

# Belyi-Morphismen und konstante Koeffizienten von nicht-holomorphen Eisensteinreihen

Diplomarbeit

Humboldt-Universität zu Berlin  
Mathematisch-Naturwissenschaftliche Fakultät II  
Institut für Mathematik

eingereicht von: Anna Elisabeth Posingies  
geboren am: 08. September 1980 in Berlin  
1. Gutachter: Prof. Ulf Kühn  
2. Gutachter: PD Dr. Werner Kleinert  
Berlin, den 16. Februar 2007



# Inhaltsverzeichnis

<b>Einleitung</b>	<b>5</b>
<b>1 Definitionen und Grundlagen</b>	<b>9</b>
1.1 Elliptische Kurven . . . . .	9
1.2 Die Modulgruppe und ihre Untergruppen . . . . .	12
<b>2 Belyi-Morphismen für elliptische Kurven</b>	<b>16</b>
2.1 Der Satz von Belyi . . . . .	16
2.2 Anwendung auf elliptische Kurven . . . . .	17
2.3 Äquivalenzen zu Belyi-Paaren . . . . .	22
<b>3 Die elliptische Kurve <math>E : y^2 = x^3 + 5x + 10</math></b>	<b>26</b>
3.1 Eigenschaften von $E$ . . . . .	26
3.2 Die zu $(E, \beta)$ assoziierte Gruppe $\Gamma_E$ . . . . .	30
3.3 Algorithmus zum Testen der Zugehörigkeit zu $\Gamma_E$ . . . . .	35
3.4 Untersuchung der Gruppe $\Gamma_E$ . . . . .	37
<b>4 Eisensteinreihen und Streumatrizen</b>	<b>41</b>
4.1 Definitionen . . . . .	41
4.2 Die Streumatrix zu $\Gamma(2)$ . . . . .	44
4.3 Die Streukonstanten zu $\Gamma(2)$ . . . . .	46
4.4 Doppelnebenklassen und Streumatrizen . . . . .	49
4.5 Ein Algorithmus zur Berechnung von Streumatrizen . . . . .	53
4.6 Die Streumatrix zur Gruppe $\Gamma_E$ . . . . .	54
4.7 Weitere Beispiele . . . . .	58
<b>5 Eigenschaften der berechneten Streumatrizen</b>	<b>65</b>
5.1 Jeder zweite Koeffizient ist null . . . . .	65
5.2 Gleiche Koeffizienten . . . . .	67
5.3 Lineare Abhängigkeiten . . . . .	70
5.4 Die Summe der Koeffizientenfunktionen zu einer Spitze . . . . .	74
5.5 Abschätzungen und Approximationen . . . . .	79

5.6	Total verzweigte Spitzen . . . . .	82
5.7	Berechnung von Streukonstanten . . . . .	86
<b>6</b>	<b>Eine arithmetische Anwendung der Streukonstanten</b>	<b>91</b>
6.1	Néron-Tate-Höhenpaarungen und Streukonstanten . . . . .	91
6.2	Der analytische Anteil der Höhe von $P = (1, 4) \in E$ . . . . .	92
<b>A</b>	<b>Anhang</b>	<b>100</b>
A.1	InGruppe.java . . . . .	100
A.2	Magma-Algorithmus . . . . .	101
	<b>Software</b>	<b>105</b>
	<b>Literatur</b>	<b>105</b>
	<b>Thesen</b>	<b>111</b>

## Einleitung

Die vorliegende Arbeit beschäftigt sich mit nicht-holomorphen Eisensteinreihen zu Untergruppen von  $SL_2(\mathbb{Z})$ , die über Belyi-Morphismen zu algebraischen Kurven definiert werden können. Dabei treten auch Nicht-Kongruenzgruppen auf. Insbesondere wird auf die konkrete Berechnung der konstanten Koeffizienten der Reihen eingegangen.

Im Jahr 1979 hat G. Belyi [Be] bewiesen, dass es zu jeder über  $\overline{\mathbb{Q}}$  definierten algebraischen Kurve  $K$  eine Überlagerung  $\beta$  in den  $\mathbb{P}^1$  gibt, die nur über drei Stellen verzweigt ist. Da die Kongruenzgruppe  $\Gamma(2)$  isomorph zur Fundamentalgruppe der Sphäre ohne drei Punkte ist, erlaubt es der Satz von Belyi, jedem Paar  $(K, \beta)$  eine Untergruppe  $\Gamma$  von  $\Gamma(2)$  zuzuordnen. Wie genau eine solche Zuordnung vorzunehmen ist, wird zum Beispiel von B. Birch in [Bi] sowie von G. Jones und D. Singerman in [JS] beschrieben. Dabei wird die Theorie der Kinderzeichnungen (Dessins d'Enfants) benutzt, die in den 80er Jahren von A. Grothendieck [Gr] begründet wurde. Kinderzeichnungen bieten eine Möglichkeit, das Verhalten von Überlagerungen in einfachen Graphen zu veranschaulichen.

Für elliptische Kurven gibt es für Belyi-Morphismen konkrete Konstruktionen von L. Khadjavi und V. Scharaschkin in [KS], die in dieser Arbeit noch erweitert werden.

Zu einer Untergruppe  $\Gamma \subset \Gamma(2)$  können nicht-holomorphe Eisensteinreihen betrachtet werden, wie T. Kubota sie in [Ku1] untersucht. Die Streumatrix zu einer Gruppe ist durch die konstanten Koeffizienten der Eisensteinreihen zu den verschiedenen Spitzen definiert. Die Arakelov-Theorie liefert Zusammenhänge zwischen der Streumatrix und der Arithmetik von algebraischen Kurven.

Zu den wichtigsten Ergebnissen dieser Arbeit zählt ein implementierter Algorithmus zum Berechnen von Koeffizienten von Streumatrizen, der von einer Gruppe, gegeben durch einen Morphismus von  $\Gamma(2)$  in eine Symmetriegruppe, ausgeht. Es lassen sich so endlich viele Koeffizienten der Einträge der Streumatrix berechnen. Dadurch kann die Streumatrix genähert werden. Der Algorithmus lässt sich mit leichten Abwandlungen auf alle Gruppen  $\Gamma$  anwenden, bei denen es möglich ist zu entscheiden, ob eine gegebene Matrix aus  $\Gamma(1)$  auch in  $\Gamma$  liegt. Die hier verwendete Darstellung der Untergruppen von  $\Gamma(2)$  durch Morphismen in Symmetriegruppen, erlaubt es auch Nicht-Kongruenzgruppen darzustellen und somit auch Koeffizienten zu Nicht-Kongruenzgruppen zu berechnen. Auch für die höheren Koeffizienten der Eisensteinreihen kann der Algorithmus Näherungen liefern. Dies jedoch ist nicht Gegenstand der vorliegenden Arbeit.

Bisher sind konkrete Berechnungen von Eisensteinreihen und Streumatrizen bis auf einzelne Spezialfälle nicht bekannt, siehe dazu A.B. Venkov [Ve] für zyklische Gruppen und V. K. Murty und D. Ramakrishnan [MR] für eine Algebraizitätsuntersuchung für höhere Koeffizienten. Außerdem hat sich D. Hejhal in [He] mit der Beschreibbarkeit von Streumatrizen zu den wichtigsten Kongruenzuntergruppen beschäftigt.

Ein weiteres Ergebnis der vorliegenden Arbeit ist, dass die Koeffizienten von Streumatrizen zu Unter- und Obergruppe eng miteinander verbunden sind. Auch wenn die einzelnen Koeffizienten unbekannt sind, kann doch immer eine Aussage über bestimmte Summen von Koeffizienten gemacht werden. Denn die Koeffizienten zu einer Obergruppe setzen sich aus den Koeffizienten der Untergruppe zusammen. So ist zum Beispiel die Summe über die Koeffizienten zu einer Spitze immer ein Vielfaches der Euler'schen  $\phi$ -Funktion, siehe dazu Satz 5.22. Als Konsequenz kann eine gewichtete Summe der Streukonstanten zu einer Spitze explizit angegeben werden.

Der Algorithmus wird auf eine Reihe dafür konstruierter Beispiele angewendet. Unter den betrachteten Gruppen befindet sich auch eine Nicht-Kongruenzuntergruppe. So entsteht umfangreiches Datenmaterial mit hunderten von Koeffizienten zu recht unterschiedlich gearteten Gruppen. Die Sichtung und die Auswertung der Tabellen führten zu vielen weiteren Untersuchungen und ergaben neue Ergebnisse (Kapitel 5).

Ausserdem sind eine Reihe weiterer Fragestellungen aufgeworfen worden, die weiterführende Forschungen motivieren.

Nach einigen einleitenden Definitionen in Kapitel 1 wird in Kapitel 2 zunächst die Konstruktion von Belyi-Morphismen behandelt. In Satz 2.11 wird für eine gegebene elliptische Kurve über  $\mathbb{Q}$  und eine endliche Menge von rationalen Punkten auf dieser Kurve eine Konstruktion für einen Belyi-Morphismus gegeben, der die Eigenschaft hat, dass der Morphismus in den gegebenen rationalen Punkten verzweigt ist. Im Gegensatz zu der Konstruktion, die G. Belyi in seinem Beweis vorschlägt, lässt sich die hier dargestellte Konstruktion einfach ausführen. Zusätzlich wird in Satz 2.12 der Grad des so konstruierten Belyi-Morphismus abgeschätzt. Im letzten Teil des Kapitels 2 wird beschrieben, wie von einem Belyi-Paar ausgehend eine Untergruppe von  $\Gamma(2)$  gefunden werden kann. Dabei wird das Vorgehen nach G. Jones und D. Singerman [JS] sowie J. Wolfart [Wo] vorgestellt.

Nach diesen allgemeinen Erläuterungen zu Belyi-Paaren wenden wir uns in Kapitel 3 einem konkreten Beispiel zu. Mit dem Belyi-Paar

$$E : y^2 = x^3 + 5x + 10, \quad \beta(x, y) = \frac{y(x - 5) + 16}{32}$$

ist aufgrund seiner einfachen Struktur gut zu arbeiten. Außerdem besitzt die

Kurve  $E$  eine unendliche Gruppe rationaler Punkte. Über Kinderzeichnungen wird die assoziierte Gruppe  $\Gamma_E \subset \Gamma(2)$  berechnet und untersucht. Aufgrund der Tatsache, dass bei dem Belyi-Paar  $(E, \beta)$  Punkte unendlicher Ordnung über den Verzweigungsstellen liegen, ist die Gruppe  $\Gamma_E$  keine Kongruenzgruppe.

In Kapitel 4 wenden wir uns Eisensteinreihen, Streumatrizen und Streukonstanten zu. In den ersten drei Teilen werden die wichtigsten Definitionen und Begriffe zu diesem Themenbereich geklärt und für die Gruppe  $\Gamma(2)$  als wichtiges Beispiel die Streumatrix und die Streukonstanten ausgerechnet. Nach dieser Einführung wird ein Algorithmus entwickelt, um die Koeffizienten der Einträge von Streumatrizen zu berechnen. Dazu ist die Berechnung eines Koeffizienten in Satz 4.17 auf die Durchführung eines endlichen Testes reduziert worden. Der entstandene Algorithmus 3 erlaubt die Berechnung von endlich vielen Koeffizienten der Streumatrix einer, nach dem Vorgehen aus Kapitel 2.3 konstruierten, Gruppe zu einem Belyi-Paar. Der Algorithmus ist implementiert und auf eine Reihe von Beispielen angewendet worden. In den Unterkapiteln 4.6 und 4.7 befinden sich Tabellen mit den ersten Koeffizienten.

Die berechneten Koeffizienten  $r_{jk}(c)$  motivieren aufgrund der großen Zahl von Regelmäßigkeiten, die zu beobachten ist, eine Reihe von Untersuchungen. Das Kapitel 5 beschreibt die wichtigsten gefundenen Eigenschaften von Streumatrizen.

Zunächst wird in 5.1 gezeigt, dass für Gruppen  $\Gamma \subset \Gamma(1)$  jeder zweite Koeffizient null ist. In den folgenden Unterkapiteln 5.2 und 5.3 wird zusammengetragen, welche Koeffizientenfunktionen gleich sind und welche lineare Abhängigkeiten zeigen. Bei diesen exakten Zusammenhängen bleiben die Erklärungsversuche auf der Ebene von Vermutungen.

