,n^{11}\\
&\quad -1071584\,n^{10}+1706592\,n^9-4471600\,n^8+8385126\,n^7-17833320\,n^6+26333640\,n^5\\
&\quad -34922340\,n^4+31905900\,n^3-24567300\,n^2+11263050\,n-4100625,\\
denom_{Im} &= 4\,n^{1,5}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}\\
&\quad -53116\,n^9+153328\,n^8-283290\,n^7+637344\,n^6-949860\,n^5+1300860\,n^4-1200420\,n^3\\
&\quad +947700\,n^2-437400\,n+164025).
\end{aligned}$$

$R_4 = \frac{numer_{Re}}{denom_{Re}} + \frac{numer_{Im}}{denom_{Im}}\,i$:

$$\begin{aligned}
numer_{Re} &= 16\,n^{19}+80\,n^{18}+100\,n^{17,5}+244\,n^{17}+600\,n^{16,5}+854\,n^{16}+1700\,n^{15,5}-306\,n^{15}\\
&\quad +11425\,n^{14,5}+16122\,n^{14}-12400\,n^{13,5}-32336\,n^{13}+157400\,n^{12,5}+121264\,n^{12}\\
&\quad -257500\,n^{11,5}-203756\,n^{11}+910200\,n^{10,5}+582262\,n^{10}-1327900\,n^{9,5}-1174364\,n^9\\
&\quad +3833200\,n^{8,5}+2896992\,n^8-7082250\,n^{7,5}-5200416\,n^7+15933600\,n^{6,5}+8779428\,n^6\\
&\quad -23746500\,n^{5,5}-11095380\,n^5+32521500\,n^{4,5}+12320100\,n^4-30010500\,n^{3,5}-10038330\,n^3\\
&\quad +23692500\,n^{2,5}+6889050\,n^2-10935000\,n^{1,5}-2952450\,n+4100625\,\sqrt{n}+984150,\\
denom_{Re} &= 4\,n^2\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10}\\
&\quad -53116\,n^9+153328\,n^8-283290\,n^7+637344\,n^6-949860\,n^5+1300860\,n^4-1200420\,n^3\\
&\quad +947700\,n^2-437400\,n+164025),\\
numer_{Im} &= 16\,n^{18}-104\,n^{17}-448\,n^{16}-762\,n^{15}-12909\,n^{14}+26664\,n^{13}-186740\,n^{12}+354632\,n^{11}\\
&\quad -1071584\,n^{10}+1706592\,n^9-4471600\,n^8+8385126\,n^7-17833320\,n^6+26333640\,n^5
\end{aligned}$$

$$
\begin{aligned}
& -34922340\,n^4+31905900\,n^3-24567300\,n^2+11263050\,n-4100625, \\
denom_{Im} \;=\; & 4\,n^{1,5}\,(4\,n^{17}+24\,n^{16}+68\,n^{15}+457\,n^{14}-496\,n^{13}+6296\,n^{12}-10300\,n^{11}+36408\,n^{10} \\
& -53116\,n^9+153328\,n^8-283290\,n^7+637344\,n^6-949860\,n^5+1300860\,n^4-1200420\,n^3 \\
& +947700\,n^2-437400\,n+164025).
\end{aligned}
$$

Aus diesen Daten wurden die Abschätzungen von Lemma 3.1.22 gewonnen.

Anhang D

Kurven: geometrisch und zahlentheoretisch

Diese Arbeit beschäftigt sich mit elliptischen und hyperelliptischen Kurven und einer mit diesen zusammenhängenden Konstruktion von algebraischen Zahlkörpern. Dabei wird ein weites theoretisches Feld überspannt, in das die folgenden Abschnitte einführen sollen.

D.1 Algebraische Funktionenkörper

Zuerst werden wichtige Begriffe aus der Theorie der algebraischen Funktionenkörper erläutert. Zugrunde liegt dabei das Buch *Algebraic Function Fields and Codes* von H. Stichtenoth [90], worauf sich die Verweise zu den einzelnen Aussagen beziehen. Der anschließende Abschnitt D.2 wird einige der hier vorkommenden Begriffe seitens algebraischer Kurven beleuchten und Parallelen aufzeigen.

Sei K ein beliebiger Körper und x ein über K transzendentes Element. Der Körper $K(x)$ aller Quotienten der Form $\frac{p(x)}{q(x)}$ mit $p(x), q(x) \in K[x], q(x) \neq 0$ heißt **rationaler Funktionenkörper** über K. Ist $f(y) \in K[x, y]$ ein irreduzibles Polynom, so ist der Quotientenkörper L von

$$K[x, y] \,/\, \langle\, f(y) \,\rangle$$

eine endliche algebraische Erweiterung von $K(x)$ und heißt **Funktionenkörper** über K, bezeichnet mit L/K.

Ein **Bewertungsring** eines Funktionenkörpers L/K ist ein Ring $\mathcal{R}$ mit $K \subsetneq \mathcal{R} \subsetneq L$, so dass für jedes $z \in L$ entweder $z \in \mathcal{R}$ oder $z^{-1} \in \mathcal{R}$ gilt.

Lemma D.1.1 (I.1.5 + I.1.6). *Solch ein Bewertungsring $\mathcal{R}$ ist ein lokaler Ring, besitzt also ein einziges maximales Ideal $P = \mathcal{R}\backslash\mathcal{R}^\times$. Für ein Element $0 \neq z \in L$ gilt dann $z \in P \Leftrightarrow z^{-1} \notin \mathcal{R}$. Weiter ist $\mathcal{R}$ ein Hauptidealring.*

Eine Aussage, die im Abschnitt zu Algebraischen Kurven in ähnlicher Form formuliert wird, ist die folgende, die sich bei Stichtenoth [90] in Lemma I.1.7 (mit $n = 1$) bzw. in Proposition I.1.14 findet.

Lemma D.1.2 (I.1.7). *Für $0 \neq z \in P$ beliebig gilt $1 \leq [L : K(z)] < \infty$.*

Ist $t \in \mathcal{R}$ ein erzeugendes Element von P, so besitzt jedes $0 \neq z \in L$ eine eindeutige Darstellung der Form $z = t^n u$, wobei $n \in \mathbb{Z}$ und $u \in \mathcal{R}^\times$ ist. Ein entsprechendes Element t mit $P = t\,\mathcal{R}$ heißt **uniformisierendes Element** von P, und das maximale Ideal P eines Bewertungsringes $\mathcal{R}$ heißt **Stelle** von L.

Ist P eine beliebige Stelle von L, so ist der zugehörige Bewertungsring eindeutig durch $\mathcal{R}_P := \mathcal{R} = \{z \in L \mid z^{-1} \notin P\}$ gegeben. Eine diskrete Bewertung v_P zu P des Funktionenkörpers L/K ist wie folgt gegeben: Sei t ein uniformisierendes Element von P und sei $z = t^n u$ eine Darstellung eines Elementes $0 \neq z \in L$ wie oben beschrieben. Dann ist $v_P(z) := n$ und $v_P(0) := \infty$.

Ist $z \in L$ und $v_P(z) > 0$ für eine Stelle P von L, so heißt P **Nullstelle** von z. Gilt $v_P(z) < 0$, so heißt P **Polstelle** von z. Ist $|\,v_P(z)\,| = m \in \mathbb{N}\backslash\{0\}$, so spricht man von einer Null- bzw. Polstelle der **Ordnung** m.

Eine wichtige Aussage zu Null- und Polstellen beinhaltet das folgende Korollar (vgl. auch Lemma D.2.17).

Korollar D.1.3 (I.3.4+I.1.19). *Sei L/K ein Funktionenkörper. Ein Element $0 \neq z \in L$ hat endlich viele Null- und Polstellen; ein über K transzendentes Element $z \in L$ besitzt mindestens eine Null- und eine Polstelle.*

Hinsichtlich der untersuchten algebraischen Kurven ist der Begriff des Divisors ein zentraler Begriff.

Definition D.1.4. *Ein* **Divisor** *ist eine formale Summe von Stellen*

$$D = \sum_{P \text{ Stelle von } L} n_P\, P,$$

wobei $n_P \in \mathbb{Z}$ und nur endlich viele $n_P \neq 0$ sind.

Die Menge aller Divisoren bildet eine freie abelsche Gruppe, die von den Stellen eines Funktionenkörpers erzeugt wird; sie heißt **Divisorengruppe** von L/K.

Nach Korollar D.1.3 ist es sinnvoll, zu einem $0 \neq z \in L$ den zugehörigen **Hauptdivisor** zu definieren:

$$(z) := \sum_{P \text{ Stelle von } L} v_P(z)\, P.$$

Die konstanten Elemente $0 \neq z \in L$ sind durch die Äquivalenz $z \in K \Leftrightarrow (z) = 0$ (der Nulldivisor) charakterisiert.

Die Hauptdivisoren bilden eine Untergruppe aller Divisoren und die entsprechende Faktorgruppe heißt **Divisorenklassengruppe**. Die Divisoren einer Nebenklasse heißen **äquivalente Divisoren**.

Im Zusammenhang mit Funktionenkörpern wird ebenso auf den Begriff des Geschlechts eines Funktionenkörpers eingegangen. Dessen Definition benötigt Grad und Dimension eines Divisors.

Sei P eine beliebige Stelle und $\mathcal{R}_P$ der zugehörige Bewertungsring. P ist das maximale Ideal von $\mathcal{R}_P$, so dass $\mathcal{R}_P/P$ ein Körper ist. Nach Voraussetzung ist weiterhin $K \subset \mathcal{R}_P$ und außerdem lässt sich K in $\mathcal{R}_P/P$ einbetten, so dass $\mathcal{R}_P/P$ als Körpererweiterung von K angesehen werden kann. Diese ist endlich (siehe Stichtenoth [90], I.1.14), und der **Grad der Stelle** P wird definiert als der Grad der Körpererweiterung $deg(P) := [\mathcal{R}_P/P : K]$. Zu einem Divisor $D = \sum n_P\, P$ definiert man $v_P(D) = n_P$ und den **Grad eines Divisors** als $deg(D) = \sum v_P(D)\, deg(P)$.

Die Menge der Divisoren eines Funktionenkörpers ist halbgeordnet durch $D_1 \leq D_2 :\Leftrightarrow v_P(D_1) \leq v_P(D_2)$ für alle Stellen P.

Damit lässt sich zu einem beliebigen Divisor D eines Funktionenkörpers L/K folgende Menge definieren:

$$\mathcal{L}(D) := \{z \in L \mid (z) \geq -D\} \cup \{0\}.$$

Lemma D.1.5 (I.4.6+I.4.7+I.4.9). *Sei D ein Divisor des Funktionenkörpers L/K. Dann ist $\mathcal{L}(D)$ ein endlich-dimensionaler Vektorraum über K und heißt* **Riemann-Roch-Raum** *von D. Sind D und D' äquivalente Divisoren, so sind die zugehörigen Riemann-Roch-Räume isomorph, $\mathcal{L}(D) \simeq \mathcal{L}(D')$. Weiter gilt $\mathcal{L}(0) = K$, und für einen Divisor $D < 0$ ist $\mathcal{L}(D) = \{0\}$.*

Die **Dimension eines Divisors** $dim(D)$ ist die Dimension des zugehörigen Vektorraumes $\mathcal{L}(D)$ über K.

Definition D.1.6. *Das* **Geschlecht** g *eines Funktionenkörpers* L/K *ist*

$$g := \max\{deg(D) - dim(D) + 1 \mid D \text{ Divisor von } L/K\}.$$

Korollar D.1.7 (I.4.16). g *ist eine nicht-negative ganze Zahl.*

D.2 Algebraische Kurven

Algebraische Kurven sind nach Definition projektive Varietäten der Dimension 1; diese Definition wird im Folgenden erläutert. Dabei wird anfangs keine Beschränkung auf Dimension 1 vorgenommen, da die allgemeinere Form keine Mehrarbeit bedeutet. Erst am Ende des Abschnittes werden Aussagen ausschließlich für Kurven formuliert.

Wie in Abschnitt D.2.3 ausgeführt, entsprechen sich gewisse Funktionenkörper und algebraische Kurven unmittelbar. In der Regel werden die im Folgenden benötigten Objekte von der algebraischen Geometrie ausgehend definiert und erläutert; nur in den Fällen, wo dies einen unvertretbaren Aufwand bedeutet, wird die Analogie zu den Funktionenkörpern genutzt.

D.2.1 Affine Varietäten

Sei K ein perfekter Körper und $\bar{K}$ der algebraische Abschluss von K. Der n-dimensionale **affine Raum** (über K) ist die Menge der n-Tupel

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \ldots, x_n) \mid x_i \in \bar{K}\}$$

und die Menge der K-rationalen Punkte von $\mathbb{A}^n$ ist

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \mid x_i \in K\}.$$

Die Automorphismen σ der Galoisgruppe $Gal(\bar{K}/K)$ operieren auf den Punkten $P \in \mathbb{A}^n$ durch $P^\sigma := \sigma(P) = (\sigma(x_1), \ldots, \sigma(x_n))$.

Sei $\bar{K}[X] := \bar{K}[x_1, \ldots, x_n]$ der Polynomring über $\bar{K}$ in n Variablen, und sei $I \subset \bar{K}[X]$ ein beliebiges Ideal. Eine **affine algebraische Menge** ist eine Menge

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ für alle } f \in I\}.$$

Umgekehrt ist das Ideal $I(V)$ zu einer algebraischen Menge V die Menge

$$I(V) = \{f \in \bar{K}[X] \mid f(P) = 0 \text{ für alle } P \in V\}.$$

Eine algebraische Menge V heißt **über** K **definiert**, falls ihr Ideal $I(V)$ durch Polynome aus $K[X]$ erzeugt werden kann; dies wird durch V/K bezeichnet. (Nach dem Hilbertschen Basissatz sind alle Ideale von $K[X]$ und $\bar{K}[X]$ endlich erzeugt.) Zu einer über K definierten algebraischen Menge V/K bezeichnet $V(K) := V \cap \mathbb{A}^n(K)$ die Menge der K-rationalen Punkte von V.

Ist V eine algebraische Menge, so heißt V (affine) **Varietät**, falls das Ideal $I(V)$ ein Primideal in $\bar{K}[X]$ ist. Der (affine) **Koordinatenring** einer über K definierten Varietät V/K ist der Faktorring

$$K[V] = K[X]/I(V/K);$$

dieser ist ein Integritätsbereich. Der Quotientenkörper zu $K[V]$ heißt **Funktionenkörper** von V/K und wird mit $K(V)$ bezeichnet. (Koordinatenring und Funktionenkörper werden entsprechend für $\bar{K}$ definiert.) Jedes Element $h \in K(V)$ lässt sich als Nebenklasse eines Quotienten zweier Polynome aus $K[X]$ darstellen: $h = h(X) = \frac{h_1(X)}{h_2(X)} + I(V/K)$ mit $h_2(X) \notin I(V/K)$.

Die **Dimension** $dim(V)$ einer Varietät V ist der Transzendenzgrad von $\bar{K}(V)$ über $\bar{K}$.

Für eine Varietät $V \subset \mathbb{A}^n$ und ein nicht-konstantes Polynom f gilt die Äquivalenz (siehe Silverman [86], I.1.4):

$$I(V) = \langle\, f(x_1, \ldots, x_n) \,\rangle \quad \Leftrightarrow \quad dim(V) = n - 1. \tag{D.1}$$

D.2.2 Projektive Varietäten

Projektive Varietäten sind affine Varietäten, bei denen ein oder mehrere „Punkte im Unendlichen“ hinzugefügt wurden. Der zugehörige projektive Raum der Dimension n ist die Menge der Geraden im affinen Raum der Dimension $n + 1$:

Der n-dimensionale projektive Raum $\mathbb{P}^n = \mathbb{P}^n(\bar{K})$ über K ist die Menge der $(n+1)$-Tupel $(x_0, x_1, \ldots, x_n) \in \mathbb{A}^{n+1} \backslash \{(0, 0, \ldots, 0)\}$ modulo der Äquivalenzrelation

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n),$$

die dadurch gegeben ist, dass ein $\lambda \in \bar{K}^\times$ mit $x_i = \lambda y_i$ für alle $0 \leq i \leq n$ existiert. Eine Äquivalenzklasse $\{(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)\}$ wird (nicht eindeutig) durch $(x_0 : x_1 : \ldots : x_n)$ bezeichnet. Die Menge der K-rationalen Punkte in $\mathbb{P}^n$ ist die Menge

$$\mathbb{P}^n(K) = \{(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \in K \text{ für alle } 0 \leq i \leq n\}.$$[1]

Ein Polynom $f \in \bar{K}[X] = \bar{K}[x_0, x_1, \ldots, x_n]$ heißt **homogen** vom Grad d, falls

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

für alle $\lambda \in \bar{K}$ gilt. Ein Ideal $I \subset \bar{K}[X]$ heißt homogen, falls es durch homogene Polynome erzeugt wird.

Nach dieser Bezeichnung ist klar, dass es sinnvoll ist, homogene Polynome $f(X)$ an Punkten $P \in \mathbb{P}^n$ im Hinblick auf $f(P) = 0$ auszuwerten. Entsprechend und in Analogie zu einer (affinen) algebraischen Menge heißt bei gegebenem homogenen Ideal I die Menge

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ für alle homogenen } f \in I\}$$

projektive algebraische Menge. Ist V eine solche projektive algebraische Menge, so heißt das Ideal $I(V)$, das von

$$\{f \in \bar{K}[X] \mid f \text{ ist homogen und } f(P) = 0 \text{ für alle } P \in V\}$$

erzeugt wird, homogenes Ideal zu V. Und V heißt **über K definiert**, falls – wie im affinen Fall – $I(V)$ durch homogene Polynome aus $K[X]$ erzeugt werden kann; bezeichnet wird dies mit V/K. Die Menge der K-rationalen Punkte ist dann $V(K) = V \cap \mathbb{P}^n(K)$.

Definition D.2.1. *Ist V eine projektive algebraische Menge, so heißt V (projektive)* **Varietät**, *falls $I(V)$ ein Primideal in $\bar{K}[X]$ ist. Eine Varietät V heißt* **abelsche Varietät**, *falls V eine kommutative Gruppe ist. Die Gruppe der K-rationalen Punkte $V(K)$ einer abelschen Varietät V/K heißt* **Mordell-Weil-Gruppe von** V.

Die folgenden Bezeichnungen (Dimension, Funktionenkörper) werden auf die analogen Bezeichnungen im affinen Fall zurückgeführt. Deshalb ist eine Verbindung zwischen affinem und projektivem Fall nötig. Diese wird zuerst formuliert.

[1] Ist $(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K)$, so folgt nicht, dass für jeden Repräsentanten $(x_0, x_1, \ldots, x_n)$ alle $x_i \in K$ liegen, sondern nur, dass es ein Repräsentantentupel $(y_0, y_1, \ldots, y_n) \in \mathbb{A}^{n+1}(K)$ mit $(y_0 : y_1 : \ldots : y_n) = (x_0 : x_1 : \ldots : x_n)$ gibt.

$\mathbb{P}^n$ enthält $n+1$ kanonische Einbettungen von $\mathbb{A}^n$, die durch

$$\phi_i \ : \ \mathbb{A}^n \to \mathbb{P}^n \quad \text{mit} \quad (x_1, \ldots, x_n) \mapsto (x_1 : x_2 : \ldots : x_{i-1} : 1 : x_i : \ldots : x_n)$$

gegeben sind. Ist $U_i = \{P = (x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$ gegeben, so existiert eine natürliche Bijektion $\phi_i^{-1} \ : \ U_i \to \mathbb{A}^n$ mit

$$(x_0 : x_1 : \ldots : x_n) \mapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right).$$

So wird durch ϕ_i bei festgehaltenem i die Menge $\mathbb{A}^n$ üblicherweise mit U_i identifiziert. Die Vereinigung der U_i überdeckt $\mathbb{P}^n$, so dass jede projektive Varietät V durch die Vereinigung der Teilmengen $V \cap U_i$ überdeckt wird.

Ist nun V eine projektive algebraische Menge mit homogenem Ideal $I(V) \subset \bar{K}[X]$, so ist der Schnitt[2] $V \cap \mathbb{A}^n$ eine affine algebraische Menge mit Ideal $I(V \cap \mathbb{A}^n) = \{f(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \mid f(x_0, \ldots, x_n) \in I(V)\}$. Dieser Schritt von $I(V)$ nach $I(V \cap \mathbb{A}^n)$ heißt **Dehomogenisierung** bzgl. x_i. Die Umkehrung – **Homogenisierung** bzgl. x_i – wird für $f \in \bar{K}[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ durch

$$f_{hom}(x_0, \ldots, x_n) := x_i^d \, f \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right)$$

beschrieben, wobei d die kleinste natürliche Zahl ist, für die f_{hom} ein Polynom ist; anders ausgedrückt ist d der Maximalgrad der Monome in f.

Ist V eine affine algebraische Menge mit Ideal $I(V)$, so besteht die Menge $\{f_{hom}(X) \mid f \in I(V)\}$ aus homogenen Polynomen. Zu dem von dieser Menge erzeugten Ideal $I(\bar{V})$ gehört die projektive algebraische Menge $\bar{V}$, der sogenannte **projektive Abschluss** $\bar{V}$ von V.

Auf Grund der Eindeutigkeit des projektiven Abschlusses $\bar{V}$ einer affinen Menge V einerseits und der mehrfachen Möglichkeiten der Dehomogenisierung andererseits besteht der folgende Zusammenhang zwischen projektiven und affinen Varietäten:

Korollar D.2.2 (Silverman [86], I.2.6). *Ist V eine affine Varietät, dann ist $\bar{V}$ eine projektive Varietät und es gilt $V = \bar{V} \cap \mathbb{A}^n$.*

Ist V eine projektive Varietät, dann gilt entweder $V \cap \mathbb{A}^n = \emptyset$ oder $V \cap \mathbb{A}^n$ ist eine affine Varietät, die $V = \overline{V \cap \mathbb{A}^n}$ erfüllt.

[2] Hierbei ist exakt $\phi_i^{-1}(V \cap U_i)$ gemeint.

Nach dieser Zusammenführung der Begriffe einer affinen und einer projektiven Varietät werden Dimension und Funktionenkörper einer Varietät im projektiven Fall auf den affinen Fall zurückgeführt:

Ist V eine projektive Varietät, so existiert ein $\mathbb{A}^n \subset \mathbb{P}^n$ mit $V \cap \mathbb{A}^n \neq \emptyset$. Zu einem solchen $\mathbb{A}^n$ heißt die Dimension von $V \cap \mathbb{A}^n$ die Dimension von V. Der Funktionenkörper $\bar{K}(V)$ von V ist der Funktionenkörper $\bar{K}(V \cap \mathbb{A}^n)$. Analoges gilt für eine über K definierte (projektive) Varietät V/K.

Ist V eine affine Varietät und $\bar{V}$ der projektive Abschluss von V, so heißen die Punkte in $\bar{V} \backslash V$ die **Punkte im Unendlichen** von V.

D.2.3 Kurven und Funktionenkörper

Definition D.2.3. *Eine algebraische* **Kurve** $\mathcal{C}$ *ist eine projektive Varietät der Dimension 1.*

Nach der in Abschnitt D.2.1 angegebenen Äquivalenz (D.1) zur Dimension einer Varietät ist also eine Kurve die Menge der Punkte in $\mathbb{P}^2$, die eine Gleichung

$$F(x, y, z) = 0$$

(bzw. in affiner Form $F(x, y) = 0$) erfüllen, wobei $F(x, y, z) \in \bar{K}[x, y, z]$ ein homogenes irreduzibles Polynom ist.

Definition D.2.4. *Ist $P \in \mathbb{A}^2$ ein Punkt einer Kurve $\mathcal{C} : F(x, y) = 0$, so heißt P* **singulärer Punkt**, *falls beide partiellen Ableitungen von $F(x, y)$ an P verschwinden, also falls $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0$.*[3] *Besitzt $\mathcal{C}$ keine singulären Punkte, so heißt $\mathcal{C}$* **glatte Kurve**.

Auf die folgende Beobachtung wird mehrmals zurückgegriffen:

Beispiel D.2.5. Sei eine Kurve $\mathcal{C}$ in der Form $F(x, y) = y^2 - f(x) = 0$ gegeben. Dann ist $\frac{\partial F}{\partial y} = 2y$ und $\frac{\partial F}{\partial x} = f'(x)$. Ist nun P ein Punkt auf $\mathcal{C}$ und verschwindet die partielle Ableitung nach y an P, so muss also $P = (x_P, 0)$ gelten. Da $P \in \mathcal{C}$ ist, folgt $F(x_p, y_p) = y_P^2 - f(x_P) = -f(x_P) = 0$. Verschwindet auch die zweite partielle Ableitung von $F(x, y)$, so folgt $f'(x_P) = 0$. Somit ist also x_P genau dann eine doppelte Nullstelle von $f(x)$, wenn der zugehörige Punkt $P = (x_P, 0)$ ein singulärer Punkt von $\mathcal{C}$ ist.

[3] Analog wird die Singularität eines Punktes $P \in \mathcal{C}$ im projektiven Fall durch $\partial F/\partial x(P) = \partial F/\partial y(P) = \partial F/\partial z(P) = 0$ charakterisiert. (Siehe z. B. Stichtenoth [90], B.6.)

Sei $P \in \mathcal{C}$ ein Punkt einer Kurve $\mathcal{C}$. Die Teilmenge M_P des (affinen) Koordinatenringes $\bar{K}[\mathcal{C}]$ mit

$$M_P := \{f \in \bar{K}[\mathcal{C}] \mid f(P) = 0\}$$

ist ein maximales Ideal von $\bar{K}[\mathcal{C}]$. Die Lokalisierung $\bar{K}[\mathcal{C}]_P$ von $\bar{K}[\mathcal{C}]$ nach M_P wird **Lokalisierung** von $\mathcal{C}$ nach P genannt und ist

$$\bar{K}[\mathcal{C}]_P = \left\{ \tfrac{f}{g} \in \bar{K}(\mathcal{C}) \mid f, g \in \bar{K}[\mathcal{C}] \text{ mit } g(P) \neq 0 \right\}.$$

Für eine solche Lokalisierung gilt folgende wichtige Aussage.

Satz D.2.6 (Silverman [86], II.1.1). *Sei $\mathcal{C}$ eine glatte Kurve und $P \in \mathcal{C}$ ein Punkt von $\mathcal{C}$. Dann ist die Lokalisierung $\bar{K}[\mathcal{C}]_P$ von $\mathcal{C}$ nach P ein diskreter Bewertungsring, dessen Bewertung durch*

$$\mathrm{ord}_P \ : \ \bar{K}[\mathcal{C}]_P \to \{0, 1, 2, \cdots\} \cup \{\infty\},$$

$$\mathrm{ord}_P(\tfrac{f}{g}) := \mathrm{ord}_P(f) := \max\{d \in \mathbb{Z} \mid f \in M_P^d\}$$

gegeben ist.