Dies ändert sich in 5.4, wo nicht mehr einzelne Ergebnisse betrachtet werden, sondern immer mehrere Koeffizientenfunktionen auf einmal. Das fundamentale Ergebnis dieses Abschnittes ist eine Relation der Koeffizienten von Gruppen  $\Gamma$  und  $\Gamma'$ , falls  $\Gamma' \subset \Gamma$  eine Untergruppe ist. Wenn die Spitzen  $\{S_i\}_{i=1}^r$  der Untergruppe die Spitze  $S_j$  der Obergruppe bilden, gilt für die Koeffizienten eine Relation der Art

$$\sum_{i=1}^n r_{ik}^{\Gamma'}(c) = ar_{jk}^{\Gamma}(c)$$

mit  $a \in \mathbb{N}$ . Eine Folge dieser Verbindung ist die Tatsache, dass die Summe der Koeffizienten zu einer fixierten Spitze immer ein Vielfaches der Euler'schen  $\phi$ -Funktion ist. Auch die Ergebnisse der beiden folgenden Unterkapitel basieren auf der Relation der Koeffizienten. In 5.5 werden die Koeffizienten abgeschätzt, wobei sich herausstellt, dass das Wachstum höchstens linear ist,

und der Versuch einer Approximation durch die Euler'schen  $\phi$ -Funktion unternommen. Kapitel 5.6 beschäftigt sich mit total verzweigten Spitzen. Hat eine Gruppe eine total verzweigte Spitze, so sind die mit dieser Spitze zusammenhängenden Teile der Streumatrix explizit beschreibbar.

Abschließend werden in Abschnitt 5.7 die Konsequenzen für die Berechnung von Streukonstanten betrachtet. Streukonstanten zu total verzweigten Spitzen sind berechenbar. Außerdem lässt sich immer bestimmen, was die mit den Spitzenbreiten gewichtete Summe der Streukonstanten zu einer fixierten Spitze ist.

Am Ende der Arbeit wird noch gezeigt, wie sich die Ergebnisse anwenden lassen. U. Kühn gibt in [Kü2] eine Formel zur Berechnung von Höhenpaarungen mittels Streukonstanten an. Diese Berechnung wird für einen Punkt der Kurve  $E$  aus Kapitel 3 durchgeführt. Dabei werden unterschiedliche Aspekte der Ergebnisse aus Kapitel 5 benutzt.

Mein herzlicher Dank gilt zuallererst Prof. Ulf Kühn für seine umfangreiche und engagierte Betreuung. Unter den vielen anderen, die mich darin unterstützten, der Arbeit die vorliegende Form zu verleihen, sind noch zwei besonders hervorzuheben. Prof. George Shabats geduldige Erklärungen zum Thema Kinderzeichnungen erlaubten mir die Konstruktionen in dieser Arbeit zu vollenden und auf eine theoretische Basis zu stellen. Fritz Hörmann hat mit seinem Verständnis nicht-holomorpher Eisensteinreihen entscheidend zu den Beweisen einiger Beobachtungen beigetragen.

# 1 Definitionen und Grundlagen

In diesem einleitenden Kapitel werden für die Arbeit benötigte Definitionen und Grundlagen dargestellt. Dabei sind die zwei Themengebiete „elliptische Kurven“ und „die Modulgruppe und ihre Untergruppen“ zu unterscheiden.

## 1.1 Elliptische Kurven

In diesem Kapitel werden elliptische Kurven definiert, so, wie sie in dieser Arbeit vorkommen. Außerdem werden einige wichtige Eigenschaften eingeführt und Höhenfunktionen definiert. Die Hauptreferenz ist [Kn].

**Definition 1.1.** *Eine elliptische Kurve  $E/\mathbb{Q}$  ist eine nichtsinguläre, projektive Kubik über  $\mathbb{Q}$  mit einem ausgezeichneten Punkt  $\mathcal{O}$  mit Koordinaten in  $\mathbb{Q}$ .*

**Lemma 1.2.** *Zu jeder über  $\mathbb{Q}$  definierten elliptischen Kurve  $E/\mathbb{Q}$  gibt es eine  $\mathbb{Q}$ -isomorphe Kurve mit der affinen Darstellung*

$$y^2 = x^3 + Ax + B, \text{ mit } A, B \in \mathbb{Z}. \quad (1.1)$$

*Beweis:* Siehe z.B. [Kn], Seite 56 ff. □

Im Folgenden wird immer angenommen, dass eine Darstellung wie in (1.1) fest gewählt ist.

Zu einer elliptischen Kurve  $E$  lassen sich die Diskriminante  $\Delta_E$  und die  $j$ -Invariante  $j_E$  definieren:

**Definition 1.3.** *Für eine elliptische Kurve  $E$ , mit affiner Darstellung wie in (1.1), ist die Diskriminante  $\Delta_E$  gegeben durch*

$$\Delta_E = -8 \cdot (2A)^3 - 27 \cdot (4B)^2. \quad (1.2)$$

*Die  $j$ -Invariante berechnet sich wie folgt:*

$$j(E) = 1728 \cdot \frac{4A^3}{\Delta_E}. \quad (1.3)$$

**Bemerkung 1.4.** *Ist  $\Delta_E \neq 0$ , so ist die Kurve nicht singulär. Die  $j$ -Invariante bestimmt über algebraisch abgeschlossenen Körpern die elliptische Kurve bis auf Isomorphie.*

**Definition 1.5.** *Die Menge der Punkte einer elliptischen Kurve mit rationalen Koordinaten wird mit  $E(\mathbb{Q})$  benannt. Analog erhält man für jeden Körper  $k$  mit  $\mathbb{Q} \subset k$  die Menge  $E(k)$ .*

**Satz 1.6.** *Eine projektive Gerade schneidet eine elliptische Kurve in 3 Punkten (mit Vielfachheiten gezählt).*

## 1 Definitionen und Grundlagen

*Beweis:* Siehe z.B. [Kn], Seite 43 f. □

**Definition 1.7.** *Mit Satz 1.6 kann folgende Verknüpfung „+“ auf der Menge  $E(\mathbb{Q})$  definiert werden:*

*Für  $P, Q \in E(\mathbb{Q})$  sei  $PQ$  der dritte Schnittpunkt der Geraden  $L(P, Q)$ , die durch  $P$  und  $Q$  geht, mit der elliptischen Kurve  $E$ . Nach Satz 1.6 existiert ein solcher Punkt  $PQ \in E(\mathbb{Q})$ ; er ist aber nicht notwendigerweise verschieden von  $P$  und  $Q$ . Für  $P = Q$  sei die Gerade  $L(P, P)$  die Tangente der elliptischen Kurve im Punkt  $P$ . Mit dem ausgezeichneten Punkt  $\mathcal{O}$  wird die Summe als  $P + Q := \mathcal{O}(PQ)$  definiert.*

**Satz 1.8** (Poincaré). *Die Menge  $E(\mathbb{Q})$  mit der eben definierten Verknüpfung „+“ bildet eine abelsche Gruppe mit neutralem Element  $\mathcal{O}$  und Inversem  $-P := (\mathcal{O}\mathcal{O})P$ . Sei  $k$  mit  $\mathbb{Q} \subset k$  ein Körper, so ist die Addition „+“ auf  $E(k)$  ausdehnbar und die Inklusion  $E(\mathbb{Q}) \subset E(k)$  ist ein Gruppenhomomorphismus.*

*Beweis:* Siehe z.B. [Kn], S. 67 ff. □

**Bemerkung 1.9.** *Für die hier betrachteten Kurven mit affiner Darstellung wird als neutrales Element der Punkt  $\infty$  gewählt.*

Ein Beispiel für eine Addition ist in Abbildung 1 auf Seite 11 zu sehen. Die zweite Gerade  $L(PQ, \mathcal{O})$  ist parallel zur  $y$ -Achse gezeichnet, dies entspricht im Affinen einer Geraden durch den Punkt  $\infty$  aus.

**Satz 1.10** (Mordell). *Die Gruppe der  $\mathbb{Q}$ -rationalen Punkte einer elliptischen Kurve über  $\mathbb{Q}$  ist endlich erzeugt. Also hat sie die Form  $\mathbb{Z}^r \oplus F$ , wobei  $r \in \mathbb{N}$  und  $F$  endlich und abelsch ist;  $F$  heißt der Torsionsanteil der Gruppe.*

*Beweis:* Siehe z.B. [Kn], Kapitel IV. □

**Satz 1.11** (Mazur). *Die Torsionsuntergruppe  $F$  der Gruppe der  $\mathbb{Q}$ -rationalen Punkte einer elliptischen Kurve über  $\mathbb{Q}$  ist eine der folgenden:*

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & \text{mit } n = 1, 2, 3, \dots, 9, 10, 12 \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{mit } n = 1, 2, 3, 4 \end{array}$$

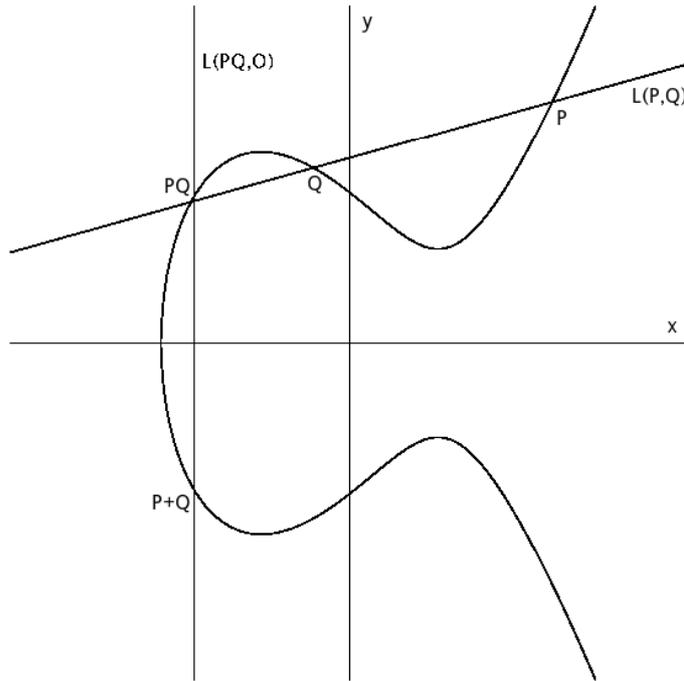


Abbildung 1: Addition auf einer elliptischen Kurve

*Beweis:* Siehe [Ma], S. 146. □

**Korollar 1.12.** Die Kardinalität des Torsionsteils von  $E(\mathbb{Q})$  ist höchstens 16.

**Bemerkung 1.13.** Der Satz 1.11 bietet eine einfache Methode herauszufinden, ob ein Punkt  $P$  auf einer elliptischen Kurve  $E$  ein Torsionspunkt ist: Der Punkt  $P$  muss nur 16 mal zu sich selbst addiert werden. Stellt sich dabei heraus, dass die Ordnung von  $P$  größer als 16 ist, so ist  $P$  kein Torsionspunkt.

Für den in dieser Arbeit behandelten einfachen Fall einer über  $\mathbb{Q}$  definierten Kurve sind explizite Berechnungsformeln für die Addition auf der Kurve bekannt.

Auf den rationalen Punkten einer Kurve können Höhenfunktionen definiert werden.

**Definition 1.14.** Sei  $E$  eine Kurve. Für einen Punkt  $P = \left(\frac{p}{q}, \frac{s}{t}\right) \in E(\mathbb{Q})$  ist die naive Höhe definiert durch

$$H(P) = \max\{|p|, |q|\}. \quad (1.4)$$

## 1 Definitionen und Grundlagen

Die logarithmische Höhe ist

$$h(P) = \log H(P). \quad (1.5)$$

**Definition 1.15.** Sei  $E$  eine Kurve und  $P \in E(\mathbb{Q})$  ein Punkt. Die kanonische Höhe oder auch Néron-Tate-Höhe ist definiert als

$$h_{NT}(P) := \lim_{n \rightarrow \infty} \frac{h(2^n P)}{4^n}. \quad (1.6)$$

**Satz 1.16** (Néron-Tate). Die kanonische Höhe  $h_{NT}$  ist eine quadratische Form und induziert eine Bilinearform:

$$\begin{aligned} \langle \cdot, \cdot \rangle_{NT} : E(\mathbb{Q}) \times E(\mathbb{Q}) &\longrightarrow \mathbb{R} \\ \langle P, Q \rangle_{NT} &= h_{NT}(P + Q) - h_{NT}(P) - h_{NT}(Q). \end{aligned} \quad (1.7)$$

*Beweis:* Siehe z.B. [Si], S. 229. □

**Definition 1.17.** Die durch die kanonische Höhe in Satz 1.16 definierte Bilinearform  $\langle \cdot, \cdot \rangle_{NT}$  heißt Néron-Tate-Höhenpaarung.

## 1.2 Die Modulgruppe und ihre Untergruppen

Die zweite wichtige Struktur dieser Arbeit ist die Modulgruppe mit ihren Untergruppen. Sei

$$\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$$

die obere Halbebene.

**Definition 1.18.** Die Modulgruppe  $\Gamma(1)$  ist definiert als:

$$\Gamma(1) = PSL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1; a, b, c, d \in \mathbb{Z} \right\} / \pm \mathbb{I}$$

Die Modulgruppe  $\Gamma(1)$  wirkt auf  $\mathbb{H}$  durch

$$\gamma(z) = \frac{az + b}{cz + d} \text{ für } \gamma \in \Gamma(1), \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ und } z \in \mathbb{H}.$$

Die Wirkung lässt sich auf  $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$  fortsetzen.

## 1.2 Die Modulgruppe und ihre Untergruppen

**Definition 1.19.** Für eine natürliche Zahl  $N$  sei  $\Gamma(N)$  gegeben als:

$$\Gamma(N) := \ker(\pi) / \pm \text{Id}, \text{ wobei } \pi : SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$$

die kanonische Projektion ist.

**Bemerkung 1.20.** Die Gruppe  $\Gamma(N)$  hat folgende Form:

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

**Definition 1.21.** Sei  $\Gamma \subseteq \Gamma(1)$  eine Untergruppe von endlichem Index. Die Äquivalenzklassen von  $\mathbb{Q} \cup \{\infty\}$  unter der Wirkung von  $\Gamma$  heißen Spitzen von  $\Gamma$ .

**Bemerkung 1.22.** Zu jeder Gruppe  $\Gamma$  wie in Definition 1.21 gibt es nur endlich viele Spitzen. Unter  $\Gamma(1)$  sind alle Elemente aus  $\mathbb{Q} \cup \{\infty\}$  äquivalent.  $\Gamma(1)$  hat also nur eine Spitze.

**Definition 1.23.** Sei  $\Gamma \subseteq \Gamma(1)$  eine Untergruppe von endlichem Index und  $S = \{S_1, \dots, S_r\}$  mit  $r \in \mathbb{N}$  ein Repräsentantensystem für die Spitzen von  $\Gamma$ . Bezeichne  $\Gamma_j$  den Stabilisator von  $S_j$  unter der Wirkung durch  $\Gamma$ . Für jede Spitze  $S_j$  existiert ein  $\gamma_j \in \Gamma(1)$  mit  $\gamma_j(\infty) = S_j$  und eine natürliche Zahl  $b_j$ , so dass für  $\sigma_j = \gamma_j \cdot \begin{pmatrix} \sqrt{b_j} & 0 \\ 0 & 1/\sqrt{b_j} \end{pmatrix}$  gilt:

$$\sigma_j^{-1} \Gamma_j \sigma_j = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle. \quad (1.8)$$

Die natürliche Zahl  $b_j$  heißt die Spitzenbreite der Spitze  $S_j$ .

**Definition 1.24.** Sei  $\Gamma \subset \Gamma(1)$  eine Untergruppe von endlichem Index. Eine zusammenhängende Teilmenge  $\mathcal{F}$  von  $\mathbb{H}$  mit der Eigenschaft, dass jeder Orbit unter der Wirkung von  $\Gamma$  genau einen Repräsentanten in  $\mathcal{F}$  hat, heißt Fundamentalbereich von  $\Gamma$ .

**Bemerkung 1.25.** Die Menge

$$\begin{aligned} \mathcal{F}_{\Gamma(1)} &= \left\{ z \in \mathbb{H} \mid -\frac{1}{2} < \text{Re}(z) < 0, |z| > 1 \right\} \\ &\cup \left\{ z \in \mathbb{H} \mid 0 \leq \text{Re}(z) \leq \frac{1}{2}, |z| \geq 1 \right\} \end{aligned} \quad (1.9)$$

ist ein Fundamentalbereich für  $\Gamma(1)$ . In Abbildung 2 auf Seite 14 ist der Fundamentalbereich  $\mathcal{F}_{\Gamma(1)}$  zu sehen.

Für die späteren Berechnungen ist die Gruppe  $\Gamma(2)$  von besonderer Bedeutung, deshalb wird sie hier genauer untersucht.

**Lemma 1.26.** Die Gruppe  $\Gamma(2)$  hat den Index 6 in  $\Gamma$ . Die Spitzen  $0, 1, \infty$  bilden ein Repräsentantensystem der Spitzen für  $\Gamma(2)$ . Alle drei haben je die Breite 2.

## 1 Definitionen und Grundlagen

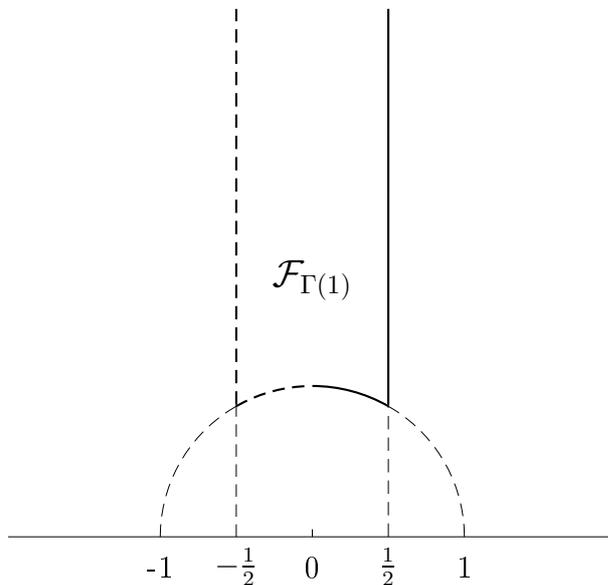


Abbildung 2: Fundamentalbereich zu  $\Gamma(1)$

*Beweis:* Die Behauptung folgt aus den Ausführungen in [La] zu  $\Gamma(2)$  auf Seite 106.  $\square$

**Bemerkung 1.27.** Ein Fundamentalbereich für  $\Gamma(2)$  ist gegeben durch

$$\begin{aligned} \mathcal{F}_{\Gamma(2)} = & \left\{ z \in \mathbb{H} \mid -1 < \operatorname{Re}(z) < 0, \left| z + \frac{1}{2} \right| > \frac{1}{2} \right\} \\ & \cup \left\{ z \in \mathbb{H} \mid 0 \leq \operatorname{Re}(z) \leq 1, \left| z - \frac{1}{2} \right| \geq \frac{1}{2} \right\}. \end{aligned} \quad (1.10)$$

In Abbildung 3 aus Seite 15 ist der Fundamentalbereich  $\mathcal{F}_{\Gamma(2)}$  zu sehen.

**Lemma 1.28.** Die Gruppe  $\Gamma(2)$  ist eine freie Gruppe vom Rang 2. Die beiden Matrizen

$$\gamma_0 := \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \quad \text{und} \quad (1.11)$$

$$\gamma_1 := \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} \quad (1.12)$$

erzeugen die Gruppe.

*Beweis:* Siehe z.B. in [JS], Seite 568.  $\square$

## 1.2 Die Modulgruppe und ihre Untergruppen

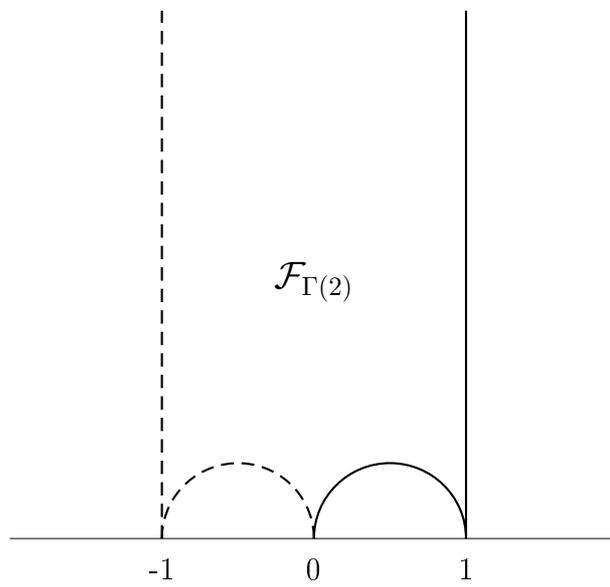


Abbildung 3: Fundamentalbereich zu  $\Gamma(2)$

## 2 Belyi-Morphismen für elliptische Kurven

In diesem Kapitel sollen der Satz von Belyi und seine Anwendung auf elliptische Kurven vorgestellt werden. Dabei werden sogenannte Belyi-Morphismen (siehe Definition 2.3) für elliptische Kurven konstruiert, wobei der Lage von rationalen Punkten der Kurven besondere Aufmerksamkeit geschenkt wird. Für einen solchen Belyi-Morphismus mit rationalen Punkten wird in Satz 2.11 eine Konstruktion vorgestellt und im folgenden Satz 2.12 der Grad des resultierenden Morphismus abgeschätzt.

Im letzten Teil 2.3 des Kapitels wird der für diese Arbeit wichtige Satz über Äquivalenzen zu Belyi-Paaren vorgestellt und beschrieben, wie zu einer über  $\overline{\mathbb{Q}}$  definierten algebraischen Kurve eine Gruppe  $\Gamma \subset \Gamma(2)$  definiert wird.

### 2.1 Der Satz von Belyi

Der Satz von Belyi beschäftigt sich mit der Möglichkeit, wenig verzweigte Abbildungen von algebraischen Kurven  $K$  auf den  $\mathbb{P}^1$  zu erzeugen.

**Definition 2.1.** *Sei  $K$  eine algebraische Kurve und  $\psi : K \rightarrow \mathbb{P}^1$  eine endliche Überlagerung, das heißt, jeder Punkt des  $\mathbb{P}^1$  hat nur endlich viele Urbilder. So ist die Zahl der Urbilder fast überall gleich. Es kann aber endlich viele Punkte in  $\mathbb{P}^1$  geben, an denen  $\psi$  weniger Urbilder hat. Diese Punkte werden als kritische Werte oder Verzweigungsstellen bezeichnet.*

**Satz 2.2** (Satz von Belyi). *Sei  $K$  eine algebraische Kurve. Dann sind folgende Eigenschaften äquivalent:*

- (i) *Die Kurve  $K$  ist über  $\overline{\mathbb{Q}}$  definiert.*
- (ii) *Es gibt einen über  $\mathbb{Q}$  definierten Morphismus  $\beta : K \rightarrow \mathbb{P}^1$ , der höchstens drei kritische Werte hat.*

*Beweis:* Die Implikation (i)  $\Rightarrow$  (ii) wurde von G. Belyi in [Be] 1979 erstmals bewiesen, durch Angabe einer Konstruktion. Die Umkehrung folgt aus schon länger bekannten Tatsachen und geht bis auf Arbeiten von Weil zurück. Ein ausführlicher Beweis findet sich z.B. in [DD] S. 445 ff.  $\square$

**Definition 2.3.** *Ein Morphismus mit den Eigenschaften der Abbildung  $\beta$  aus Satz 2.2 heißt Belyi-Morphismus; das Paar  $(K, \beta)$ , bestehend aus der Kurve  $K$  und dem Morphismus  $\beta$ , heißt ein Belyi-Paar.*

**Bemerkung 2.4.** *Belyi gibt für den Morphismus eine explizite Konstruktion an, doch ist diese Konstruktion schwer durchzuführen. Sie erfordert die Berechnung von Minimalpolynomen und Nullstellen von Polynomen hohen Grades.*

## 2.2 Anwendung auf elliptische Kurven

Der Satz von Belyi besagt, dass es für über  $\mathbb{Q}$  definierte algebraische Kurven einen Belyi-Morphismus gibt. Dies gilt insbesondere für elliptische Kurven. Im Beweis des Satzes wird ein Algorithmus gegeben, einen solchen Morphismus zu berechnen. Doch dieser Algorithmus ist schwer umzusetzen. L. Khadjavi und V. Scharaschkin haben sich in [KS] mit der Möglichkeit beschäftigt einfache Belyi-Morphismen zu elliptischen Kurven anzugeben. Sinnvoll ist es, Belyi-Morphismen zu berechnen, die einen möglichst kleinen Grad haben, denn nur diese erlauben es, mit dem Belyi-Paar zu arbeiten.

Betreffend elliptischer Kurven gilt der folgende Satz:

**Satz 2.5** (Khadjavi, Scharaschkin). *Sei  $E$  eine über  $\mathbb{Q}$  definierte elliptische Kurve mit  $j$ -Invarianten  $j_E$ . Dann gibt es einen Belyi-Morphismus  $\beta : E \rightarrow \mathbb{P}^1$ , mit folgender Eigenschaft:*

- (i)  $\deg(\beta) \leq 4$ , falls  $j_E = 1728$
- (ii)  $\deg(\beta) \leq 6$ , falls  $j_E = 0$
- (iii)  $\deg(\beta) \leq 24H\left(\frac{j_E}{1728}\right)$ , sonst, wobei  $H\left(\frac{p}{q}\right) = \max\{|p|, |q|\}$  die naive Höhe ist.