Die Bewertung ord_P wird durch $\mathrm{ord}_P(\frac{f}{g}) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ auf den gesamten Funktionenkörper $\bar{K}(\mathcal{C})$ fortgesetzt und als Bild wird $\mathbb{Z} \cup \{\infty\}$ erreicht.

Das von M_P in $\bar{K}[\mathcal{C}]_P$ erzeugte Ideal $M_P \bar{K}[\mathcal{C}]_P$ (im Folgenden wird dafür verkürzt M_P geschrieben) ist nach Lemma D.1.1 ein Hauptideal; ein erzeugendes Element $t \in \bar{K}(\mathcal{C})$ heißt **uniformisierendes Element** für $\mathcal{C}$ an P und es gilt $\mathrm{ord}_P(t) = 1$.

Eine wichtige Aussage in Richtung Funktionenkörpertheorie ist das folgende Lemma (vgl. Lemma D.1.2).

Lemma D.2.7 (Silverman [86], II.1.4). *Sei $\mathcal{C}/K$ eine Kurve und $t \in K(\mathcal{C})$ ein uniformisierendes Element für $\mathcal{C}$ an einem nicht-singulären Punkt $P \in \mathcal{C}$. Dann ist der Funktionenkörper $K(\mathcal{C})$ eine endliche Erweiterung von $K(t)$.*

Nach diesen Ausführungen zu den diskreten Bewertungsringen $\bar{K}[\mathcal{C}]_P$ und den Bewertungen ord_P ist es nachvollziehbar, dass es eine Eins-Zu-Eins-Beziehung (bis auf Isomorphie) zwischen algebraischen Kurven $\mathcal{C}/K$ und den

zugehörigen Funktionenkörpern $K(\mathcal{C})$ gibt.[4] Dabei entsprechen die Bewertungsringe $\bar{K}[\mathcal{C}]_P \leftrightarrow \mathcal{R}$ und deren maximale Ideale $M_{P_\mathcal{C}} \leftrightarrow P_\mathcal{R}$ einander. Da dem Ideal $M_{P_\mathcal{C}}$ genau ein Punkt $P_\mathcal{C}$ auf der zugrunde liegenden Kurve $\mathcal{C}$ zugeordnet werden kann, identifiziert man auch die Stellen $P_\mathcal{R} \subset \mathcal{R}$ mit den Punkten $P_\mathcal{C} \in \mathcal{C}$. (Siehe auch Knapp [34], Satz XI.11.44.) Entsprechend sind viele Begriffe in der Literatur übertragbar, auch wenn die jeweiligen Definitionen (vgl. Divisor, Geschlecht) dies nicht immer erkennen lassen. So wird z. B. vom **Geschlecht einer Kurve** $\mathcal{C}$ gesprochen und die zugrundeliegende Definition ist das Geschlecht des entsprechenden Funktionenkörpers $K(\mathcal{C})$. (Siehe Stichtenoth [90], B.9+B.10.)

Den Abschluss dieses Abschnitts bilden Definitionen zu elliptischen (siehe Silverman [86], III.1) und hyperelliptischen Kurven (siehe Stichtenoth [90], VI.2.1) und eine Aussage zu Kurven vom Geschlecht $g = 2$ (siehe auch Stichtenoth [90], VI.2.2).

Definition D.2.8. *Eine Kurve $\mathcal{C}$ vom Geschlecht 1 (mit einem ausgezeichneten Punkt $\mathcal{O}$) heißt* **elliptische Kurve**. *Sind $\mathcal{C}$ und auch $\mathcal{O}$ über K definiert, so sagt man, die Kurve ist über K definiert und schreibt $\mathcal{C}/K$.*

Definition D.2.9. *Eine Kurve $\mathcal{C}$ mit zugehörigem Funktionenkörper $\bar{K}(\mathcal{C})$ vom Geschlecht $g \geq 2$ heißt* **hyperelliptische Kurve**, *falls es eine Funktion $x \in \bar{K}(\mathcal{C})$ gibt, so dass die Körpererweiterung $[\bar{K}(\mathcal{C}) : \bar{K}(x)]$ den Grad 2 besitzt. Ist $\mathcal{C}$ über K definiert, so schreibt man $\mathcal{C}/K$.*

Satz D.2.10 (Hindry/Silverman [27], A.4.5). *Jede Kurve $\mathcal{C}$ vom Geschlecht $g = 2$ ist hyperelliptisch.*

D.2.4 Abbildungen zwischen Kurven

Definition D.2.11. *Seien $\mathcal{C}_1, \mathcal{C}_2$ zwei (projektive) algebraische Kurven. Eine* **rationale Abbildung** *von $\mathcal{C}_1$ nach $\mathcal{C}_2$ ist eine Abbildung $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ mit $\phi = [\phi_1, \phi_2, \phi_3]$, wobei $\phi_i \in \bar{K}(\mathcal{C}_1)$, und für jeden Punkt $P \in \mathcal{C}_1$, an dem jedes ϕ_i definiert ist, gilt $\phi(P) \in \mathcal{C}_2$.*

Ist ϕ_i an einem Punkt P nicht definiert, so kann es dennoch ein $g \in \bar{K}(\mathcal{C}_1)$ geben, so dass $g\,\phi_i$ an P definiert ist und somit $\phi(P)$ ausgewertet werden kann.

[4] Zur Deutlichkeit wird hier auch formal zwischen dem Punkt $P = P_\mathcal{C}$ einer Kurve $\mathcal{C}$ und der Stelle $P = P_\mathcal{R}$ eines Funktionenkörpers unterschieden.

Entsprechend heißt eine rationale Abbildung $\phi = [\phi_1, \phi_2, \phi_3] : \mathcal{C}_1 \to \mathcal{C}_2$ **definiert an einem** $P \in \mathcal{C}_1$, falls es eine Funktion $g \in \bar{K}(\mathcal{C}_1)$ gibt, so dass jedes $g\,\phi_i$ an P definiert ist und außerdem mindestens ein $g\,\phi_i(P) \neq 0$ ist. Ist dies der Fall, so ist $\phi(P) = (g\phi_1(P) : g\phi_2(P) : g\phi_3(P))$.[5]

Definition D.2.12. *Eine rationale Abbildung, die an jedem Punkt definiert ist, heißt* **Morphismus**.

In Abschnitt D.3.1 wird der folgende Satz über Morphismen benötigt.

Satz D.2.13 (Silverman [86], II.2.3). *Sei $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ ein Morphismus. Dann ist ϕ entweder konstant oder surjektiv.*

Ist $\phi : \mathcal{C}_1/K \to \mathcal{C}_2/K$ ein (nicht-konstanter) Morphismus zwischen Kurven, so induziert dieser einen injektiven Homomorphismus $\phi^* : K(\mathcal{C}_2) \to K(\mathcal{C}_1)$ mit $f \mapsto f \circ \phi$, so dass also $\phi^*(K(\mathcal{C}_2))$ als Unterkörper von $K(\mathcal{C}_1)$ aufgefasst werden kann. Den Grad der Körpererweiterung $[K(\mathcal{C}_1) : \phi^*(K(\mathcal{C}_2))]$ nennt man **Grad des Morphismus** ϕ; ist ϕ ein konstanter Morphismus, so definiert man den Grad von ϕ als 0. (Siehe Silverman [86], II.2.4.)[6]

Ist ϕ ein nicht-konstanter Morphismus zwischen zwei Kurven und invertierbar, so spricht man von Isomorphie.

Definition D.2.14. *Seien $\mathcal{C}_1$ und $\mathcal{C}_2$ zwei (algebraische) Kurven. Gibt es zwei Morphismen $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ und $\psi : \mathcal{C}_2 \to \mathcal{C}_1$, so dass $\psi \circ \phi$ bzw. $\phi \circ \psi$ die Identität auf $\mathcal{C}_1$ bzw. $\mathcal{C}_2$ sind, so heißen $\mathcal{C}_1$ und $\mathcal{C}_2$* **isomorph** *zueinander und man schreibt $\mathcal{C}_1 \simeq \mathcal{C}_2$.*

$\mathcal{C}_1/K$ und $\mathcal{C}_2/K$ sind isomorph über K, falls ϕ, ψ über K definiert werden können.

D.2.5 Divisoren

Ein zentraler Begriff bei der Untersuchung algebraischer Kurven ist der des Divisors, der wiederum in einer eindeutigen Beziehung zum selben Begriff im Funktionenkörperfall (siehe Definition D.1.4) steht.

[5] Zu verschiedenen Punkten P kann es nötig sein, verschiedene g zu wählen.

[6] Mit dieser Bezeichnung wird in der Literatur häufig der Begriff einer *hyperelliptischen Kurve* definiert: Sei $\mathcal{C}$ eine algebraische Kurve vom Geschlecht $g \geq 2$. Gibt es einen Morphismus $\phi : \mathcal{C} \to \mathbb{P}^1$ vom Grad 2, so heißt $\mathcal{C}$ hyperelliptische Kurve. (Siehe z. B. Silverman/Hindry [27], A.4.5.)

Definition D.2.15. *Ein* **Divisor** *einer Kurve $\mathcal{C}$ ist eine formale Summe der Punkte $P \in \mathcal{C}$ der Form*

$$D = \sum_{P \in \mathcal{C}} n_P \, P,$$

wobei $n_P \in \mathbb{Z}$ und fast alle $n_P = 0$. Der **Grad des Divisors** *D ist durch*

$$deg(D) = \sum_{P \in \mathcal{C}} n_P$$

definiert. Die Zahl n_P heißt die **Ordnung** *$ord_P(D)$ des Divisors am Punkt P. Die* **Divisorengruppe** *$Div(\mathcal{C})$ ist die freie abelsche Gruppe, die durch die Punkte P der Kurve erzeugt wird, also die Menge aller Divisoren von $\mathcal{C}$. Ist $\mathcal{C}/K$ über K definiert, so heißt ein zugehöriger Divisor D über K* **definiert**, *falls er unter der Operation der Galoisgruppe $Gal(\bar{K}/K)$ festgehalten wird, wobei $D^\sigma := \sigma(D) := \sum n_p \, \sigma(P)$ für $\sigma \in Gal(\bar{K}/K)$ ist.*

Die Teilmenge aller Divisoren vom Grad 0 bildet eine Untergruppe der Divisorengruppe und wird mit $Div^0(\mathcal{C})$ bezeichnet.

Die auf allen Funktionen des Funktionenkörpers $\bar{K}(\mathcal{C})$ definierte Abbildung ord_P (siehe Satz D.2.6) erlaubt, eine weitere Menge von Divisoren zu beschreiben. Dazu wird folgende Definition und insbesondere das anschließende Lemma benötigt.

Definition D.2.16. *Sei $\mathcal{C}$ eine beliebige Kurve, $P \in \mathcal{C}$ ein nicht-singulärer Punkt und $f \in \bar{K}(\mathcal{C})$. Die* **Ordnung von** *$f$* **an** *$P$ ist $\mathrm{ord}_P(f)$. Man sagt, f besitzt an P eine* **Nullstelle**, *falls $\mathrm{ord}_P(f) > 0$ gilt. Ist $\mathrm{ord}_P(f) < 0$, so hat f eine* **Polstelle** *an P. Gilt $\mathrm{ord}_P(f) \geq 0$, so heißt f* **regulär** *oder* **definiert** *an P und man kann $f(P)$ berechnen; ansonsten schreibt man $f(P) = \infty$.*

Die Anzahl von Null- und Polstellen einer Funktion ist endlich (vgl. Korollar D.1.3):

Lemma D.2.17 (Silverman [86], II.1.2). *Sei $\mathcal{C}$ eine glatte Kurve und $f \in \bar{K}(\mathcal{C})$. Dann besitzt f nur endlich viele Null- und Polstellen. Insbesondere ist $f \in \bar{K}$, sofern f keine Polstelle hat.*

Dieses Lemma bestätigt, dass folgende Definition sinnvoll ist, denn dabei sind fast alle Summanden Null.

Definition D.2.18. *Sei $\mathcal{C}$ eine glatte Kurve und sei $f \in \bar{K}(\mathcal{C})^\times$. Der Divisor*

$$div\,(f) := (f) := \sum_{P \in \mathcal{C}} \mathrm{ord}_P(f)\, P$$

heißt **Hauptdivisor**.

Ein Hauptdivisor ist genau dann über K definiert, wenn die zugehörige rationale Funktion f Koeffizienten aus K hat. (Siehe Menezes [56], §7.) Die Hauptdivisoren liegen außerdem in der Gruppe $Div^0(\mathcal{C})$ der Divisoren vom Grad 0, wie das folgende Lemma bestätigt; und sie bilden eine Untergruppe von $Div^0(\mathcal{C})$.

Lemma D.2.19 (Silverman [86], II.3.1). *Sei $\mathcal{C}$ eine glatte Kurve und $f \in \bar{K}(\mathcal{C})^\times$. Der Grad des Hauptdivisors $div(f)$ ist 0. Außerdem ist $div\,(f) = 0$ genau dann, wenn $f \in \bar{K}^\times$ ist.*

Damit besitzen die abelschen Gruppen $Div(\mathcal{C})$ und $Div^0(\mathcal{C})$ eine Untergruppe, so dass es Sinn macht, die entsprechenden Faktorgruppen zu untersuchen.