*Beweis:* Siehe [KS]. Im Beweis werden für die Belyi-Morphismen konkrete Konstruktionen gegeben. □

**Bemerkung 2.6.** *Die Belyi-Morphismen aus dem Beweis zu Satz 2.5, siehe dazu [KS], sind, ausgehend von einer affinen Darstellung der elliptischen Kurve, direkt abzulesen.*

**Bemerkung 2.7.** *Der Grad des Morphismus, wie er von Khadjavi und Scharaschkin konstruiert wird, ist schon für Kurven mit kleinen Koeffizienten sehr groß. Möglicherweise gibt es Belyi-Morphismen von kleinerem Grad.*

Wir wollen nun weitere Anforderungen an den Belyi-Morphismus stellen. Sei  $E$  eine elliptische Kurve und  $P = \{P_1, \dots, P_r\}$  eine endliche Menge von Punkten aus  $E(\mathbb{Q})$ . Gesucht ist ein Belyi-Morphismus  $\beta$ , für den die Menge  $P$  über den kritischen Werten liegt, d.h. ein Morphismus mit  $P \subseteq \beta^{-1}\{\text{Verzweigungsstellen}\}$ . Für diesen Fall ist die Konstruktion von [KS] nicht mehr anwendbar.

A. Granville hat sich mit der entsprechenden Frage für Belyi-Morphismen  $\beta : \mathbb{P}^1 \rightarrow \mathbb{P}^1$  beschäftigt.

## 2 Belyi-Morphismen für elliptische Kurven

**Satz 2.8** (Granville). *Sei  $\mathfrak{M} = \{x_1, \dots, x_r\}$  eine Menge rationaler Zahlen mit mindestens zwei Elementen. Dann gibt es einen Belyi-Morphismus  $\beta : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ , bei dem die Punkte von  $\mathfrak{M}$  über  $\{0, 1, \infty\}$  liegen, mit:*

$$\deg(\beta) \leq \max_{i=1, \dots, r} H(x_i)^{(r-1)(r+2)},$$

wobei  $H\left(\frac{p}{q}\right) = \max\{|p|, |q|\}$  ist.

*Beweis:* Der vollständige Beweis findet sich in [Li], S.335 f. Hier wird nur die Konstruktion vorgestellt, da sie später benötigt wird. Sei  $A$  die kleinste positive ganze Zahl, so dass :

$$a_i = \frac{A}{\prod_{\substack{j=1 \\ j \neq i}}^r (x_j - x_i)} \in \mathbb{Z}, \forall i \quad (2.1)$$

Dann ist

$$\beta(x) = \prod_{i=1}^r (x - x_i)^{a_i} \quad (2.2)$$

ein Belyi-Morphismus mit den gewünschten Eigenschaften.  $\square$

**Bemerkung 2.9.** *Die Abschätzung aus Satz 2.8 ist nicht scharf.*

Das Resultat aus Satz 2.8 läßt sich nutzen, um für eine elliptische Kurve mit einer Menge von rationalen Punkten einen Belyi-Morphismus zu finden und dessen Grad abzuschätzen. Als Vorbereitung wird folgendes Lemma bewiesen:

**Lemma 2.10.** *Sei  $E : y^2 = x^3 + Ax + B$  mit  $A, B \in \mathbb{Z}$  eine elliptische Kurve. Dann ist die Abbildung*

$$\begin{aligned} \psi : E &\longrightarrow \mathbb{C} \\ (x, y) &\longmapsto \frac{1}{4A^3} (27y^4 - 2 \cdot 27By^2 + 4A^3 + 27B^2) \end{aligned}$$

*nur noch verzweigt über  $\left\{0, 1, \frac{4A^3 + 27B^2}{4A^3}, \infty\right\}$ .*

## 2.2 Anwendung auf elliptische Kurven

*Beweis:* Die Projektion  $\pi : (x, y) \mapsto y$  ist über  $\infty$  verzweigt, da  $\pi^{-1}(\infty) = \infty$ . An einer anderen Stelle  $a \in \mathbb{C}$  ist  $\pi$  verzweigt, wenn  $p := x^3 + Ax + B - a^2$  doppelte Nullstellen hat. Dafür muss die Diskriminante von  $x^3 + Ax + B - a^2$  null sein, also  $p$  und  $p'$  eine gemeinsame Nullstelle haben. Dies tritt für genau die  $a$  ein, die sich durch Einsetzen der Nullstellen von  $p' = 3x^2 + A$  in  $\pm\sqrt{x^3 + Ax + B}$  ergeben. Als Lösungen ergeben sich vier nicht unbedingt rationale Punkte. Seien dies die Punkte  $p_1, p_2, p_3$  und  $p_4$ . Verknüpft man nun die Projektion  $\pi$  mit dem Polynom  $g$ , gegeben durch:

$$g := (y - p_1)(y - p_2)(y - p_3)(y - p_4) = y^4 - 2By^2 + \frac{4}{27}A^3 + B^2,$$

so werden diese Verzweigungspunkte auf die Null verschoben. Die Verknüpfung ist also über 0 verzweigt und weiterhin über  $\infty$ , da  $g(\infty) = \infty$ . Jedoch können neue Verzweigungspunkte entstehen: Die Stellen  $a$ , für die das Polynom  $g - a$  doppelte Nullstellen hat. Die Nullstellen von  $g' = 4y^3 - 4By$  sind  $\left\{0, \pm\sqrt{B}\right\}$ ; eingesetzt in  $g$  ergeben sich  $\left\{0, \frac{4A^3}{27}, \frac{4A^3}{27} + B^2\right\}$ . Diese Punkte sind alle rational. Die Abbildung  $g \circ \pi$  ist also verzweigt über

$$\left\{0, \frac{4A^3}{27}, \frac{4A^3}{27} + B^2, \infty\right\}.$$

Mit  $\psi = \frac{27}{4A^3} \cdot (g \circ \pi)$  folgt die Behauptung. □

Nach dieser Vorarbeit ist es möglich einen Belyi-Morphismus für eine elliptische Kurve und eine Anzahl rationaler Punkte anzugeben:

**Satz 2.11.** *Sei  $E : y^2 = x^3 + Ax + B$  mit  $A, B \in \mathbb{Z}$  die affine Darstellung einer elliptischen Kurve und  $P = \{P_1, \dots, P_r\}$  eine endliche Menge von Punkten aus  $E(\mathbb{Q})$ . Weiterhin seien  $\psi$  der Morphismus*

$$\begin{aligned} \psi : E &\longrightarrow \mathbb{C} \\ (x, y) &\longmapsto \frac{1}{4A^3} (27y^4 - 2 \cdot 27By^2 + 4A^3 + 27B^2) \end{aligned}$$

und

$$P' = \psi(P) \cup \left\{0, 1, \frac{4A^3 + 27B^2}{4A^3}\right\}$$

sowie

$$a_p = \frac{A}{\prod_{q \in P' \setminus \{p\}} (q - p)} \in \mathbb{Z}, \quad \forall i,$$

## 2 Belyi-Morphismen für elliptische Kurven

wobei  $A$  die kleinste positive Zahl ist, so dass alle  $a_p$  in  $\mathbb{Z}$  liegen.  
Dann ist die Abbildung

$$\begin{aligned} \beta_P : E &\longrightarrow \mathbb{C} \\ (x, y) &\longmapsto \left( \prod_{p \in P'} (y - p)^{a_p} \right) \circ \psi(y) \end{aligned} \quad (2.3)$$

ein Belyi-Morphismus mit  $P \subseteq \beta_P^{-1} \{0, 1, \infty\}$ .

*Beweis:* Aus Lemma 2.10 und der Konstruktion aus dem Beweis von Satz 2.8, siehe dazu die Formeln (2.1) und (2.2), folgt die Behauptung.  $\square$

Im folgenden Satz wird nun der Grad des Morphismus aus Satz 2.11 abgeschätzt.

**Satz 2.12.** *Sei  $E : y^2 = x^3 + Ax + B$  mit  $A, B \in \mathbb{Z}$  die affine Darstellung einer elliptischen Kurve und  $P = \{P_1, \dots, P_r\}$  eine endliche Menge von Punkten aus  $E(\mathbb{Q})$ , dann gibt es einen Belyi-Morphismus  $\beta : E \longrightarrow \mathbb{C}$  mit  $P \subseteq \beta^{-1} \{0, 1, \infty\}$  für dessen Grad gilt:*

$$\deg(\beta) \leq \left( K \cdot \max_{i=1 \dots r} H(P_i)^4 \right)^{(r+2)(r+5)},$$

wobei

$$K = \max(4A^3, 3^4|B| + |\Delta_E|)$$

mit  $\Delta_E = 4A^3 + 27B^2$ .

*Beweis:* Betrachte den Belyi-Morphismus  $\beta_P$  aus Formel (2.3). Dieser Morphismus erfüllt die Behauptung. Der Satz von Granville (Satz 2.8) soll auf  $\beta_P$  angewendet werden.

Um den Grad abzuschätzen, muss zunächst die Höhe von  $\psi(P)$  abgeschätzt werden. Sei  $p = \left(\frac{s}{t}, \frac{p}{q}\right)$  ein rationaler Punkt auf der Kurve, dann gilt:

$$\begin{aligned} \psi\left(\frac{s}{t}, \frac{p}{q}\right) &= \frac{1}{4A^3} \left( 27 \left(\frac{p}{q}\right)^4 - 2 \cdot 27B \left(\frac{p}{q}\right)^2 + 4A^3 + 27B^2 \right) \\ &= \frac{27p^4 - 2 \cdot 27Bp^2 + (4A^3 + 27B^2)q^4}{4A^3q^4} \end{aligned}$$

Für die Höhe folgt:

$$\begin{aligned} H\left(\psi\left(\frac{s}{t}, \frac{p}{q}\right)\right) &\leq H\left(\frac{p}{q}\right)^4 \max(4A^3, 27 + 2 \cdot 27|B| + |\Delta_E|) \\ &\leq H\left(\frac{p}{q}\right)^4 \max(4A^3, 3^4|B| + |\Delta_E|) \end{aligned}$$

## 2.2 Anwendung auf elliptische Kurven

Nach Satz 2.8 erhält man dann folgende Abschätzung:

$$\begin{aligned} \deg(\beta) &\leq \max_{p' \in P'} H(p')^{(r+2)(r+5)} \\ &\leq \left( \max(4A^3, 3^4|B| + |\Delta_E|) \cdot \max_{i=1, \dots, r} H(P_i)^4 \right)^{(r+2)(r+5)}, \end{aligned}$$

womit der Satz bewiesen ist.  $\square$

Zum Ende dieses Unterkapitels sollen die Sätze 2.11 und 2.12 auf eine elliptische Kurve angewendet werden, die in der weiteren Arbeit eine wichtige Rolle spielt. Später wird ein anderer Belyi-Morphismus zu dieser Kurve verwendet, vergleiche dazu Satz 3.6.

**Beispiel 2.13.** *Wir betrachten die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$ . Diese hat den rationalen Punkt  $P = (1, 4)$ .*

*Für die Kurve  $E$  und die Menge  $M = \{P\}$ , die nur aus dem einen Punkt besteht, ergibt sich mit Satz 2.11 der Morphismus:*

$$\beta(x, y) = \left( \frac{1}{500}(27y^4 - 54y^2) + \frac{32}{5} \right)^{a_0} \left( \frac{1}{500}(27y^4 - 54y^2) + \frac{28}{5} \right)^{a_1} \left( \frac{1}{500}(27y^4 - 54y^2) \right)^{a_2} \left( \frac{1}{500}(27y^4 - 54y^2) - \frac{1512}{125} \right)^{a_3},$$

wobei

$$\begin{aligned} a_0 &= 2^2 3^{11} 5^4 7^2, \\ a_1 &= 2^8 3^3 5^4 7 \cdot 17^2, \\ a_2 &= 3^8 5^5 17^2 \quad \text{und} \\ a_3 &= 2^4 5^9 7. \end{aligned}$$

Es ist also

$$\begin{aligned} \deg(\beta) &= 4(2^2 3^{11} 5^4 7^2 + 2^8 3^3 5^4 7 \cdot 17^2 + 3^8 5^5 17^2 + 2^4 5^9 7) \\ &= 216740920000 \\ &\approx 10^{12}. \end{aligned}$$

Die Abschätzung nach Satz 2.12 liefert

$$\deg(\beta) \leq 2^{72} \cdot 5^{18} \cdot 17^{36} \cdot 401^{18}.$$

Die Abschätzung ist von der Größenordnung von  $10^{126}$ .

Dieses Beispiel veranschaulicht, dass der Morphismus aus Satz 2.11 schon für einfache Beispiele sehr kompliziert werden kann. Außerdem erkennt man, dass die Abschätzung eher grob ist.

### 2.3 Äquivalenzen zu Belyi-Paaren

Belyi-Paare zu elliptischen Kurven bieten einen Ansatz, die Kurven aus anderen Perspektiven zu betrachten und zu bearbeiten, weil die Menge der Belyi-Paare in 1-1-Korrespondenz zu ganz anders gearteten Mengen steht.