Definition D.2.20. *Die Faktorgruppe aller Divisoren einer Kurve $\mathcal{C}$ nach den Hauptdivisoren heißt* **Divisorenklassengruppe** *oder* **Picard-Gruppe** $\mathrm{Pic}(\mathcal{C})$. *Die Faktorgruppe der Divisoren vom Grad 0 nach den Hauptdivisoren heißt* **Jacobische Varietät** *$J_\mathcal{C}$ (auch mit $\mathrm{Pic}^0(\mathcal{C})$ bezeichnet) von $\mathcal{C}$.*[7] *Ist D ein Divisor vom Grad 0, so wird seine Klasse in $J_\mathcal{C}$ durch $[D]$ angegeben. Ist $[D] = [\tilde{D}]$, so schreibt man $D \equiv \tilde{D}$ und nennt D äquivalent zu $\tilde{D}$.*

$J_\mathcal{C}(K)$ ist die Menge aller K-rationalen Divisorenklassen[8] von $J_\mathcal{C}$, das heißt $[D]^\sigma = [D]$ für alle $\sigma \in Gal(\bar{K}/K)$, also $[D^\sigma] = [D] \Leftrightarrow D^\sigma = D + (f)$. $J_\mathcal{C}(K)$ ist eine Untergruppe von $J_\mathcal{C}$. (Siehe Menezes [56], §7.)

D.3 Modulkurven

Dieser Abschnitt liefert eine Einführung in Modulkurven $X_0(N)$. Gleichungen solcher Kurven für bestimmte natürliche Zahlen N finden sich in D.3.2.

[7] Diese Definition ist kanonisch, entspricht aber nicht der allgemeinen Definition einer Jacobischen Varietät. (Siehe dazu z. B. Hindry/Silverman [27], A.6.3.1.) Es kann jedoch gezeigt werden, dass die hier definierte Faktorgruppe isomorph zu einer Jacobischen Varietät ist. (Siehe Hindry/Silverman [27], A.8.1.1.)

[8] $\mathrm{Pic}^0(\mathcal{C})(K)$ sind die Divisorenklassen, die von einem K-rationalen Divisor erzeugt werden. Somit gilt: $\mathrm{Pic}^0(\mathcal{C})(K) \subseteq J_\mathcal{C}(K)$.

Die analytische Theorie elliptischer Kurven und Modulfunktionen stellt ein weites Feld dar, welches hier nur in einigen Details beleuchtet wird. So soll Abschnitt D.3.1 mit Aussagen zu elliptischen Kurven über $\mathbb{C}$ eine knappe Heranführung an den anschließenden Teil D.3.2 sein. In letzterem wird dann erläutert, worum es sich bei Modulkurven $X_0(N)$ handelt. Andere Modulkurven werden in D.3.4 angesprochen.

D.3.1 Elliptische Kurven über $\mathbb{C}$

Definition D.3.1. *Eine diskrete Untergruppe* Λ *von* $\mathbb{C}$

$$\Lambda := \left\{ \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \mid \omega_1, \omega_2 \in \mathbb{C}, \frac{\omega_1}{\omega_2} \notin \mathbb{R} \right\},$$

die eine $\mathbb{R}$*-Basis für* $\mathbb{C}$ *beinhaltet, heißt* **Gitter** *in* $\mathbb{C}$*. Man schreibt auch* $\Lambda = \langle\, \omega_1, \omega_2 \,\rangle$*. Zwei Gitter* Λ_1, Λ_2 *heißen* **homothetisch**, *falls* $\lambda\Lambda_1 = \Lambda_2$ *für ein* $\lambda \in \mathbb{C}^\times$ *gilt.*

Homothetie ist ein Isomorphiebegriff für Gitter, der näher untersucht wird. Ist $\Lambda = \langle\, \omega_1, \omega_2 \,\rangle$ ein Gitter in $\mathbb{C}$, so ist dieses homothetisch zu $\langle\, 1, \frac{\omega_1}{\omega_2} \,\rangle$ und zu $\langle\, 1, \frac{\omega_2}{\omega_1} \,\rangle$. Nach Voraussetzung gilt $\Im(\frac{\omega_1}{\omega_2}) \neq 0$, und entweder ist $\Im(\frac{\omega_1}{\omega_2}) > 0$ oder $\Im(\frac{\omega_2}{\omega_1}) > 0$, wie man unmittelbar mit Hilfe der Polarkoordinatendarstellung von ω_1 und ω_2 sehen kann. Somit ist Λ homothetisch zu einem Gitter der Form $\Lambda_\tau = \langle\, 1, \tau \,\rangle$, wobei $\Im(\tau) > 0$ gilt. Trotz der vorgenommenen Einschränkung $\tau \in \mathcal{H}$, der oberen Halbebene von $\mathbb{C}$, können auch zwei solche Gitter Λ_τ und $\Lambda_{\tau'}$ homothetisch sein: Λ_τ ist genau dann homothetisch zu $\Lambda_{\tau'}$, wenn $\tau' = \frac{a\tau+b}{c\tau+d}$ für eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$[9] gilt. (Siehe Silverman [87], I.1.2.b.)

Somit kann man sagen, dass die Gruppe $SL_2(\mathbb{Z})$ auf der oberen Halbebene $\mathcal{H}$ durch $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \tau = \frac{a\tau+b}{c\tau+d}$ operiert. Es gibt folglich eine Abbildung von $\mathcal{H}$ in die Menge von Homothetieklassen von Gittern, die durch $\tau \mapsto \Lambda_\tau$ gegeben ist, wobei zwei Gitter Λ_τ und $\Lambda_{\tau'}$ genau dann homothetisch sind, wenn es ein $\gamma \in SL_2(\mathbb{Z})$ mit $\tau = \gamma\tau'$ gibt.

[9] Die positive Determinante garantiert, dass das Element $\frac{a\tau+b}{c\tau+d}$ in der oberen Halbebene $\mathcal{H}$ liegt.

Definition D.3.2. *Sei Λ ein Gitter in $\mathbb{C}$. Die* **Weierstraßsche $\wp$-Funktion** *(bzgl. des Gitters Λ) ist für $z \in \mathbb{C}$ durch die Reihe*

$$\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

definiert.

Die Weierstraßsche $\wp$-Funktion konvergiert absolut und gleichmäßig auf jeder kompakten Teilmenge von $\mathbb{C}\backslash\Lambda$. Sie besitzt einen doppelten Pol an jedem Gitterpunkt und keine weiteren Pole. (Beweis: Silverman [86], VI.3.1.b.)

Mit Hilfe der Weierstraßschen $\wp$-Funktion und der Homothetie von Gittern lassen sich folgende Aussagen formulieren, deren Beweise ebenfalls bei Silverman [86] zu finden sind:

Satz D.3.3 (Silverman [86], VI.5.1+VI.4.1.1). *Sei $\mathcal{C}/\mathbb{C}$ eine elliptische Kurve in homogener Form. Dann existiert ein bis auf Homothetie eindeutiges Gitter Λ in $\mathbb{C}$, so dass*

$$\Phi \ : \ \mathbb{C}/\Lambda \to \mathcal{C}(\mathbb{C}) \quad \Phi(z) = (\wp(z;\Lambda) : \wp'(z;\Lambda) : 1)$$

ein Isomorphismus ist.

Sind $\mathcal{C}_1/\mathbb{C}$ und $\mathcal{C}_2/\mathbb{C}$ zwei elliptische Kurven, die mit den Gittern Λ_1 und Λ_2 korrespondieren, dann sind $\mathcal{C}_1$ und $\mathcal{C}_2$ genau dann (über $\mathbb{C}$) isomorph, falls Λ_1 und Λ_2 homothetisch zueinander sind.

Nun ist also garantiert, dass jede elliptische Kurve $\mathcal{C}/\mathbb{C}$ mit einem Gitter Λ in $\mathbb{C}$ identifiziert werden kann. Es gilt aber auch die umgekehrte Aussage, dass zu jedem Gitter Λ in $\mathbb{C}$ eine elliptische Kurve korrespondiert. (Beweis: Silverman [86] VI.3.6.b.) Somit besteht eine Eins-Zu-Eins-Beziehung zwischen den Homothetieklassen von Gittern und den Isomorphieklassen von elliptischen Kurven Ell($\mathbb{C}$):

$$\begin{array}{rcl} \mathcal{H}/SL_2(\mathbb{Z}) & \leftrightarrow & \mathrm{Ell}(\mathbb{C}) \\ \tau & \to & \mathbb{C}/\Lambda_\tau \\ \frac{\omega_1}{\omega_2} & \leftarrow & \mathbb{C}/\langle \omega_1,\omega_2 \rangle. \end{array}$$

D.3.2 $Y_0(N)$ und $X_0(N)$

Wie im vorangegangenen Abschnitt deutlich wurde, können Isomorphieklassen von komplexen elliptischen Kurven mit Elementen von $\mathcal{H}/SL_2(\mathbb{Z})$ identifiziert werden. Die Menge dieser Isomorphieklassen wird mit $Y_0(1)$ bezeichnet; vereinfacht schreibt man auch $\mathcal{H}/SL_2(\mathbb{Z}) = Y_0(1)$.

Da $SL_2(\mathbb{Z})$ von den beiden Matrizen

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

erzeugt wird (siehe Silverman [87], Corollary I.1.6), wobei für ein $\tau \in \mathcal{H}$ die Bilder unter S und T gerade $S \circ \tau = -\frac{1}{\tau}$ und $T \circ \tau = \tau + 1$ sind, ergibt sich der Fundamentalbereich von $\mathcal{H}/SL_2(\mathbb{Z})$, wie in Abbildung D.1 zu sehen ist. (Dabei ist ρ die sechste Einheitswurzel $\frac{1}{2} + \frac{\sqrt{3}}{2}i$.)

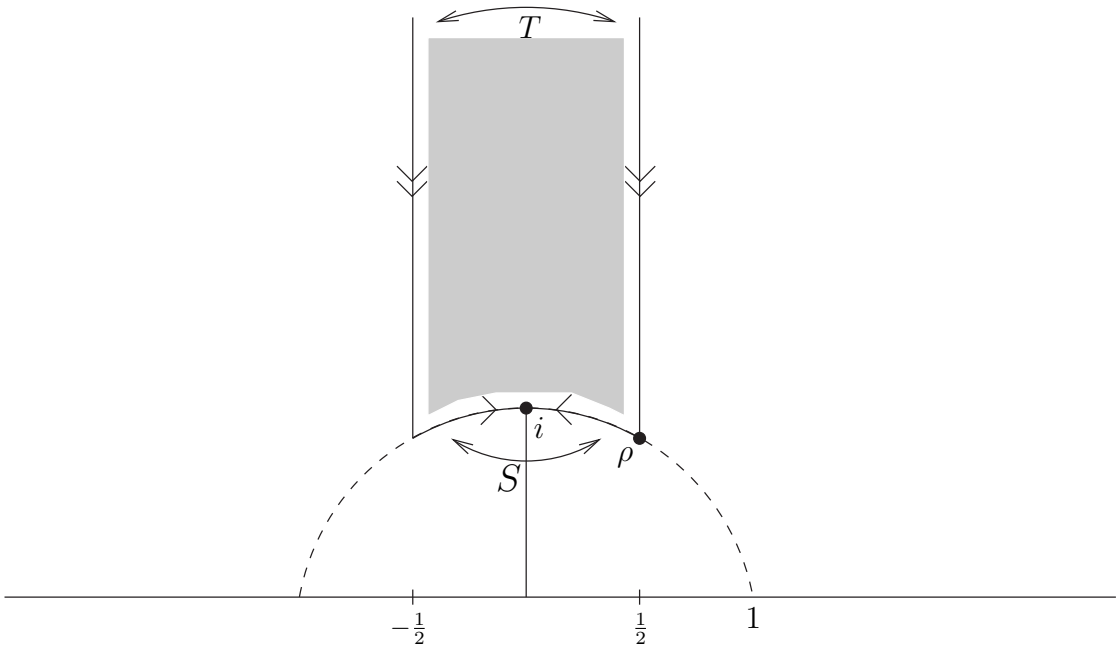

Abbildung D.1: Fundamentalbereich für $\mathcal{H}/SL_2(\mathbb{Z})$

$Y_0(1)$ ist ein nicht-kompaktes Gebiet, welches durch Hinzufügen eines Punktes, der sogenannten Spitze im Unendlichen (man schreibt (∞)) (siehe Abbildung D.2), zu einer kompakten Riemannschen Fläche wird.[10]

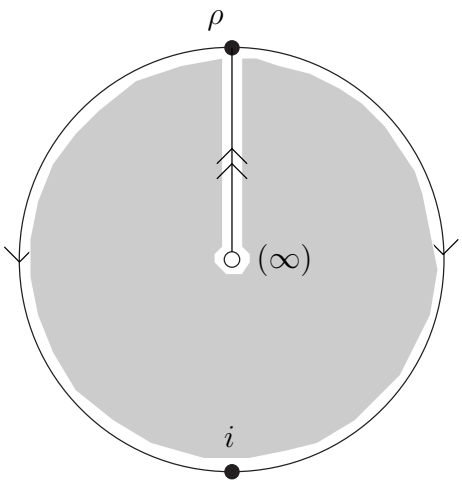

Abbildung D.2: Fundamentalbereich für $\mathcal{H}/SL_2(\mathbb{Z})$ nach Identifizierung

Formal wird dies z. B. durch Setzen von $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ erreicht (siehe Silverman, [87], I.2), womit der Punkt $(1:0) \in \mathbb{P}^1(\mathbb{Q})$ (Spitze) zur oberen Halbebene $\mathcal{H}$ hinzugefügt wird. Wird nun wieder die Operation von $SL_2(\mathbb{Z})$ auf $\mathcal{H}^*$ untersucht, so ist dies in Analogie zu Abschnitt D.3.1 als $(x:y) \mapsto (ax+by : cx+dy)$ zu verstehen (siehe Silverman [87], I.2). Dabei werden (genauer als zuvor) die Bilder von $\mathbb{P}^1(\mathbb{Q})$ in $\mathcal{H}^*/SL_2(\mathbb{Z})$ die Spitzen von $\mathcal{H}^*/SL_2(\mathbb{Z})$ genannt.