Eine der korrespondierenden Mengen, die der Dessins d'Enfants, ist in der Literatur nicht einheitlich definiert. Deshalb sei folgende Definition zuerst angeführt.

**Definition 2.14.** *Sei  $M$  eine orientierte kompakte 2-Mannigfaltigkeit und  $D$  ein zusammenhängender bipartiter, d.h. 2-färbbarer, Graph auf  $M$  mit der Eigenschaft, dass  $M \setminus D$  disjunkte Vereinigung einfach zusammenhängender, offener Mengen ist. Dann heißt  $D$  ein Dessin d'Enfants auf  $M$ .*

Jetzt lässt sich folgender Satz formulieren:

**Satz 2.15.** *Folgende Mengen stehen in 1-1-Korrespondenz, wobei bei allen Mengen noch gewisse Identifikationen beachtet werden müssen:*

- (i) *Belyi-Paare  $(E, \beta)$  vom Grad  $n$ .*
- (ii) *Paare  $(M, \Phi)$ , wobei  $M$  eine kompakte Riemannsche Fläche und  $\Phi : M \rightarrow \mathbb{P}^1(\mathbb{C})$  eine  $n$ -blättrige Überdeckung mit höchstens drei Verzweigungsstellen ist.*
- (iii) *Dessin d'Enfants mit  $n$  Kanten.*
- (iv) *Tripel  $(\sigma_0, \sigma_1, \sigma_\infty)$  mit  $\sigma_0, \sigma_1, \sigma_\infty \in S_n$ , wobei  $\langle \sigma_0, \sigma_1 \rangle$  transitiv wirkt und  $\sigma_0 \sigma_1 \sigma_\infty = id$  gilt.*
- (v) *Untergruppen  $\Gamma \subset \Gamma(2)$  vom Index  $n$ .*

*Beweis:* Dieser Satz ist eine Kombination des Theorems I.5.2 aus [Bo] und den Äquivalenzen in Theorem 1 in [Bi]. □

In dieser Arbeit wird im Weiteren interessieren, wie man zu einem Belyi-Paar aus (i) die assoziierte Untergruppe aus (v) bestimmt. Eine Möglichkeit dies zu tun wurde in [JS] und [Wo] ausführlich erläutert. Im Folgenden wird das Vorgehen nach diesen beiden Artikeln skizziert.

**Vorgehen:** Die Berechnung der assoziierten Untergruppe von  $\Gamma(2)$  zu einem Belyi-Paar geschieht in drei Schritten:

- 1. Schritt** Das Dessin  $D$  zu dem Belyi-Paar  $(E, \beta)$  wird bestimmt.
- 2. Schritt** Die Permutationsgruppe  $\langle \sigma_0, \sigma_1 \rangle$  wird abgelesen.
- 3. Schritt** Die Untergruppe  $\Gamma \subset \Gamma(2)$  wird durch einen Morphismus beschrieben.

**Der 1. Schritt:** Sei  $(E, \beta)$  ein Belyi-Paar. Der projektive Raum  $\mathbb{P}^1(\mathbb{C})$  kann mit  $\mathbb{C} \cup \infty$  identifiziert werden. Die Verzweigungsstellen von  $\beta$  können als  $\{0, 1, \infty\}$  angenommen werden. Über eine Konstruktion mit der Weierstraß'schen  $\wp$ -Funktion sind elliptische Kurven Riemannsche Flächen vom Geschlecht eins. Folgende Mengen bilden ein Dessin d'Enfants  $D$  auf der Riemannschen Fläche, die durch  $E$  gegeben ist:

$\beta^{-1}(]0, 1[)$  bildet die Kanten von  $D$ .

$\beta^{-1}(0)$  ist die Menge der weißen Ecken von  $D$ .

$\beta^{-1}(1)$  ist die Menge der schwarzen Ecken von  $D$ .

Für ein Dessin, das auf diese Art und Weise entsteht, ist die Anzahl der Kanten durch den Grad des Belyi-Morphismus' gegeben; die Ecken des Dessins entsprechen den Urbildern von Null sowie Eins und jedes Urbild von  $\infty$  entsprechen einer Fläche.

**Der 2. Schritt:** Sei ein Dessin  $D$  mit  $n$  Kanten gegeben. Aus diesem Dessin können drei Permutationen abgelesen werden.

Als erstes müssen die Kanten abgezählt werden; die Reihenfolge ist dabei unbedeutend. Wenn die Kanten nummeriert sind, kann an jeder Ecke des Dessins ein Zykel abgelesen werden. Der Zykel ergibt sich, indem die mit der Ecke verbundenen/inzidenten Kanten entsprechend der Orientierung abgezählt werden. Nun wird die Permutation  $\sigma_0$  durch das Produkt der disjunkten Zyklen, die zu den weißen Ecken gehören, gegeben und  $\sigma_1$  als das Produkt der Zyklen der schwarzen Ecken. Die dritte Permutation läßt sich dann durch  $\sigma_\infty = \sigma_1^{-1} \circ \sigma_0^{-1}$  berechnen.  $\sigma_\infty$  korrespondiert dann mit den Flächen des Dessins.  $\langle \sigma_0, \sigma_1 \rangle$  wirkt transitiv, da das Dessin zusammenhängend ist.

## 2 Belyi-Morphismen für elliptische Kurven

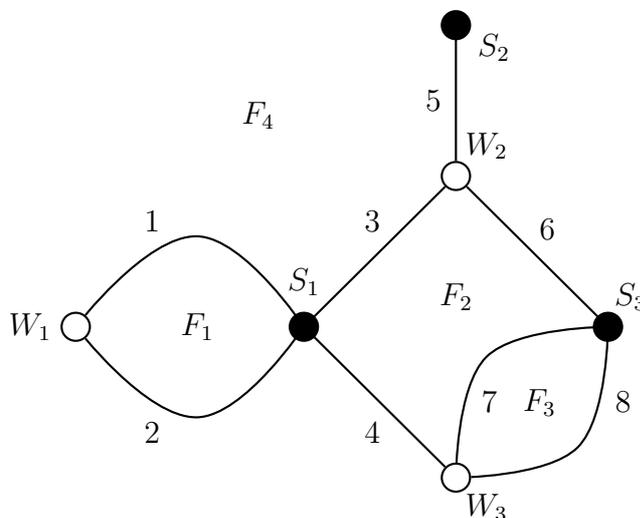


Abbildung 4: Ein Dessin auf der Ebene

**Beispiel 2.16.** Um das Ablezen der Permutationen besser zu verstehen, wird ein Beispiel betrachtet. Sei das Dessin in Abbildung 4 gegeben und die Ecken, Kanten und Flächen wie in der Abbildung benannt.

Das Dessin hat 8 Kanten. Die gesuchten Permutationen sind also aus  $S_8$ . Betrachte zuerst die weißen Ecken. Die Kanten 1 und 2 sind mit  $W_1$  verbunden, also bleibt als Zykel nur die Transposition  $(1, 2)$ . In  $W_2$  treffen drei Kanten auf einander: 3, 5 und 6. Wenn die Kanten entsprechend des mathematische Drehsinns rotiert werden, ergibt sich der Zykel  $(3, 6, 5)$ . Für  $W_3$  liest man entsprechend  $(4, 8, 7)$  ab. Da der Graph bipartit ist, d.h. jede Kante mit genau einer weißen Ecke verbunden ist, sind die Zyklen disjunkt. Dies führt dazu, dass das Produkt der Zyklen nicht von der Reihenfolge der Verknüpfung abhängt und somit eindeutig bestimmt ist. Das gleiche Vorgehen bei den schwarzen Ecken ergibt drei anderen Zyklen. Da  $S_2$  nur mit einer Kante verbunden ist gehört zu  $S_2$  die Identität. Insgesamt gilt:

$$\sigma_0 = (1, 2) (3, 6, 5) (4, 8, 7)$$

$$\sigma_1 = (1, 2, 4, 3) (6, 7, 8)$$

$$\sigma_\infty = \sigma_1^{-1} \sigma_0^{-1} = (1, 3, 4, 2) (6, 8, 7) (1, 2) (3, 5, 6) (4, 7, 8) = (2, 3, 5, 8) (4, 6)$$

**Bemerkung 2.17** ( $\sigma_\infty$  korrespondiert zu den Flächen). So wie die Permutationen  $\sigma_0$  und  $\sigma_1$  um die weißen und die schwarzen Ecken „läuft“, läuft  $\sigma_\infty$  um die Flächen. Jeder Zykel gehört zu einer Fläche. Da aber jede Kante an zwei Flächen grenzt (oder an eine Fläche doppelt) und die Zyklen disjunkt sind, taucht in dem Zykel zu einer Fläche nur jede zweite Kante auf. Dement-

## 2.3 Äquivalenzen zu Belyi-Paaren

*sprechend korrespondiert der Zykel  $(2, 3, 5, 8)$  zur Fläche  $F_4$ , der Zykel  $(4, 6)$  zur Fläche  $F_2$  und die Fixpunkte 1 und 7 zu den Flächen  $F_1$  und  $F_3$ , die von nur zwei Kanten umschlossen werden.*

**Der 3. Schritt:** Sei ein Tripel von Permutationen  $(\sigma_0, \sigma_1, \sigma_\infty)$  gegeben. Die Relation  $\sigma_0\sigma_1\sigma_\infty = id$  bewirkt, dass  $\langle \sigma_0, \sigma_1, \sigma_\infty \rangle = \langle \sigma_0, \sigma_1 \rangle =: G$  gilt.

Also existiert ein natürlicher Morphismus  $\varphi'$  von  $\langle p, q \rangle$ , der von zwei Elementen erzeugten freien Gruppe, in die Gruppe  $G$  wie folgt:

$$\begin{aligned} \varphi' : \langle p, q \rangle &\longrightarrow G \\ p &\longmapsto \sigma_0 \\ q &\longmapsto \sigma_1 \end{aligned}$$

Außerdem gilt: Die Gruppe  $\Gamma(2)$  ist isomorph zu  $\langle p, q \rangle$ , da nach Lemma 1.28  $\Gamma(2)$  frei erzeugt wird von

$$\gamma_0 := \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \text{ und } \gamma_1 := \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}.$$

Es ergibt sich folgender surjektiver Morphismus von  $\Gamma(2)$  auf  $G$ :

$$\begin{aligned} \varphi : \Gamma(2) &\longrightarrow \langle p, q \rangle \longrightarrow G \\ \gamma_0 &\longmapsto p \longmapsto \sigma_0 \\ \gamma_1 &\longmapsto q \longmapsto \sigma_1 \end{aligned} \tag{2.4}$$

Sei  $H$  die Stabilisatoruntergruppe eines Elementes in  $G$ . Aus dem Beweis von Satz 2.15 folgt dann, dass  $\varphi^{-1}(H)$  die gesuchte Gruppe ist, also

$$\Gamma := \varphi^{-1}(H).$$

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

### 3 Die elliptische Kurve $E : y^2 = x^3 + 5x + 10$

Ziel dieses Abschnittes ist es, ein Beispiel genauer zu betrachten. Für die elliptische Kurve  $E$ , affin gegeben durch

$$E : y^2 = x^3 + 5x + 10,$$

soll eine gewisse assoziierte Untergruppe  $\Gamma_E$  von  $\Gamma(2)$  berechnet werden. Dazu sind drei Schritte notwendig. Zuerst wird das Dessin bestimmt, dann das dazugehörige Tripel an Permutationen und schließlich die Gruppe.

Als erstes wollen wir aber die Kurve etwas genauer betrachten und dabei motivieren, wieso gerade dieses Beispiel gewählt wurde.

#### 3.1 Eigenschaften von $E$

Von der elliptische Kurve  $E : y^2 = x^3 + 5x + 10$  sind folgende Eigenschaften bekannt:

**Nummerierung:** Die Kurve ist in den Tabellen von Cremona [Cr] unter der Nummer 400H1 gelistet.

$E(\mathbb{Q})$ : Der Rang der Gruppe  $E(\mathbb{Q})$  ist 1 und die Torsion trivial (siehe [Cr]). Elkies gibt in [El1] den Punkt  $P = (1, 4)$  als Erzeuger von  $E(\mathbb{Q})$  an.

**$L$ -Reihe:** Zu der Kurve gibt es eine  $L$ -Reihe folgender Form:

$$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Mit Hilfe des Computeralgebrasystems Pari lassen sich die Koeffizienten der  $L$ -Reihe berechnen. Das Programm benötigt dafür eine Darstellung der Kurve in global minimaler Weierstraßform.