Die somit erhaltene kompakte Riemannsche Fläche $\mathcal{H}^*/SL_2(\mathbb{Z})$ wird mit $X_0(1)$ bezeichnet.

Eine Verallgemeinerung dieser Betrachtung besteht darin, dass Äquivalenzklassen von (modularen) Paaren $(\mathcal{C},\mathcal{N})$ betrachtet werden, wobei $\mathcal{C}$ eine elliptische Kurve und $\mathcal{N} \subset \mathcal{C}(\mathbb{C})$ eine zyklische Untergruppe der Ordnung N der komplexen Punkte von $\mathcal{C}$ ist. Ein solches Paar $(\mathcal{C},\mathcal{N})$ bleibt im Gegensatz zur Situation, wie sie in Abschnitt D.3.1 dargestellt wurde, nicht mehr invariant unter der Operation der $SL_2(\mathbb{Z})$, sondern nur unter der Operation der **Kongruenzuntergruppe** $\Gamma_0(N)$ der $SL_2(\mathbb{Z})$ mit

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}.$$

[10] Eine Riemannsche Fläche ist im Grunde ein topologischer Raum, in dem jeder Punkt eine Umgebung besitzt, die zu einer offenen Teilmenge von $\mathbb{C}$ isomorph ist. Zur Topologie siehe z. B. Knapp [34], XI.2.

(Siehe dazu Silverman [86], C.13.) Entsprechend bezeichnet man

$$Y_0(N) := \mathcal{H}/\Gamma_0(N)$$

und die Kompaktifizierung

$$X_0(N) := \mathcal{H}^*/\Gamma_0(N).$$

Beispiel D.3.4. Sei $N = 11$. $\Gamma_0(11)$ wird von $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $U = \begin{pmatrix} 7 & -2 \\ 11 & -3 \end{pmatrix}$ und $V = \begin{pmatrix} 8 & -3 \\ 11 & -4 \end{pmatrix}$ erzeugt. (Siehe Weston [95], §2, Seite 6.) Ein Fundamentalbereich von $\mathcal{H}/\Gamma_0(11)$ sieht wie in Abbildung D.3 dargestellt aus.

Identifiziert man nun die durch den Dreifachpfeil gekennzeichneten Ränder des Fundamentalbereiches bei $\Re(\tau) = 0$ und $\Re(\tau) = 1$, so läßt sich der entstandene Bereich vereinfacht als Rechteck interpretieren, wie in Abbildung D.4 veranschaulicht. Dabei ist zu beachten, dass die fünf Punkte $0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}$ und 1 auf der reellen Achse nicht zur oberen Halbebene und damit nicht zum Fundamentalbereich für $\mathcal{H}/\Gamma_0(11)$ gehören. Somit besitzt das entsprechende Rechteck nicht nur eine Spitze im Unendlichen (gekennzeichnet mit (∞)), sondern noch eine weitere Spitze bei Null. Dass es sich dabei nur um eine Spitze handelt, wird nach der Identifizierung der Doppelpfeilseiten und der Einfachpfeilseiten (letztere ist nicht mehr abgebildet) deutlich. Nach diesen Identifizierungen ergibt sich der Fundamentalbereich für $\mathcal{H}/\Gamma_0(11)$ zu einem Torus (bei dem zwei Punkte fehlen). Fügt man diese beiden Spitzen zu $Y_0(11)$ hinzu, so bekommt man die kompaktifizierte Modulkurve $X_0(11)$. Anschaulich ist nachvollziehbar, dass diese Kurve Geschlecht 1 besitzt.

Gemäß der Konstruktion repräsentiert jeder Punkt auf der Modulkurve $Y_0(N)$ über $\mathbb{C}$ eine Isomorphieklasse elliptischer Kurven mit einer zyklischen Untergruppe der Ordnung N. Bei der Kompaktifizierung $X_0(N)$ kommen dabei die Spitzen, also die Bilder von $\mathbb{P}^1(\mathbb{Q})$ in $\mathcal{H}^*/\Gamma_0(N)$, hinzu, die keiner Äquivalenzklasse elliptischer Kurven entsprechen. $X_0(N)$ besitzt genau zwei Spitzen, falls $N \neq 2$ eine Primzahl ist; beide sind rational über $\mathbb{Q}$ und werden mit (0) und (∞) bezeichnet. (Siehe Silverman [86], C.13.3.)

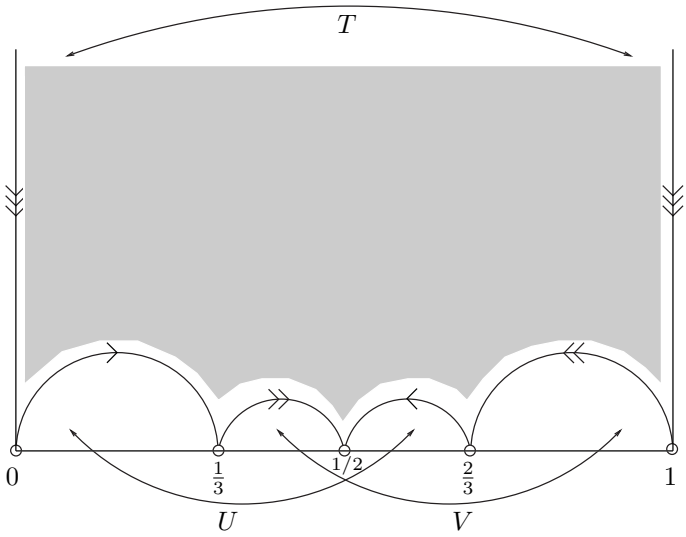

Abbildung D.3: Fundamentalbereich für $\mathcal{H}/\Gamma_0(11)$

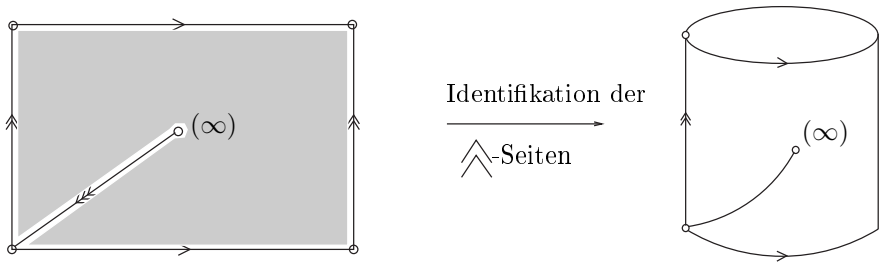

Abbildung D.4: Fundamentalbereich für $\mathcal{H}/\Gamma_0(11)$ nach Identifizierung

D.3.3 Gleichungen von $X_0(N)$ über $\mathbb{Q}$

Über den komplexen Zahlen $\mathbb{C}$ besteht eine Eins-Zu-Eins-Beziehung zwischen den (komplexen) Punkten der Modulkurve $X_0(N)$ und den Äquivalenzklassen modularer Paare $(\mathcal{C}, \mathcal{N})$ (zuzüglich der Spitzen, die keinen Paaren entsprechen), wie im vorangegangenen Abschnitt ausgeführt wurde. $X_0(N)$ ist eine Riemannsche Fläche und entspricht – wie jede Riemmansche Fläche (siehe Knapp [34], XI.11.17) – einer (projektiven) algebraischen Kurve über $\mathbb{C}$. Um zu zeigen, dass $X_0(N)$ auch über $\mathbb{Q}$ definiert ist, muss eine endlich erzeugte Körpererweiterung K über $\mathbb{Q}$ vom Transzendenzgrad 1 gefunden werden, so dass $\mathbb{C}K = L$ gilt, wobei L der Funktionenkörper von $X_0(N)$ (siehe Weston [95], §3, Seite 7) ist. Ist eine solche Erweiterung K gefunden und bezeichnet $X_0(N)_{\mathbb{Q}}$ die zu K gehörende algebraische Kurve, so garantiert die Bedingung $\mathbb{C}K = L$, dass alle ursprünglichen Punkte von $X_0(N)$ über $\mathbb{C}$ unter den

komplexen Punkten $X_0(N)_{\mathbb{Q}}(\mathbb{C})$ von $X_0(N)_{\mathbb{Q}}$ sind.

Die explizite Berechnung einer Gleichung von $X_0(N)_{\mathbb{Q}}$ basiert in der Regel auf Modulfunktionen (siehe z. B. Ogg [72], Rovira [22], Murabayashi [65]) und liefert die folgenden Gleichungen für (hyper-)elliptische Modulkurven $X_0(N)$; weitere solche Kurven existieren nicht.

(Die letzte Spalte der Tabelle gibt immer die Quelle an: Die Buchstaben G, GR und M beziehen sich auf Galbraith [19], González Rovira [22] und Murabayashi [65].)

N	g	$y^2 = f(x)$	
11	1	$x^4 + 4x^3 - 88x^2 - 668x - 1272$	GR
14	1	$x^4 - 14x^3 + 19x^2 - 14x + 1$	GR
15	1	$x^4 - 10x^3 - 13x^2 + 10x + 1$	GR
17	1	$x^4 + 2x^3 - 39x^2 - 176x - 212$	GR
19	1	$x^4 - 32x^2 - 76x - 48$	GR
20	1	$x^4 - 8x^3 - 2x^2 - 8x + 1$	GR
21	1	$x^4 - 6x^3 - 17x^2 - 6x + 1$	GR
22	2	$x^6 - 4x^4 + 20x^3 - 40x^2 + 48x - 32$	G
23	2	$x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$	M
24	1	$x^4 - 8x^3 + 2x^2 + 8x + 1$	GR
26	2	$x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$	GR
27	1	$x^4 - 18x^2 - 36x - 27$	GR
28	2	$x^6 + 10x^4 + 25x^2 + 28$	G
29	2	$x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$	M
30	3	$x^8 + 6x^7 + 9x^6 + 6x^5 - 4x^4 - 6x^3 + 9x^2 - 6x + 1$	GR
31	2	$x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3$	M
32	1	$x^4 - 8x^3 + 12x^2 - 16x + 4$	GR
33	3	$x^8 + 10x^6 - 8x^5 + 47x^4 - 40x^3 + 82x^2 - 44x + 33$	G
35	3	$x^8 - 4x^7 - 6x^6 - 4x^5 - 9x^4 + 4x^3 - 6x^2 + 4x + 1$	GR
36	1	$x^4 - 4x^3 - 6x^2 - 4x + 1$	GR
37	2	$x^6 + 14x^5 + 35x^4 + 48x^3 + 35x^2 + 14x + 1$	G
39	3	$x^8 - 6x^7 + 3x^6 + 12x^5 - 23x^4 + 12x^3 + 3x^2 - 6x + 1$	GR
40	3	$x^8 + 8x^6 - 2x^4 + 8x^2 + 1$	GR
41	3	$x^8 - 4x^7 - 8x^6 + 10x^5 + 20x^4 + 8x^3 - 15x^2 - 20x - 8$	G
46	5	$x^{12} - 2x^{11} + 5x^{10} + 6x^9 - 26x^8 + 84x^7 - 113x^6 + 134x^5$ $-64x^4 + 26x^3 + 12x^2 + 8x - 7$	G
47	4	$x^{10} - 6x^9 + 11x^8 - 24x^7 + 19x^6 - 16x^5 - 13x^4 + 30x^3$ $-38x^2 + 28x - 11$	G

N	g	$y^2 = f(x)$	
48	3	$x^8 + 14\,x^4 + 1$	GR
49	1	$x^4 - 2\,x^3 - 9\,x^2 + 10\,x - 3$	GR
50	2	$x^6 - 4\,x^5 - 10\,x^3 - 4\,x + 1$	GR
59	5	$x^{12} - 8\,x^{11} + 22\,x^{10} - 28\,x^9 + 3\,x^8 + 40\,x^7 - 62\,x^6 + 40\,x^5$ $-3\,x^4 - 24\,x^3 + 20\,x^2 - 4\,x - 8$	G
71	6	$x^{14} + 4\,x^{13} - 2\,x^{12} - 38\,x^{11} - 77\,x^{10} - 26\,x^9 + 111\,x^8 + 148\,x^7$ $+x^6 - 122\,x^5 - 70\,x^4 + 30\,x^3 + 40\,x^2 + 4\,x - 11$	GR

D.3.4 Weitere Modulkurven

$X_0(N)$ parametrisiert die Isomorphieklassen elliptischer Kurven $\mathcal{C}$, die eine zyklische Untergruppe $\mathcal{N}$ der Ordnung N enthalten, wie in Abschnitt D.3.2 deutlich wurde. In Anlehnung an diese Betrachtung können Isomorphieklassen elliptischer Kurven mit einem Punkt P der Ordnung N parametrisiert werden: dies geschieht durch Untersuchung der Operation der Untergruppe $\Gamma_1(N)$ (eine andere **Kongruenzuntergruppe**) der $SL_2(\mathbb{Z})$ auf der oberen Halbebene $\mathcal{H}$ bzw. auf $\mathcal{H}^*$, wobei

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N, a \equiv d \equiv 1 \bmod N \right\}$$

ist, und man erhält die Modulkurve

$$X_1(N) := \mathcal{H}^*/\Gamma_1(N).$$

Naheliegenderweise gibt es eine Abbildung $X_1(N) \to X_0(N)$, die Paare $(\mathcal{C}, P)$ auf Paare $(\mathcal{C}, \langle P \rangle)$ abbildet, wobei $\langle P \rangle$ die von P erzeugte Untergruppe bezeichnet. $X_1(N)$ besitzt für eine Primzahl $N \neq 2$ genau $N-1$ Spitzen, von denen nur die Hälfte $\mathbb{Q}$-rational sind. (Siehe Silverman [86], C.13.3.)

Die Modulkurven $X_1(N)$ sind elliptisch für $N = 11, 14, 15$. Mestre [58] hat gezeigt, dass $X_1(N)$ genau für $N = 13, 16, 18$ hyperelliptisch ist; diese drei haben Geschlecht $g = 2$. $X_1(20)$ besitzt als einzige Geschlecht $g = 3$ und ist nicht hyperelliptisch. Alle weiteren ($N = 17, 19$ oder $N > 20$) haben Geschlecht $g \geq 5$ und sind nicht hyperelliptisch. (Siehe Jeon et. all. [30].)

Diese Betrachtung kann weiter verallgemeinert werden, indem man die Kongruenzuntergruppe abwandelt (siehe Silverman [86], C.13.1), oder indem für

$n \mid N$ Faktorgruppen[11] $X_0(N)/W_n$ untersucht werden (siehe Galbraith [19]); dabei ist $W_n \in SL_2(\mathbb{R})$ eine **Involution**[12] auf $X_0(N)$, das heißt eine Abbildung, deren Quadrat die Identität ergibt. W_N ist die **Atkin-Lehner-Involution** (sie vertauscht die Spitzen (0) und (∞)) und man definiert $X_0^*(N) := X_0(N)/W_N$ (siehe Hasegawa [26]); dort finden sich auch die Werte N, für die $X_0^*(N)$ hyperelliptisch ist.[13]

Korollar D.3.5 (Baker [1], S. 3). *$X_0(N)$ ist genau dann hyperelliptisch, wenn $X_0^*(N)$ Geschlecht $g = 0$ hat oder $N = 37$ ist.*

[11] $X_0(N)/W_n$ ist wieder eine algebraische Kurve und für $n = N$ über $\mathbb{Q}$ definiert (siehe Baker [1], S. 3).

[12] Siehe auch Ogg [74], S. 453.

[13] Es handelt sich dabei um genau 64 Werte: 57 Werte mit $g = 2$ ($N \geq 67$), 5 Werte mit $g = 3$ ($N \geq 136$) und je einen Wert für $g = 4$ ($N = 176$) und für $g = 5$ ($N = 279$).

Symbolverzeichnis

Die Sortierung der folgenden Symbole, die in dieser Arbeit benutzt werden, erfolgt alphabetisch nach dem griechischen und dem lateinischen Alphabet; sonstige Symbole sind zuerst aufgeführt.

$\oplus$	Punktaddition auf einer elliptischen Kurve
(0)	endliche Spitze einer Modulkurve $X_0(N)$
(∞)	Spitze im Unendlichen einer Modulkurve $X_0(N)$
$[m]$	Multiplikation-mit-m-Isogenie
(f)	Hauptdivisor einer Funktion $f \in \bar{K}(\mathcal{C})^\times$
Γ	Untergruppe einer elliptischen Kurve E
$\Gamma_0(N)$	eine Kongruenzuntergruppe von $SL_2(\mathbb{Z})$
$\Gamma_1(N)$	eine Kongruenzuntergruppe von $SL_2(\mathbb{Z})$
$\Delta(E)$	Diskriminante einer elliptischen Kurve E
$\Delta(K)$	Diskriminante eines Zahlkörpers K
ε	Einheit in einer Ordnung eines Zahlkörpers
ζ	Torsionseinheit in einer Ordnung eines Zahlkörpers
Λ	Gitter in $\mathbb{C}$
ρ, ϱ	Nullstelle eines Polynoms
σ	Element von $Gal(\bar{K}/K)$
τ	komplexe Zahl, einem Gitter zugeordnet
ϕ	Isogenie zwischen zwei Kurven $\mathcal{C}_1$ und $\mathcal{C}_2$
ϕ^*	durch ϕ induzierter Monomorphismus von $K(\mathcal{C}_2)$ nach $K(\mathcal{C}_1)$
ω_i	komplexe Zahl, Erzeuger eines Gitters in $\mathbb{C}$
Ω_b	quadratischer Zahlkörper

A	Punkt $(0,0)$ auf einer Kubertkurve E_l
$\mathbb{A}^n$	n-dimensionaler affiner Raum über $\bar{K}$
$\mathbb{A}^n(K)$	K-rationale Punkte von $\mathbb{A}^n$
$\mathbb{C}$	Körper der komplexen Zahlen
$\mathcal{C}$	algebraische Kurve
$\mathcal{C}/K$	über K definierte algebraische Kurve
$\mathcal{C}(K)$	K-rationale Punkte von $\mathcal{C}$
C_l	zyklische Gruppe mit l Elementen
$\mathcal{C}_l$	Indikatorfunktion zur Galoisgruppe C_l
Cl_K	Idealklassengruppe eines Zahlkörpers K
$Cl(O_K)$	Idealklassengruppe einer Maximalordnung O_K
D	Divisor einer algebraischen Kurve oder eines Funktionenkörpers
D_l	Diedergruppe mit $2\,l$ Elementen
$\mathcal{D}_l$	Indikatorfunktion zur Galoisgruppe $D_{l/2}$
$Div(\mathcal{C})$	Divisorengruppe einer algebraischen Kurve $\mathcal{C}$
$Div^0(\mathcal{C})$	Gruppe der Divisoren vom Grad 0 von $\mathcal{C}$
$div(f)$	Hauptdivisor einer Funktion $f \in \bar{K}(\mathcal{C})^\times$
E	elliptische Kurve über $\bar{K}$
E_l	Kubertkurven: parametr. ellipt. Kurven mit Punkt der Ordnung l
$E[m]$	Untergruppe von E aller Torsionspunkte, deren Ordnung m teilt
E/K	über K definierte elliptische Kurve
$E(K)$	K-rationale Punkte einer elliptischen Kurve E
E_{tors}	Torsionsuntergruppe einer elliptischen Kurve E
$E(K)_{tors}$	Gruppe der K-rationalen Torsionspunkte von E
$End(E)$	Endomorphismenring einer elliptischen Kurve E
$End_K(E)$	Ring der über K definierten Endomorphismen von E/K
F_l	Polynom mit Galoisgruppe D_l für $3 \leq l \leq 10$ und $l = 12$
$\tilde{F}_l$	vereinfachtes Polynom mit Galoisgruppe D_l
g	Geschlecht eines Funktionenkörpers oder einer algebr. Kurve
$G_{l,i}$	Polynome mit Galoisgruppe C_l

$\mathcal{H}$	obere Halbebene von $\mathbb{C}$
$\mathcal{H}^*$	erweiterte obere Halbebene: $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$
H_l	Polynome mit Galoisgruppe $D_{l/2}$
$H^0(G, E)$	0-te Kohomologiegruppe eines G-Moduls E
$H^1(G, E)$	1-te Kohomologiegruppe eines G-Moduls E
I	Ideal in $\bar{K}[X]$
i_Q	Albanese-Einbettung von $\mathcal{C}$ in $J_\mathcal{C}$
$I(V)$	Ideal in $\bar{K}[X]$, das zu einer algebraischen Menge V gehört
$\Im(\omega)$	Imaginärteil einer komplexen Zahl $\omega \in \mathbb{C}$
$j(E)$	j-Invariante einer elliptischen Kurve E
$J_\mathcal{C}$	Jacobische Varietät einer algebraischen Kurve $\mathcal{C}$
J_E	Jacobische Varietät einer elliptischen Kurve E
$J_\mathcal{C}(K)$	über K definierte Jacobische Varietät von $\mathcal{C}$
J_{tors}	Torsionsuntergruppe einer Jacobischen Varietät $J_\mathcal{C}$
$J(K)_{tors}$	Gruppe der K-rationalen Torsionspunkte einer Jacobischen Varietät
$J_0(N)$	Jacobische Varietät einer Modulkurve $X_0(N)$
K	algebraischer Zahlkörper
$\bar{K}$	algebraischer Abschluss von K
$K^\times$	Gruppe der multiplikativen Einheiten von K
$K[V]$	affiner Koordinatenring $K[X]/I(V/K)$ für eine algebr. Menge V
$K(V)$	Funktionenkörper von V/K, also Quotientenkörper von $K[V]$
$K[X]$	Polynomring in n Variablen: $X = (x_1, \ldots, x_n)$
$\bar{K}[\mathcal{C}]_P$	Lokalisierung von $\bar{K}[\mathcal{C}]$ nach M_P
l	Torsionsordnung eines Punktes
L	algebraischer Funktionenkörper über $K(x)$
$\mathcal{L}(D)$	Riemann-Roch-Raum eines Divisors D
M_P	Ideal aller Funktionen $f \in \bar{K}[\mathcal{C}]$, mit $f(P) = 0$ für $P \in \mathcal{C}$
$\mathbb{N}$	Menge der natürlichen Zahlen
O_K	Maximalordnung eines algebraischen Zahlkörpers K
$\mathcal{O}$	Punkt im Unendlichen einer (hyper-)elliptischen Kurve
$\mathcal{O}^+, \mathcal{O}^-$	Punkte im Unendlichen von $\mathcal{C} : y^2 = f(x)$, falls $deg\, f(x)$ gerade

P	Punkt auf einer algebr. Kurve oder Stelle eines Funktionenkörpers
$\wp$	Weierstraßsche p-Funktion
$\mathbb{P}^n$	n-dimensionaler projektiver Raum über $\bar{K}$
$\mathbb{P}^n(K)$	K-rationale Punkte in $\mathbb{P}^n$
$\mathbb{P}(1,a,1)$	gewichteter projektiver Raum der Dimension 2
$\mathrm{Pic}(\mathcal{C})$	Divisorengruppe einer algebraischen Kurve $\mathcal{C}$
$\mathrm{Pic}^0(\mathcal{C})$	Gruppe der Divisoren vom Grad 0 von $\mathcal{C}$
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{Q}^\times$	multiplikative Einheiten in $\mathbb{Q}$
$\mathbb{R}$	Körper der reellen Zahlen
$\mathcal{R}$	Ring/Ordnung in einem algebr. Zahl- oder Funktionenkörper
$r_l(Cl_K)$	l-Rang der Idealklassengruppe Cl_K eines Zahlkörpers K
$\Re(\omega)$	Realteil einer komplexen Zahl $\omega \in \mathbb{C}$
$SL_2(\mathbb{Z})$	2×2-Matrizen mit Einträgen aus $\mathbb{Z}$ und Determinante 1
t	uniformisierendes Element einer Stelle P oder an einem Punkt $P \in \mathcal{C}$
V_4	Kleinsche Vierergruppe
V_I	algebraische Menge zu einem Ideal $I \subset \bar{K}[X]$
V/K	über K definierte algebraische Menge
$V(K)$	K-rationale Punkte einer algebraischen Menge V
v_P	diskrete Bewertung zu einer Stelle P eines Funktionenkörpers
$X_0(N)$	(kompaktifizierte) Modulkurve
$X_1(N)$	(kompaktifizierte) Modulkurve
$X_0(N)^*$	Modulkurve $X_0(N)$ modulo der Atkin-Lehner-Involution
$X_0(N)_\mathbb{Q}$	über $\mathbb{Q}$ definierte Modulkurve $X_0(N)$
$X_0(N)_\mathbb{Q}(\mathbb{C})$	$\mathbb{C}$-rationale Punkte von $X_0(N)_\mathbb{Q}$
$Y_0(N)$	nicht kompakte Modulkurve
$\mathbb{Z}$	Ring der ganzen Zahlen
$\mathbb{Z}[\rho]$	von ρ erzeugte Gleichungsordnung eines Zahlkörpers $K = \mathbb{Q}(\rho)$

Index

A

abelsche Varietät 140
absolut einfache Jac. Varietät 16
affin
– algebraische Menge 138
– Koordinatenring 139
– Raum 138
– Varietät 139
Albanese-Einbettung 14
algebraische Kurve 142
algebraische Menge
– affin 138
– projektiv 140
– über K definiert 139
Atkin-Lehner-Involution 156

B

Bewertung
– ord_P 143
– v_P 136
Bewertungsring 136
Brumer, Armand 52

C

CKR-Vermutung 29

D

Darmon, Henri 52
Dedekind-Kriterium 76
definiert über K
– algebraische Menge 139
– Divisor 146
– projektive Variet. 140
definiert an P
– Funktion 146
– rationale Abbildung 145
Dehomogenisierung 141
Dimension
– Divisor 138
– Jacobische Varietät 16
– Varietät 139
diskrete Bewertung
– ord_P 143
– v_P 136
Diskriminante e. ellipt. Kurve 4
Divisor
– äquivalenter 137
– Dimension 138
– einer Kurve 146
– eines Funktionenkörpers 136
– ggT 17
– Grad 137, 146
– Ordnung an P 146
– reduziert 17
– semi-reduziert 17
– über K definiert 146
Divisorengruppe
– einer Kurve 146
– eines Funktionenkörpers 137
Divisorenklassengruppe
– einer Kurve 147
– eines Funktionenkörper 137