**Definition 3.1.** *Eine Gleichungsdarstellung einer elliptischen Kurve  $E$  ist minimal in der Primzahl  $p$ , wenn die Potenz von  $p$ , die  $\Delta_E$  teilt, nicht durch einen zulässigen Variablenwechsel über  $\mathbb{Q}$  reduziert werden kann, so dass alle Koeffizienten  $p$ -ganz sind, d.h.  $p$  zum Nenner der Koeffizienten teilerfremd ist.*

*Eine Gleichungsdarstellung heißt global minimal, wenn sie in allen Primzahlen minimal ist und die Koeffizienten ganz sind.*

### 3.1 Eigenschaften von $E$

Das folgende Lemma 3.2 bietet eine einfache Methode zu bestimmen, ob eine Gleichungsdarstellung global minimal ist.

**Lemma 3.2.** *Sei  $p$  eine Primzahl und  $E$  eine elliptische Kurve mit ganzen Koeffizienten und Diskriminante  $\Delta_E \in \mathbb{Z}$ . Wenn für die Primfaktorzerlegung von  $\Delta_E = p_1^{r_1} \cdot \dots \cdot p_n^{r_n}$  gilt, dass  $r_i < 12$  für alle  $i = 1, \dots, n$ , so liegt  $E$  in minimaler Weierstraßform vor.*

*Beweis:* Die Behauptung folgt aus Lemma 10.1. auf Seite 291 [Kn] und der Definition der global minimalen Weierstraßform.  $\square$

Angewandt auf die Kurve  $E$  ergibt sich:

**Korollar 3.3.** *Die elliptische Kurve  $E$  liegt mit der Darstellung  $y^2 = x^3 + 5x + 10$  in global minimaler Weierstraßform vor.*

*Beweis:* Mit  $p = 5$  und  $q = 10$  ist die Diskriminante von  $E$  nach Formel (1.2)

$$\Delta_E = -8(2p)^3 - 27(4q)^2 = -8 \cdot 10^3 - 27 \cdot 40^2 = -51200 = -2^{11} \cdot 5^2.$$

Aus Lemma 3.2 folgt nun die Behauptung.  $\square$

Die Bedingungen, die Pari an die eingegebenen Daten stellt, sind also erfüllt. Der folgende Befehl berechnet die ersten 30 Koeffizienten der  $L$ -Reihe, wobei die erste Zeile die Kurve definiert und die zweite die Koeffizienten berechnet.

```
E = ellinit([0,0,0,5,10]);
ellan(E,30)
```

Pari berechnet als erste Summanden der  $L$ -Reihe:

$$L(E, s) = \frac{1}{1^s} - \frac{3}{3^s} + \frac{2}{7^s} + \frac{6}{9^s} - \frac{1}{11^s} - \frac{4}{13^s} - \frac{5}{17^s} - \frac{1}{19^s} - \frac{6}{21^s} + \dots$$

**Regulator:** Auch der Regulator dieser Kurve lässt sich mit Pari berechnen. Nach [E11] ist bekannt, dass  $E(\mathbb{Q})$  Rang 1 hat und die Gruppe vom Punkt  $P = (1, 4)$  erzeugt wird.

**Definition 3.4.** *Seien  $E$  eine über  $\mathbb{Q}$  definierte elliptische Kurve und die Menge  $\{P_1, \dots, P_n\}$  eine Basis für den freien Anteil von  $E(\mathbb{Q})$ . Der Regulator von  $E$  ist*

$$R_{E/\mathbb{Q}} = \det (\langle P_i, P_j \rangle_{NT}).$$

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

Im Fall von Rang 1 reduziert sich die Berechnung des Regulators auf die Höhenpaarung des erzeugenden Elements mit sich selbst. Mit Pari ist dies durch die folgenden Befehle möglich:

```
E = ellinit([0,0,0,5,10]);
ellbil(E, [1,4], [1,4])
```

Das Ergebnis ist

$$R_E = 0,128375062946050869. \quad (3.1)$$

**Belyi-Paar:** N. Elkies gibt in [El1] zu der Kurve  $E$  einen sehr einfachen Belyi-Morphismus von geringem Grad an.

**Lemma 3.5.**  $\beta(x, y) = y(x - 5)$  ist ein Morphismus vom Grad 5.

*Beweis:* Der Grad der Abbildung  $\beta$  ist die Anzahl der Blätter. Sei  $a \in \beta(E)$ . Gesucht ist die Anzahl der Urbilder von  $a$ . Dies sind die Lösungen des Gleichungssystems:

$$\begin{aligned} a &= y(x - 5) \\ y^2 &= x^3 + 5x + 10 \end{aligned} \quad (3.2)$$

Für  $x \neq 5$  folgt  $y = \frac{a}{x-5}$ , also

$$\begin{aligned} \left(\frac{a}{x-5}\right)^2 &= x^3 + 5x + 10 \\ \Leftrightarrow a^2 &= (x^3 + 5x + 10)(x^2 - 10x + 25) \\ \Leftrightarrow 0 &= x^5 - 10x^4 + 30x^3 - 40x^2 + 25x + 250 - a^2. \end{aligned} \quad (3.3)$$

Es ergibt sich ein Polynom vom Grad 5. Im allgemeinen gibt es demnach 5 Urbilder, also 5 Blätter. Die Abbildung hat demnach Grad 5.  $\square$

**Satz 3.6.** *Das Paar*

$$E : y^2 = x^3 + 5x + 10, \quad \beta(x, y) = y(x - 5) \quad (3.4)$$

*ist ein Belyi-Paar vom Grad 5.*

*Beweis:* Aus Lemma 3.5 ist bekannt, dass der Morphismus  $\beta$  den Grad 5 hat. Um den Satz zu beweisen, bleibt zu prüfen, dass die Abbildung  $\beta$  nicht mehr als drei Verzweigungsstellen hat.

Es ist sofort ersichtlich, dass  $\beta$  in  $\infty$  verzweigt ist, da  $\beta^{-1}(\infty) = \infty$ . Weitere Verzweigungsstellen liegen dort, wo für  $a \in \mathbb{C}$  das System aus Formel (3.2) nicht die maximalen 5 Lösungen hat, also dort, wo die Gleichung (3.3) doppelte Nullstellen hat. Dies sind jene Fälle, in denen die Diskriminante null ist. Mit dem Computeralgebraprogramm Maple lässt sich die Diskriminante berechnen und die Nullstellen finden:

### 3.1 Eigenschaften von $E$

```
solve(discrim(x^5-10*x^4+30*x^3-40*x^2+25*x+250-a^2
,x)=0,a);
```

Das Ergebnis ist  $\{0, \pm 16\}$ . In Null ist der Morphismus nicht verzweigt, denn neben den drei Lösungen für  $y = 0$  liefert  $x = 5$ , was oben ausgeschlossen wurde, noch zwei Lösungen. Also ist der Morphismus höchstens über  $\{\pm 16, \infty\}$  verzweigt.  $\square$

**Bemerkung 3.7.** Wenn bekannt ist, wo der Belyi-Morphismus verzweigt ist, lassen sich diese Stellen auf  $\{0, 1, \infty\}$  normieren. Für die Kurve  $E$  ist

$$\begin{aligned} \beta : E &\longrightarrow \mathbb{P}^1 \\ (x, y) &\longmapsto \frac{y(x-5) + 16}{32} \end{aligned} \quad (3.5)$$

ein Belyi-Morphismus, der nur über  $\{0, 1, \infty\}$  verzweigt ist.

**Verzweigungen:**

**Satz 3.8.** Für den Belyi-Morphismus aus Bemerkung 3.7 gilt:

$$\begin{aligned} \beta^*(0) &= 4 \cdot (1, 4) + 1 \cdot (6, -16) \\ \beta^*(1) &= 4 \cdot (1, -4) + 1 \cdot (6, 16) \\ \beta^*(\infty) &= 5 \cdot \infty \end{aligned} \quad (3.6)$$

*Beweis:* Die Behauptung folgt leicht durch Berechnen der Lösungen des Gleichungssystems

$$\begin{aligned} a &= \frac{y(x-5) + 16}{32} \\ y^2 &= x^3 + 5x + 10 \end{aligned}$$

für  $a \in \{0, 1, \infty\}$ .  $\square$

Somit liegt der Erzeuger von  $E(\mathbb{Q})$  über den Verzweigungsstellen.

**Bemerkung 3.9.** Der Grad des Morphismus'  $\beta$  zur Kurve  $E$  ist deutlich kleiner, als der Grad eines nach Satz 2.12 konstruierten Belyi-Morphismus', bei dem sich ein Morphismus von 12-stelligem Grad ergab. Siehe dazu Beispiel 2.13 auf Seite 21.

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

### 3.2 Die zu $(E, \beta)$ assoziierten Gruppe $\Gamma_E$

Für das Belyi-Paar

$$\begin{aligned} E : y^2 &= x^3 + 5x + 10 \\ \beta(x, y) &= \frac{y(x-5) + 16}{32} \end{aligned} \quad (3.7)$$

soll jetzt die zugehörige Untergruppe  $\Gamma_E$  von  $\Gamma(2)$  berechnet werden. Dazu wird die Methode benutzt, die in Kapitel 2.3 vorgestellt wurde.

Ergebnis dieses Kapitels ist der folgende Satz:

**Satz 3.10.** *Zu dem Belyi-Paar  $(E, \beta)$  aus Formel (3.7) ist die assoziierte Gruppe  $\Gamma_E \subset \Gamma(1)$  gegeben durch den Morphismus*

$$\begin{aligned} \varphi_E : \Gamma(2) &\longrightarrow S_5 \\ \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} &\longmapsto (1235) \\ \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} &\longmapsto (1234) \end{aligned} \quad (3.8)$$

als

$$\Gamma_E = \{\gamma \in \Gamma(2) \mid \varphi_E(\gamma) \in \text{Stab}(5)\}. \quad (3.9)$$

*Beweis:* Der Satz 3.10 folgt aus den Ausführungen in diesem Kapitel.  $\square$

**Satz 3.11.** *Die Gruppe  $\Gamma_E$  ist keine Kongruenzuntergruppe.*

*Beweis:* Der Punkt  $P = (1, 4) \in E$  erzeugt die unendliche Gruppe  $E(\mathbb{Q})$ . In diesen Fall ist sowohl  $P \in \{0, 1, \infty\}$  als auch  $0_E \in \{0, 1, \infty\}$ . Aus der Theorie der elliptischen Kurven folgt, dass der Spitzendivisor  $P - 0_E \in \text{Pic}^0(E)$  kein Torsionsdivisor ist. Mit dem Theorem von Manin und Drinfeld, siehe z.B. [El2], folgt dann die Behauptung.  $\square$

#### Herleitung der Gruppe $\Gamma_E$

Nach der Methode aus Kapitel 2.3 muss das zu  $(E, \beta)$  gehörende Dessin berechnet werden. Die Urbilder der Verzweigungsstellen und die zugehörigen Verzweigungsordnungen sind aus Formel (3.6) bekannt. Demnach ist die Anzahl der Ecken und deren Valenzen bekannt: Es handelt sich also um einen 5-kantigen bipartiten Graphen, der zwei weiße und zwei schwarze Ecken hat, von denen jeweils eine die Valenz vier und eine die Valenz eins hat. Der

### 3.2 Die zu $(E, \beta)$ assoziierten Gruppe $\Gamma_E$

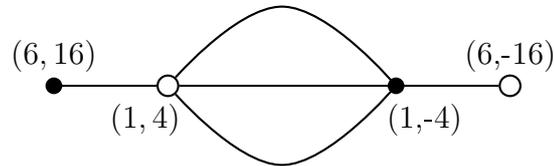


Abbildung 5: Der abstrakte Graph auf der Ebene

Graph, der sich in der Ebene ergibt, ist auf Abbildung 5 auf Seite 31 zu sehen.

Da  $\infty$  nur ein Urbild besitzt, hat das Dessin nur eine Fläche und weil es sich um eine elliptische Kurve handelt, ist das Dessin in einen Torus eingebettet.