E

einfache Jacobische Varietät 16
– Kontrolle 16
elliptische Kurve 144
– Diskriminante 4

– Gitter ... 149
– Gruppengesetz ... 3
– Jacobische Varietät ... 2
– j-Invariante ... 4
– kompl. Multiplikation ... 6
– Mordell-Weil-Gruppe ... 8
– Quotientenkurve ... 6, 85
– Rang ... 8
– Torsionsuntergruppe ... 7
Endomorphismenring ... 6

F

Familie von Shanks ... 89
Flynn-Vermutung ... 27
Fundamentalbereich
– von $\mathcal{H}/SL_2(\mathbb{Z})$ ... 150
Funktionenkörper ... 135
– einer Varietät ... 139
– Geschlecht ... 138
– rationaler ... 135
– Stelle ... 136

G

Geschlecht
– Funktionenkörper ... 138
– Kurve ... 144
gewichteter projektiver Raum ... 19
ggT zweier Divisoren ... 17
Gitter
– elliptische Kurve ... 149
– in $\mathbb{C}$ ... 148
glatte Kurve ... 142
Grad
– Divisor einer Kurve ... 146
– einer Stelle ... 137
– eines Divisors ... 137
– eines Morphismus ... 145
Gras, Marie-Nicole ... 92
Gruppengesetz e. ellipt. Kurve ... 3

H

Hauptdivisor
– Funktionenkörper ... 137
– Kurve ... 147
homogenes Ideal ... 140
homogenes Polynom ... 140
Homogenisierung ... 141
homothetisch ... 148
hyperelliptische Kurve ... 144
– Dimension ... 16
– Punktgruppe ... 16

I

Igusa-Invarianten ... 15
Indikatorfunktion
– C_l ... 82
– $D_{l/2}$ ... 97
Invarianten einer hyperell. Kurve 15
Involution ... 156
Isogenie ... 5
– nicht-trivial ... 5
isomorphe Kurven ... 145

J

Jacobische Varietät ... 147
– absolut einfach ... 16
– einer elliptischen Kurve ... 2
– einfache ... 16
– – Kontrolle ... 16
– Konstruktion reduzibler J.V. ... 16
– reduzibel ... 16
– vollständig zerlegt ... 16
j-Invariante e. ellipt. Kurve ... 4

K

Kamienny, Sheldon ... 8
Kohomologiegruppen ... 87
komplexe Multiplikation ... 6
Kongruenzuntergruppe $\Gamma_0(N)$ .. 151
Koordinatenring – affin ... 139
Kubert-Kurven ... 10
Kurve ... 142
– Divisor ... 146
– Divisorengruppe ... 146

– Divisorenklassengruppe 147
– elliptisch 144
– Geschlecht 144
– glatt 142
– Grad eines Divisors 146
– Hauptdivisor 147
– hyperelliptisch 144
– isomorph 145
– Lokalisierung an P 143
– Picard-Gruppe 147
– uniformisier. Element an P ... 143

L

Lokalisierung von $\mathcal{C}$ an P 143

M

m-Torsionsuntergruppe von E 7
Manin-Mumford-Vermutung 14
Martinais, Dominique 52
Mazur, Barry 8
Modulraum 13
Mordell-Vermutung 14
Mordell-Weil-Gruppe von E 8
Mordell-Weil-Gruppe von V 140
Morphismus 145
– Grad 145

N

nicht-triviale Isogenie 5
Nullstelle
– einer Funktion 136
– einer Funktion an P 146
– Ordnung 136

O

obere Halbebene $\mathcal{H}$ 148
Obreschkoff, Nikola 66
Ordnung
– einer Funktion an P 146
– eines Divisors an P 146
– von Null-/Polstelle 136

P

Pell-Gleichung 42
Picard-Gruppe von $\mathcal{C}$ 147
Polstelle
– einer Funktion 136
– einer Funktion an P 146
– Ordnung 136
projektiv
– Abschluss 141
– algebraische Menge 140
– gewichteter Raum 19
– Raum 139
– Varietät 140
Punkte im Unendlichen 142
Punkte im Unendlichen $\mathcal{O}^{\pm}$ 19
Punktgruppe von $\mathcal{C}$ 16

Q

Quotientenkurve 6
Quotientenkurven (Vélu) 85

R

Rang von E 8
rationale Abbildung 144
– an P definiert 145
rationale Punkte 139
rationaler Funktionenkörper 135
reduzible Jacobische Varietät 16
– Konstruktion 16
reduzierter Divisor 17
reguläre Funktion 146
Riemann-Roch-Raum 137

S

Satz von Sturm 64
Schneps, Leila 52
Schrankensatz 9
Selmergruppe 87
semi-reduzierter Divisor 17
Shanks, Daniel 89
Shimura-Untergruppe 29
singulärer Punkt 142
Spitzen von $\mathcal{H}^*/SL_2(\mathbb{Z})$ 151

Spitzen-Untergruppe 29
Stelle
– eines Funktionenkörpers 136
– Grad 137
– uniformisierendes Element 136
Stichtenoth, Henning 135
Sturm, Satz von 64

T

Tate-Shafarevich-Gruppe 87
Torsionsuntergruppe von E 7

U

uniformisierendes Element
– einer Stelle 136
– für eine Kurve an P 143

V

Varietät
– abelsche 140
– absolut einfache Jacobische V.. 16
– affine 139
– Dimension 139
– einfache Jacobische Varietät ... 16
– – Kontrolle 16
– Funktionenkörper 139
– Jacobische 147
– Jacobische V. e. ellipt. Kurve ... 2
– Konstruktion reduzibler Jac. V. 16
– Mordell-Weil-Gruppe 140
– projektive 140
– reduzible Jacobische V..... 16
– vollständig zerlegte Jac. V..... 16
Vélu, Jacques 84
Vermutung
– Coleman-Kaskel-Ribet 29
– Flynn 27
– Manin-Mumford 14
– Mordell 14

W

Weierstraßgleichung 2
Weierstraßpunkt 28
Weierstraßsche $\wp$-Funktion 148

X

$X_0(1)$ 151
$X_0(11)$ 152
$X_0(37)$ 30
$X_0(N)$ über $\mathbb{Q}$ 154
$X_1(13)$ 27
$X_1(18)$ 27
$X_1(N)$ 155

Y

$Y_0(1)$ 150

Literaturverzeichnis

Das Literaturverzeichnis ist alphabetisch nach dem ersten Autor geordnet. Innerhalb des Werkes eines Autors sind die zitierten Publikationen chronologisch nach Erscheinungsdatum, beginnend mit dem ältesten Werk, sortiert. *Kursiv* ist immer der Titel des (übergeordneten) Werkes gedruckt, das ist der Buchtitel bzw. bei einem Artikel der Zeitschriftentitel. Veröffentlichungen, die (nur) elektronisch verfügbar sind, wurden unter Angabe der Internetseite zitiert.

[1] Baker, Matthew: *Torsion Points on Modular Curves*, Thesis, Berkeley 1994.
http://www.math.gatech.edu/~mbaker/THESIS.html 14, 29, 156

[2] Belabas, Karim: On quadratic fields with large 3-rank, in: *Math. Comput.* 73.248, 2004, 2061–2074. 101

[3] Boxall, John; Grant, David; Leprévost, Franck: 5-torsion points on curves of genus 2, in: *J. Lond. Math. Soc., II Ser.* 64.1, 2001, 29–43. 34

[4] Cassels, John W.S.; Flynn, E. Victor: *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, (London Mathematical Society Lecture Notes Series 230), Cambridge Univ. Press 1996. 16, 31

[5] Cantor, David: Computing in the Jacobian of a Hyperelliptic Curve, in: *Math. Comput.* 48.117, 1987, 95–101. 17, 18

[6] Cohen, Henri: *A Course in Computational Algebraic Number Theory*, (Graduate Texts in Mathematics 138), Springer 1993. 64, 80

[7] Craig, Maurice: A construction for irregular discriminants, in: *Osaka J. Math.* 14, 1977, 365–402. 101

[8] Darmon, Henri: Une famille de polynômes liées à $X_0(5)$, *unveröffentlichte Notizen*, 1993. 52

[9] Dem'yanenko, V.A.: The torsion of elliptic curves over cyclotomic fields, in: *St. Petersburg. Math. J.* 9.5, 1998, 931–943. 9

[10] Edixhoven, Bas: Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur), in: *Astérisque* 227, (Séminaire Bourbaki 1993/94), 1995, 209–227. 9

[11] Elkies, Noam D.: *Curves of genus 2 over Q whose Jacobians are absolutely simple abelian surfaces with torsion points of high order.* www.math.harvard.edu/~elkies/g2_tors.html 28

[12] Faltings, Gerd: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, in: *Invent. Math.* 73.3, 1983, 349–366. 14

[13] Fermigier, Stéfane: Un exemple de courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 19, in: *C. R. Acad. Sci. Paris, Sér. I*, 315.6, 1992, 719–722. 8

[14] Fermigier, Stéfane: Exemples de courbes elliptiques de grand rang sur $\mathbb{Q}(t)$ et sur $\mathbb{Q}$ possédant des points d'ordre 2, in: *C. R. Acad. Sci. Paris, Sér. I*, 322.10, 1996, 949–952. 10

[15] Fermigier, Stéfane: Une courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 22, in: *Acta Arith.* 82.4, 1997, 359–363. 8

[16] Flynn, E. Victor: Large rational torsion on abelian varieties, in: *J. Number Theory* 36.3, 1990, 257–265. 26, 27

[17] Flynn, E. Victor: Sequences of rational torsions on abelian varieties, in: *Invent. Math.* 106.2, 1991, 433–442. 28

[18] Fujita, Yasutsugu: *Torsion of elliptic curves over number fields*, (Tohoku Mathematical Publications 27), Thesis, Tohoku University 2003. http://www.math.tohoku.ac.jp/tmj/PDFofTMP/tmp27.pdf 9

[19] Galbraith, Steven D.: *Equations for modular Curves*, Thesis, University of Oxford 1996. http://www.isg.rhul.ac.uk/~sdg/thesis.html 154, 156

[20] Gaudry, Pierrick: *Mémoire de DEA – Courbes hyperelliptiques et cryptographie*, Laboratoire d'Informatique, Palaiseau 1995. 18

[21] Geißler, Katharina: *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, Thesis, TU Berlin 2003. 81, 97

[22] González Rovira, Josep: Equations of hyperelliptic modular curves, in: *Ann. Inst. Fourier, Grenoble* 41.4, 1991, 779–795. 29, 44, 154

[23] Gras, Marie-Nicole: Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$, in: *Publ. Math. Fac. Sci. Besançon* 2, 1978. 92

[24] Griffiths, Phillip; Harris, Joseph: *Principles of algebraic geometry*, Wiley 1978. 13

[25] Hartshorne, Robin: *Algebraic geometry*, (Graduate Texts in Mathematics 52), Springer 1977. 13

[26] Hasegawa, Yuji: Hyperelliptic modular curves $X_0^*(N)$, in: *Acta Arith.* 81.4, 1997, 369–385. 156

[27] Hindry, Marc; Silverman, Joseph H.: *Diophantine Geometry*, (Graduate Texts in Mathematics 201), Springer 2000. 2, 7, 8, 9, 13, 14, 15, 16, 26, 28, 102, 144, 145, 147

[28] Howe, Everett W.; Leprévost, Franck; Poonen, Bjorn: Large torsion subgroups of split Jacobians of curves of genus two or three, in: *Forum Math.* 12.3, 2000, 315–364. 26, 36

[29] Igusa, Jun-ichi: Arithmetic variety of moduli for genus two, in: *Ann. Math., Ser. II*, 72, 1960, 612–649. 15, 37

[30] Jeon, Daeyeol; Kim, Chang H.; Schweizer, Andreas: On the torsion of elliptic curves over cubic number fields, in: *Acta Arithm.* 113.3, 2004, 291–301. 9, 155

[31] Kamienny, Sheldon: Torsion points on elliptic curves and q-coefficients of modular forms, in: *Invent. Math.* 109.2, 1992, 221–229. 8

[32] KANT: http://www.math.tu-berlin.de/~kant 47, 63, 65, 76

[33] Kihel, Omar: Groupe des unités pour des extensions diédrales complexes de degré 10 sur $\mathbb{Q}$, in: *J. Théor. Nombres Bordeaux* 13.2, 2001, 469–482. 52

[34] Knapp, Anthony W.: *Elliptic Curves*, (Mathematical Notes 40), Princeton Univ. Press 1992. 144, 151, 153

[35] Kubert, Daniel Sion: Universal bounds on the torsion of elliptic curves, in: *Proc. London Math. Soc.* 3.33, 1976, 193–237. 10

[36] Kulesz, Leopoldo: Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$, in: *Acta Arith.* 108.4, 2003, 339–356. 10

[37] Lecacheux, Odile: Rang de courbes elliptiques sur $\mathbb{Q}$ avec un groupe de torsion isomorphe à $\mathbb{Z}/5\mathbb{Z}$, in: *C. R. Acad. Sci. Paris, Sér. I,* 332.1, 2001, 1–6. 10

[38] Lehner, Joseph; Newman, Morris: Weierstraß points of $\Gamma_0(n)$, in: *Ann. Math., Ser. II,* 79, 1964, 360–368. 30

[39] Leprévost, Franck: Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13, in: *C. R. Acad. Sci. Paris, Sér. I*, 313.7, 1991, 451–454. 27, 38

[40] Leprévost, Franck: Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21, in: *C. R. Acad. Sci. Paris, Sér. I*, 313.11, 1991, 771–774. 27, 28, 38