Um zu bestimmen, wie genau das Dessin aussieht, betrachten wir direkt die Permutationsgruppe  $G$ . Die Gruppe  $G$  ist eine Untergruppe von  $S_5$ , da der Belyi-Morphismus Grad 5 hat. Die Informationen über die Anzahl der Punkte und der Valenzen reichen aus, die Gestalt der erzeugenden Permutationen zu kennen. Zu den Verzweigungspunkten gehören folgende Zyklen:

zu 0:

1 Punkt mit Valenz 4  $\longleftrightarrow$  4-Zykel  
 1 Punkt mit Valenz 1  $\longleftrightarrow$  1-Zykel

zu 1:

1 Punkt mit Valenz 4  $\longleftrightarrow$  4-Zykel  
 1 Punkt mit Valenz 1  $\longleftrightarrow$  1-Zykel

zu  $\infty$ :

1 Punkt mit Valenz 5  $\longleftrightarrow$  5-Zykel

Die Permutationen  $\sigma_0$  und  $\sigma_1$  sind 4-Zykel, da ein 1-Zykel ein Fixpunkt ist. Die Benennung der Kanten ist beliebig und so kann der erste 4-Zykel als  $\sigma_0 = (1234)$  gewählt werden. Im zweiten 4-Zykel muss die Kante 5 enthalten sein, denn sonst wirkt  $\langle \sigma_0, \sigma_1 \rangle$  nicht transitiv. Die Benennung der Kanten kann so gewählt werden, dass 4 nicht im Zykel vorkommt. Der Zykel kann mit  $\sigma_1 = (abc5)$  benannt werden, wobei  $\{a, b, c\} = \{1, 2, 3\}$ . Bei dem Dessin handelt es sich um eine Verknüpfung der beiden Teile, die in Abbildung 6 auf Seite 32 dargestellt sind. Mögliche Belegungen für  $a, b, c$  sind die, bei denen  $\sigma_0\sigma_1$  ein 5-Zykel ist, da zu dem einen Punkt über  $\infty$  ein 5-Zykel korrespondiert.

Jetzt können alle Möglichkeiten für  $a, b, c$  ausprobiert werden. In Tabelle 1 auf Seite 32 sind alle 4-Zykel aus 1,2,3 und 5 für  $\sigma_1$  sowie die resultierende Permutation  $\sigma_0\sigma_1$  aufgelistet.

Es gibt also drei mögliche Belegungen  $A, B$  und  $C$  für das Tripel  $(a, b, c)$ .

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

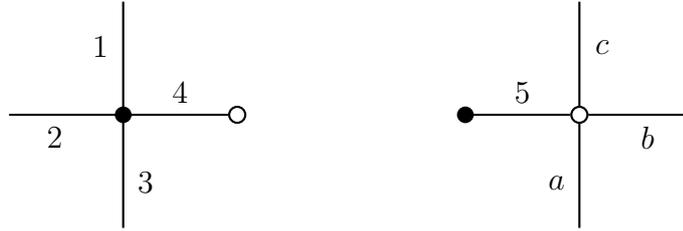


Abbildung 6: Bestandteile des Dessins zu  $(E, \beta)$

	$\sigma_1$	$\sigma_0\sigma_1$	5-Zykel?
A	(1235)	(13524)	ja
	(1325)	(14)(25)	nein
	(2135)	(14)(35)	nein
B	(2315)	(15324)	ja
C	(3125)	(13254)	ja
	(3215)	(154)	nein

Tabelle 1: Mögliche Permutationen zu  $(E, \beta)$

Die Dessins, die diesen entsprechen, sind in den Abbildungen 7 bis 9 zu sehen. Die Tori, in welche die Dessins eingebettet sind, sind in den Abbildungen als Rechtecke dargestellt, deren gegenüberliegenden Seiten zu identifizieren sind.

Nun bleibt als Problem übrig, zu entscheiden, welches dieser drei Dessins dem gewählten Belyi-Paar entspricht. Birch [Bi] und Wolfart [Wo] haben ein weiteres Belyi-Paar, welches den Typ  $(41,41,5)$  hat, d.h. welches eine Fläche und vier Ecken mit den Valenzen 4,1 und 4,1 hat, untersucht.

$$\begin{aligned}
 C : y^2 &= x^3 + \frac{35}{4}x^2 + 25x + 25 \\
 \beta_C(x, y) &= xy + i \left( \frac{5}{2}x^2 + 15x + 22 + 4i \right)
 \end{aligned}
 \tag{3.10}$$

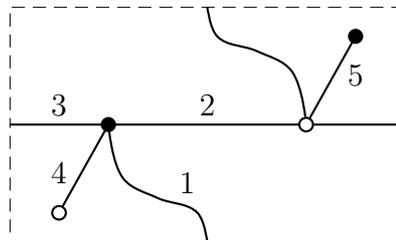


Abbildung 7: Dessin zu A:  $\sigma_1 = (1235)$

### 3.2 Die zu $(E, \beta)$ assoziierten Gruppe $\Gamma_E$

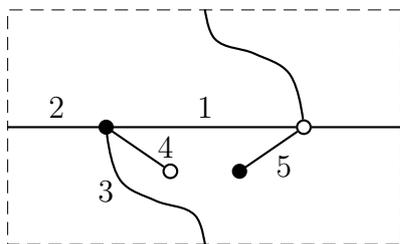


Abbildung 8: Dessin zu  $B$ :  $\sigma_1 = (1523)$

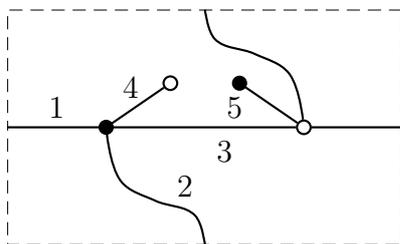


Abbildung 9: Dessin zu  $C$ :  $\sigma_1 = (1253)$

Dieses Belyi-Paar ist verschieden von dem hier untersuchten aus Formel (3.7). Es muss also zu einem anderen Dessin gehören.

Eine Möglichkeit, Dessins und Belyi-Paare zu untersuchen, ist, die Wirkung der absoluten Galois-Gruppe zu nutzen, wie sie S. Lando und A. Zvonkin in [LZ], Kapitel 2.4 beschreiben: Dabei wirkt ein Element  $\sigma$  der Galois-Gruppe auf einem Belyi-Paar, indem  $\sigma$  auf die Koeffizienten der definierenden Gleichungen angewendet wird. Bezüglich der Galois-Wirkung gilt folgender Satz:

**Satz 3.12.** *Die Wirkung eines Elements der absoluten Galois-Gruppe  $\overline{\mathbb{Q}}/\mathbb{Q}$  überführt ein Belyi-Paar in ein anderes vom selben Typ.*

*Beweis:* Siehe z.B. [LZ] Seite 116 f. □

Betrachte die komplexe Konjugation  $\iota$  und ihre Wirkung auf die Belyi-Paare  $(E, \beta)$  und  $(C, \beta_C)$ . Da  $(E, \beta)$  über  $\mathbb{Q}$  definiert ist, bleibt dieses Belyi-Paar invariant unter der Wirkung von  $\iota$ . Bei  $(C, \beta_C)$  ändert sich der Belyi-Morphismus und es ergibt sich  $(C, \beta'_C)$ :

$$\begin{aligned} C : y^2 &= x^3 + \frac{35}{4}x^2 + 25x + 25 \\ \beta'_C(x, y) &= xy - i\left(\frac{5}{2}x^2 + 15x + 22 - 4i\right). \end{aligned} \tag{3.11}$$

Sei  $D_1$  das Dessin zu  $(C, \beta_C)$  und  $D_2$  das Dessin zu  $(C, \beta'_C)$ . Die beiden Dessins sind eng miteinander verbunden. Für einen Punkt  $P = (x, y) \in \mathbb{C}^2$

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

mit  $P \in C$  gilt:

$$\beta'_C(\bar{x}, \bar{y}) = \overline{\beta_C(x, y)}. \quad (3.12)$$

Da das Dessin zu einem Belyi-Paar durch das Urbild des Intervalls  $[0, 1]$  unter dem Belyi-Morphismus gegeben ist, gilt für ein  $P \in D_1$ , dass  $\beta_C(P) \in \mathbb{R}$ , also  $\beta_C(P) = \overline{\beta_C(P)}$ . Mit Formel (3.12) folgt, dass  $\bar{P} = (\bar{x}, \bar{y})$  zu  $D_2$  gehört. Zwischen den Dessins gibt es also folgende bijektive Abbildung:

$$\psi : \begin{array}{ccc} D_1 & \longrightarrow & D_2 \\ P & \longmapsto & \bar{P} \end{array} \quad (3.13)$$

Die Abbildung  $\psi$  läßt sich auf die ganze Kurve  $C$  anwenden und definiert dort eine Spiegelung, d.h.  $D_1$  und  $D_2$  sind Spiegelungen voneinander.

Die Belyi-Paare  $(C, \beta)$  und  $(C, \beta')$  sind nicht gleich. Folglich müssen die Dessins sich unterscheiden. Mit den Belyi-Paaren  $(E, \beta)$ ,  $(C, \beta_C)$  und  $(C, \beta'_C)$  gibt es drei Kandidaten für die drei Dessins. Außerdem ist bekannt, dass  $D_1$  und  $D_2$  Spiegelungen voneinander sind.

Zu den Dessins, die Spiegelungen voneinander sind, müssen die assoziierten Permutationsgruppen isomorph sein:

$$\langle \sigma_0^\beta, \sigma_1^\beta \rangle \cong \langle \sigma_0^{\beta'}, \sigma_1^{\beta'} \rangle.$$

Für die Permutationsgruppe zu den drei Kandidaten ergibt sich (mit Maple berechenbar):

$$\begin{aligned} A : & \langle (1234), (1235) \rangle = S_5 \\ B : & \langle (1234), (1523) \rangle = A_5 \\ C : & \langle (1234), (1253) \rangle = A_5 \end{aligned}$$

Betrachtet man die Dessins genauer, wird deutlich, dass die Dessins auf den Abbildungen 8 und 9 Spiegelungen voneinander sind. Also müssen sie zu den Belyi-Paaren  $(C, \beta_C)$  und  $(C, \beta'_C)$  korrespondieren. Zu  $(E, \beta)$  korrespondiert also das Dessin aus Abbildung 7, d.h. die Gruppe aus Fall A.

In Abbildung 10 auf Seite 35 ist das Dessin zum Belyi-Paar  $(E, \beta)$  auf einem Torus zu sehen.

Zu dem Belyi-Paar korrespondieren folgende drei Permutationen:

$$\begin{aligned} \sigma_0 &= (1235) \\ \sigma_1 &= (1234) \\ \sigma_\infty &= \sigma_1^{-1} \circ \sigma_0^{-1} = (15243), \end{aligned}$$

die zusammen die Gruppe  $G = S_5$  erzeugen.

### 3.3 Algorithmus zum Testen der Zugehörigkeit zu $\Gamma_E$

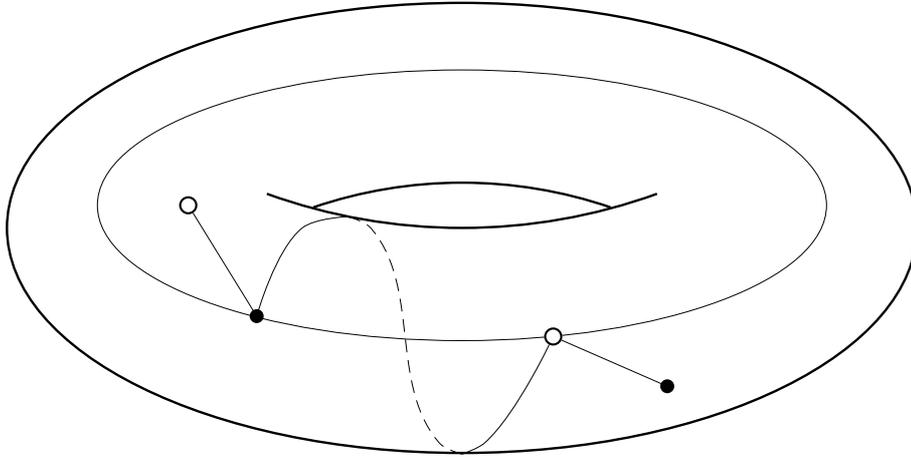


Abbildung 10: Dessin zu  $(E, \beta)$  auf dem Torus

Die gesuchte Gruppe  $\Gamma$  ist das Urbild des Stabilisators  $\text{Stab}(a)$  einer beliebigen Kante  $a$  unter dem Morphismus  $\varphi : \Gamma(2) \rightarrow G$  (siehe Formel (2.4)), also die Menge:

$$\Gamma_E = \{\gamma \in \Gamma(2) \mid \varphi(\gamma) \in \text{Stab}(a)\}. \quad (3.14)$$

Im Folgenden wird die Kante 5 gewählt; der zugehörige Stabilisator ist

$$\text{Stab}(5) = \langle (1234), (243) \rangle = \langle \sigma_1, \sigma_0^2 \sigma_1 \sigma_0 \rangle.$$

Damit ergeben sich der Morphismus

$$\begin{aligned} \varphi_E : \Gamma(2) &\longrightarrow S_5 \\ \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} &\longmapsto (1235) \\ \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} &\longmapsto (1234) \end{aligned} \quad (3.15)$$

und die Gruppe

$$\Gamma_E = \{\gamma \in \Gamma(2) \mid \varphi_E(\gamma) \in \text{Stab}(5)\}. \quad (3.16)$$

Der Satz 3.10 ist damit bewiesen.