[41] Leprévost, Franck: Torsion sur des familles de courbes de genre g, in: *Manuscr. Math.* 75.3, 1992, 303–326. 15, 28, 42

[42] Leprévost, Franck: Courbes modulaires et 11-rang de corps quadratiques, in: *Exp. Math.* 2.2, 1993, 137–146. 101, 102

[43] Leprévost, Franck: Points rationnels de torsion de jacobiennes de certaines courbes de genre 2, in: *C. R. Acad. Sci. Paris, Sér. I*, 316.8, 1993, 819–821. 27, 28

[44] Leprévost, Franck: Famille de courbes hyperelliptiques de genre g munies d'une classe de diviseurs rationnels d'ordre $2g^2+4g+1$, in: David, Sinnou (Hrsg.): *Séminaire de théorie des nombres, Paris, 1991-92*, (Progress in Mathematics 116), Birkhäuser 1994, 107–119. 15, 28, 42

[45] Leprévost, Franck: Jacobiennes de certaines courbes de genre 2: torsion et simplicité. in: *J. Théor. Nombres Bordeaux* 7.1, 1995, 283–306. 16, 25, 31, 37

[46] Leprévost, Franck: Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes, in: *J. Reine Angew. Math.* 473, 1996, 59–68. 15, 27, 42

[47] Leprévost, Franck: Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 1$, in: *Manuscr. Math.* 92.1, 1997, 47–63. 15, 42

[48] Leprévost, Franck; Pohst, Michael E.; Schöpp, Andreas: Familles de polynômes liées aux courbes modulaires $X_1(l)$ unicursales et points rationnels non-triviaux de courbes elliptiques quotient, in: *Acta Arith.* 110.4, 2003, 401–410. viii, 52, 90, 91, 92, 93, 94, 95, 110

[49] Leprévost, Franck; Pohst, Michael E.; Schöpp, Andreas: Rational Torsion of $J_0(N)$ for Hyperelliptic Modular Curves and Families of Jacobians of Genus 2 and Genus 3 Curves with a Rational Point of Order 5, 7 or 10, in: *Abh. Math. Sem. Univ. Hamburg* 74, 2004, 193–203. viii, 40, 44

[50] Leprévost, Franck; Pohst, Michael E.; Schöpp, Andreas: Units in some parametric families of quartic fields, erscheint in: *Acta Arith.*, 2006. viii

[51] Lutz, Elisabeth: Sur l'equation $y^2 = x^3 - A\,x - B$ dans les corps p-adic, in: *J. Reine Angew. Math.* 177, 1937, 238–247. 8

[52] MAGMA: http://magma.maths.usyd.edu.au 26, 47, 49, 59, 65, 119

[53] MAPLE: http://www.maplesoft.com 47, 49, 88, 95

[54] Martinais, Dominique; Schneps, Leila: Polynômes à groupe de Galois diédral, in: *Sém. Théor. Nombres Bordeaux, Sér. II,* 4.1, 1992, 141–153. 52

[55] Mazur, Barry: Modular curves and the Eisenstein ideal, in: *Publ. Math. Inst. Hautes Étud. Sci.* 47, 1977, 33–186. 8

[56] Menezes, Alfred; Wu, Yi-Hong; Zuccherato, Robert J.: An elementary introduction to hyperelliptic curves, in: Koblitz, Neal: *Algebraic aspects of cryptography*, Springer 1998, 155–178. 17, 147

[57] Merel, Loïc: Bornes pour la torsion des courbes elliptiques sur les corps de nombres, in: *Invent. Math.* 124.1-3, 1996, 437–449. 9

[58] Mestre, Jean-François: Corps euclidiens, unités exceptionnelles et courbes élliptiques, in: *J. Number Theory* 13.2, S. 123–137, 1981. 155

[59] Mestre, Jean-François: Construction d'une courbe elliptique de rang $\geq$ 12, in: *C. R. Acad. Sci. Paris, Sér. I*, 295, 1982, 643–644. 8

[60] Mestre, Jean-François: Groupes de classes d'idéaux non cycliques de corps de nombres, (Théorie des nombres, Sémin. Delange-Pisot-Poitou, Paris 1981/82), in: *Prog. Math.* 38, 1983, 189–200. 102

[61] Mestre, Jean-François: Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang ≥ 15, in: *C. R. Acad. Sci. Paris, Sér. I*, 314.6, 1992, 453–455. 8

[62] Mestre, Jean-François: Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3, in: *C. R. Acad. Sci. Paris, Sér. I*, 315.4, 1992, 371–374. 101

[63] Mestre, Jean-François: 3-rangs de coprs quadratiques, (Un exposée au séminaire de théorie des nombres de Chevaleret le 7 février 2005): www.math.jussieu.fr/projets/tn/STN/05/mestre-05.html 101

[64] Mumford, David: *Curves and Their Jacobians*, University of Michigan Press 1978. 13

[65] Murabayashi, Naoki: On normal forms of modular curves of genus 2, in: *Osaka J. Math* 29, 1992, 405–418. 29, 154

[66] Nagao, Koh-ichi; Kouya, Tomonori: An example of elliptic curve over $\mathbb{Q}$ with rank > 21, in: *Proc. Japan Acad., Ser. A*, 70.4, 1994, 104–105. 8

[67] Nagao, Koh-ichi: Construction of high-rank elliptic curves with a non-trivial torsion point, in: *Math. Comput.*, 66.217, 1997, 411–415. 10

[68] Nagell, Trygve: Zur Arithmetik der Polynome, in: *Abh. Math. Sem. Univ. Hamburg* 1, 1922, 179–194. 58

[69] Nagell, Trygve: Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre, in: *Skr. Norske Vid.-Akad. Oslo* 1, 1935, 1–25. 8

[70] Nakamula, Ken: Certain Quartic Fields with Small Regulators, in: *J. Number Theory* 57, 1996, 1–21. 61

[71] Obreschkoff, Nikola: *Verteilung und Berechnung der Nullstellen reeller Polynome*, (Hochschulbücher für Mathematik 55), Dt. Verlag der Wissenschaften 1963. 66

[72] Ogg, Andrew P.: Functional Equations of Modular Forms, in: *Math. Ann.* 183, 1969, 337–340. 154

[73] Ogg, Andrew P.: Rational points on certain elliptic modular curves, in: Diamond, Harold G. (Hrsg.): *Analytic Number Theory*, (Proc. Symp. Pure Math. 24), American Math. Soc. 1973, 221–231. 27, 29

[74] Ogg, Andrew P.: Hyperelliptic modular curves, in: *Bull. Soc. Math. France* 102, 1974, 449–462. 29, 30, 156

[75] Parent, Pierre: Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, in: *J. Reine Angew. Math.* 506, 1999, 85–116. 9

[76] Parent, Pierre: Torsion des courbes elliptiques sur les corps cubiques, in: *Ann. Inst. Fourier* 50.3, 2000, 723–749. 9

[77] PARI: http://pari.math.u-bordeaux.fr 47

[78] Pohst, Michael E.; Zassenhaus, Hans J.: *Algorithmic algebraic number theory*, (Encyclopedia of Mathematics and its applications), Cambridge University Press 1997. 33, 75, 76

[79] Poonen, Bjorn: Computational aspects of curves of genus at least 2, in: Cohen, Henri: *Algorithmic Number Theory*, (ANTS II – Lecture Notes in Computer Science 1122), Springer 1996, 283–306. 15

[80] Poonen, Bjorn: Computing torsion points on curves, in: *Exp. Math.* 10.3, 2001, 449–465. 28

[81] Quer, Jordi: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, in: *C. R. Acad. Sci. Paris, Sér. I*, 305, 1987, 215–218. 101

[82] Raynaud, Michel: Courbes sur une variété abélienne et points de torsion, in: *Invent. Math.* 71, 1983, 207–233. 14

[83] Reid, Miles: Graded rings and varieties in weighted projective space. http://www.maths.warwick.ac.uk/~miles/surf/more/grad.pdf 19

[84] Schoof, René J.: Class groups of complex quadratic fields, in: *Math. Comput.* 41.163, 1983, 295–302. 101

[85] Shanks, Daniel: The simplest cubic fields, in: *Math. Comput.* 28, 1974, 1137–1152. 89

[86] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves*, (Graduate Texts in Mathematics 106), Springer 1986. v, 1, 2, 3, 4, 5, 6, 7, 8, 15, 87, 139, 141, 143, 144, 145, 146, 147, 149, 152, 155

[87] Silverman, Joseph H.: *Advanced Topics in the Arithmetic of Elliptic Curves*, (Graduate Texts in Mathematics 151), Springer 1994. v, 148, 150, 151

[88] Solderitsch, James J.: Quadratic fields with special class groups, in: *Math. Comput.* 59.200, 1992, 633–638. 101

[89] Spallek, Anne-Monika: *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, Thesis, Unversität Essen 1994. 18

[90] Stichtenoth, Henning: *Algebraic Function Fields and Codes*, (Universitext), Springer 1993. 14, 135, 136, 137, 142, 144

[91] Stoll, Michael: Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil rank at least 19, in: *C. R. Acad. Sci. Paris, Sér. I*, 321.10, 1995, 1341–1344. 16, 37

[92] van der Waerden, Bartel L.: Zur algebraischen Geometrie. XI. Projektive und birationale Äquivalenz und Moduln von ebenen Kurven, in: *Math. Ann.* 114, 1937, 683–699. 13

[93] Vélu, Jacques: Isogénies entre courbes elliptiques, in: *C. R. Acad. Sci. Paris, Sér. A*, 273, 1971, 238–241. 84

[94] Webb, William A.; Yokota, Hisashi: Polynomial Pell's equation - II, in: *J. Number Theory* 106, 2004, 128–141. 42, 43

[95] Weston, Tom: *The modular curves* $X_0(11)$ *and* $X_1(11)$. http://www.math.umass.edu/~weston/ep.html 152, 153

[96] Yamamoto, Yoshihiko: On unramified Galois extensions of quadratic number fields, in: *Osaka J. Math.* 7, 1970, 57–76. 101

Zusammenfassung

Sei $f(x) \in K[x]$ ein normiertes Polynom vom Grad $2g+1$ oder $2g+2$ ohne mehrfache Nullstellen über einem Zahlkörper K. Die Kurve

$$\mathcal{C} \; : \; y^2 = f(x)$$

ist eine elliptische Kurve für $g = 1$ bzw. eine hyperelliptische Kurve für $g \geq 2$.

Es werden (für $g \geq 2$) parametrisierte Kurvenfamilien berechnet, deren Jacobische Varietäten eine Divisorenklasse der Ordnung $l = 5, 7, 10$ besitzen. Außerdem werden für $3 \leq l \leq 10$ und $l = 12$ Familien von Zahlkörpern konstruiert, deren Galoisgruppe die Diedergruppe D_l ist. Für $l = 4, 5$ bei Signatur $(2, 1)$ bzw. $(1, 2)$ werden Fundamentaleinheiten für die parametrisierten Körper bestimmt. Darüber hinaus werden für $3 \leq l \leq 6$ Unterfamilien der Zahlkörper angegeben, deren Galoisgruppe zyklisch mit Ordnung l ist.

Ausgangspunkt der Kurvenberechnung ist die Polynomgleichung $P^2 - Q^2 F = c \in K^\times$. Es wird bewiesen, dass die Jacobische Varietät der zur Polynomgleichung gehörenden Kurve $y^2 = F(x)$ eine Divisorenklasse besitzt, deren Ordnung den Grad von P teilt. Familien hyperelliptischer Kurven werden konstruiert, deren Jacobische Varietäten eine Divisorenklasse der Ordnung $5, 7$ bzw. 10 besitzen. Es wird gezeigt, dass in diesen Familien die Modulkurven $X_0(N)$ mit $N = 22, 29, 31, 41$ liegen. Im Zusammenhang mit der Konstruktion steht für $X_0(N)$ mit Gleichung $y^2 = F(x)$ eine Faktorisierung $F(x) = F_1(x)\, F_2(x)$, die auch für $N = 23, 47, 59, 71$ angegeben wird.

Zur Konstruktion von Zahlkörperfamilien mit Galoisgruppe D_l wird ein Torsionspunkt A der Ordnung l einer parametrisierten Familie elliptischer Kurven (Kubert-Kurven) genutzt. Die x-Koordinate der Punkte $P \oplus iA$ für $1 \leq i \leq l$ und einen beliebigen, nicht-rationalen Punkt P ergeben das erzeugende Polynom in der Form $F_l = \prod (x - x(P \oplus iA))$, dessen Galoisgruppe die Diedergruppe D_l ist. Für $l = 4$ und Signatur $(2, 1)$ bzw. für $l = 5$ und Signatur $(1, 2)$ werden Systeme von Fundamentaleinheiten in der von F_l erzeugten Gleichungsordnung $\mathbb{Z}[\rho]$ angegeben. Der Beweis der Fundamentalität für $l = 5$ erfordert dabei Abschätzungen der komplexen Nullstellen von F_5.

Die Bestimmung von Zahlkörperfamilien mit Galoisgruppe C_l erfolgt über eine Indikatorfunktion, die in engem Zusammenhang zu Quotientenkurven steht. C_l-Zahlkörper werden für $3 \leq l \leq 6$ angegeben.

Abschließend werden ausgehend von den konstruierten hyperelliptischen Kurven 49 imaginärquadratische Zahlkörper mit $r_5(Cl_K) = 3$ und 67 Zahlkörper mit $r_7(Cl_K) = 2$ berechnet.