### 3.3 Algorithmus zum Testen der Zugehörigkeit zu $\Gamma_E$

Für die weitere Arbeit mit der Gruppe  $\Gamma_E$  aus Formel (3.9) ist es notwendig zu wissen, wie die Matrizen in  $\Gamma_E$  aussehen. Denn im Kapitel 4 wird sich die Frage stellen, ob gewisse Matrizen in  $\Gamma_E$  liegen. Die Tatsache, dass die Gruppe

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

$\Gamma_E$  durch einen Morphismus in eine endliche Gruppe beschrieben ist, bietet eine einfache und schöne Möglichkeit zu testen, ob eine gegebene Matrix aus  $\Gamma(1)$  in  $\Gamma_E$  liegt. Ein Algorithmus für einen solchen Test wird hier vorgestellt.

Die Gruppe  $\Gamma_E$  ist als Menge derjenigen Elemente von  $\Gamma(2)$  gegeben, für die das Bild unter dem Morphismus  $\varphi_E$  das Element 5 als Fixpunkt hat. Sobald das Bild  $\varphi_E(M)$  einer Matrix  $M$  bekannt ist, ist es einfach zu entscheiden, ob die Matrix in der Gruppe  $\Gamma_E$  liegt, da nur noch eine endliche Permutation  $\varphi_E(M)$  an der Stelle 5 ausgewertet werden braucht.

Ein Algorithmus, der für eine Matrix  $M$  entscheidet, ob sie in  $\Gamma_E$  liegt, kann wie folgt aussehen:

---

**Algorithmus 1** Test: Liegt ein Element  $M \in \Gamma(1)$  in  $\Gamma_E$ ?

---

```
1: if  $M \notin \Gamma(2)$  then
2:   return false
3: else
4:   Berechne die Darstellung der Matrix  $M$  als Wort in den Erzeugern von
       $\Gamma(2)$ . (*)
5:   Bestimme das Bild von  $M$  unter  $\varphi_E$ .
6:   if  $\varphi_E(M) \in \text{Stab}(5)$  then
7:     return true
8:   else
9:     return false
10:  end if
11: end if
```

---

Die einzige Zeile, die nicht einfach auszuführen ist, ist die Zeile 4, die mit dem Stern (\*) gekennzeichnete. Doch dafür bietet das Computeralgebraprogramm Magma eine Funktion, mit der das Wort zu einer Matrix berechnet werden kann. Sei  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ , dann gibt folgende Befehlsfolge das gesuchte Wort:

```
G2 := CongruenceSubgroup(2);
g := G2![a, b, c, d];
FindWord(G2, g);
```

Ob das so berechnete Wort in  $\Gamma_E$  liegt, testet das Programm `InGruppe.java`. Der Programmcode ist im Anhang unter A.1 auf Seite 100 zu finden.

### 3.4 Untersuchung der Gruppe $\Gamma_E$

Weitere Informationen, die über die Gruppe  $\Gamma_E$  aus Formel (3.9) benötigt werden, sind die Anzahl und Breite der Spitzen sowie ein Repräsentantensystem für die Spitzen. In diesem Unterkapitel werden diese Daten berechnet.

Als erstes werden einige Matrizen eingeführt, die für die weiteren Berechnungen benötigt werden. Sei  $j \in \mathbb{Z}$ , dann sei

$$\gamma_j := \begin{pmatrix} j & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma(1). \quad (3.17)$$

Diese Matrix hat die Eigenschaft den Randpunkt  $\infty$  auf den Randpunkt  $j$  abzubilden. Außerdem definieren wir

$$\tau_n := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \Gamma(1), \quad (3.18)$$

mit  $n \in \mathbb{Z}$ . Diese Matrizen sind genau jene, die  $\infty$  fixieren. Für zwei ganze Zahlen  $j$  und  $k$  gilt für die Verknüpfung

$$\gamma_{jk,n} = \gamma_k \circ \tau_n \circ \gamma_j^{-1} \quad (3.19)$$

für beliebiges  $n \in \mathbb{Z}$ , dass  $\gamma_{jk,n}(j) = k$ .

**Bemerkung 3.13.** *Alle Matrizen  $\mu \in \Gamma(1)$  mit der Eigenschaft  $\mu(j) = k$  sind von der Form  $\gamma_{jk,n}$ .*

**Lemma 3.14.** *Die Menge  $\{0, 1, 3, 6, \infty\} \subset \overline{\mathbb{H}}$  ist ein Repräsentantensystem für die Spitzen von  $\Gamma_E$ .*

*Beweis:* Da die Verzweigungspunkte des Morphismus'  $\beta$  aus Formel (3.5) insgesamt fünf Urbilder haben, gibt es fünf Spitzen. Es genügt also zu zeigen, dass die Spitzen  $0, 1, 3, 6, \infty$  nicht äquivalent zueinander sind, d.h. zu zeigen ist, dass es keine Matrix in  $\Gamma_E$  gibt, die zwei dieser Spitzen ineinander überführt. Seien  $\{j, k\} \subset \{0, 1, 3, 6\}$ , dann hat eine Matrix  $\gamma_{jk,n}$  aus Formel (3.19) mit  $\gamma_{jk}(j) = k$ , die  $j$  in  $k$  überführt die Form

$$\gamma_{jk,n} = \gamma_k \circ \tau_n \circ \gamma_j^{-1} = \begin{pmatrix} 1-nk & k-j+jkn \\ -n & nj+1 \end{pmatrix}. \quad (3.20)$$

Für die Spitze  $\infty$  und eine beliebige andere Spitze ist der Fall einfacher:

$$\gamma_{j\infty} = \tau_n \circ \gamma_j^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & j \end{pmatrix}.$$

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

Für die Überführungsmatrizen ergeben sich:

$$\begin{array}{llll}
j \text{ bel. } & k = \infty & \rightsquigarrow & \gamma_{j\infty,n} = \begin{pmatrix} 0 & 1 \\ -1 & j \end{pmatrix} & \notin \Gamma_E & \forall n \\
j = 0 & k = 1 & \rightsquigarrow & \gamma_{01,n} = \begin{pmatrix} 1-kn & k-j+jkn \\ -n & nj+1 \end{pmatrix} = \begin{pmatrix} 1-n & 1 \\ -n & 1 \end{pmatrix} & \notin \Gamma_E & \forall n \\
j = 0 & k = 3 & \rightsquigarrow & \gamma_{03,n} = \begin{pmatrix} 1-kn & k-j+jkn \\ -n & nj+1 \end{pmatrix} = \begin{pmatrix} 1-3n & 3 \\ -n & 1 \end{pmatrix} & \notin \Gamma_E & \forall n \\
j = 0 & k = 6 & \rightsquigarrow & \gamma_{06,n} = \begin{pmatrix} 1-kn & k-j+jkn \\ -n & nj+1 \end{pmatrix} = \begin{pmatrix} 1-6n & 6 \\ -n & 1 \end{pmatrix} & \stackrel{?}{\in} \Gamma_E & (i) \\
j = 1 & k = 3 & \rightsquigarrow & \gamma_{13,n} = \begin{pmatrix} 1-kn & k-j+jkn \\ -n & nj+1 \end{pmatrix} = \begin{pmatrix} 1-3n & 2+3n \\ -n & n+1 \end{pmatrix} & \stackrel{?}{\in} \Gamma_E & (ii) \\
j = 1 & k = 4 & \rightsquigarrow & \gamma_{14,n} = \begin{pmatrix} 1-kn & k-j+jkn \\ -n & nj+1 \end{pmatrix} = \begin{pmatrix} 1-6n & 3+6n \\ -n & n+1 \end{pmatrix} & \notin \Gamma_E & \forall n \\
j = 3 & k = 4 & \rightsquigarrow & \gamma_{34,n} = \begin{pmatrix} 1-kn & k-j+jkn \\ -n & nj+1 \end{pmatrix} = \begin{pmatrix} 1-6n & 1+18n \\ -n & 3n+1 \end{pmatrix} & \notin \Gamma_E & \forall n
\end{array}$$

Jene Zeilen, in denen steht, dass  $\gamma_{jk,n}$  für alle  $n$  nicht in  $\Gamma_E$  liegt, lässt sich diese Aussage direkt ablesen, da die fraglichen Matrizen schon nicht in  $\Gamma(2)$  liegen können: Damit der Eintrag unten links gerade ist, muss  $n$  gerade sein. Dann folgt aber in diesen Fällen, dass der Eintrag oben rechts ungerade ist.

In zwei Zeilen steht ein Fragezeichen. In diesen Fällen ist für gerade  $n$   $\gamma_{jk,n} \in \Gamma(2)$ . Hier muss noch untersucht werden, ob eine Matrix der Form (i) oder (ii) in  $\Gamma_E$  liegen kann. Sei also  $n$  gerade, dann lassen sich die Matrizen aus (i) und (ii) wie folgt in ihre Darstellung in den Erzeugern

$$\gamma_0 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \quad \text{und} \quad \gamma_1 = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}$$

von  $\Gamma(2)$  zerlegen:

$$\begin{aligned}
(i) \quad \pm \begin{pmatrix} 1-6n & 6 \\ -n & 1 \end{pmatrix} &= \begin{pmatrix} 11 & -6 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} (-1)^{n/2-1} & 0 \\ (n-2) \cdot (-1)^{n/2} & (-1)^{n/2-1} \end{pmatrix} \\
&= \begin{pmatrix} 11 & -6 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}^{\frac{n}{2}-1} \\
&= \begin{pmatrix} -1 & 0 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}^{\frac{n}{2}-1} \\
&= \gamma_1^{-1} \gamma_0^{-1} \gamma_1^{-1} \gamma_0^{-1} \gamma_1^{-1} \gamma_0^{\frac{n}{2}-1} \\
(ii) \quad \begin{pmatrix} 1-3n & 2+3n \\ -n & n+1 \end{pmatrix} &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -n+1 & n \\ -n & n+1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}^{\frac{n}{2}} \\
&= \begin{pmatrix} -1 & 0 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}^{\frac{n}{2}} \\
&= \gamma_1^{-1} \gamma_0^{-1} \gamma_1^{\frac{n}{2}}
\end{aligned}$$

Aus dieser Darstellung ist das Bild der Matrizen unter der Abbildung  $\varphi_E$ ,

### 3.4 Untersuchung der Gruppe $\Gamma_E$

welche die Gruppe  $\Gamma_E$  definiert, siehe Formel (3.8), berechnenbar:

$$\begin{aligned}
 \varphi_E \left( \begin{pmatrix} 1-6n & 6 \\ -n & 1 \end{pmatrix} \right) &= \varphi_E \left( (\gamma_1^{-1} \gamma_0^{-1} \gamma_1^{-1} \gamma_0^{-1} \gamma_1^{-1}) \gamma_0^{\frac{n}{2}-1} \right) \\
 &= \sigma_1^{-1} \sigma_0^{-1} \sigma_1^{-1} \sigma_0^{-1} \sigma_1^{-1} \sigma_0^{\frac{n}{2}-1} \\
 &= (4321)(5321)(4321)(5321)(4321)(1235)^{\frac{n}{2}-1} \\
 &= (45)(1235)^{\frac{n}{2}-1} \\
 \varphi_E \left( \begin{pmatrix} 1-3n & 2+3n \\ -n & n+1 \end{pmatrix} \right) &= \varphi_E \left( (\gamma_1^{-1} \gamma_0^{-1}) \gamma_1^{\frac{n}{2}} \right) \\
 &= \sigma_1^{-1} \sigma_0^{-1} \sigma_1^{\frac{n}{2}} \\
 &= (4321)(5321)(1234)^{\frac{n}{2}} \\
 &= (15243)(1234)^{\frac{n}{2}}
 \end{aligned}$$

Eine Matrix ist genau dann in  $\Gamma_E$ , wenn das Bild unter  $\varphi_E$  den Fixpunkt 5 hat. Es ist einfach zu sehen, dass dies in beiden Fällen nicht auftreten kann, womit das Lemma bewiesen wäre.  $\square$

Für das weitere Vorgehen werden auch die Spitzenbreiten benötigt.

Die Spitzenbreite ist in Definition 1.23 als Zahl aus einer Skalierungsmatrix gegeben. Umformen der Gleichung (1.8) führt zu der Identität

$$\gamma_j^{-1} \Gamma_j \gamma_j = \left\langle \begin{pmatrix} 1 & b_j \\ 0 & 1 \end{pmatrix} \right\rangle, \quad (3.21)$$

d.h.  $b_j$  ist die kleinste natürliche Zahl, so dass

$$\gamma_j \begin{pmatrix} 1 & b_j \\ 0 & 1 \end{pmatrix} \gamma_j^{-1} \in \Gamma_E. \quad (3.22)$$

Um die Spitzenbreite zu bestimmen, muss also getestet werden, für welche natürliche Zahl die Matrix aus Formel (3.22) in  $\Gamma_E$  liegt. Dafür wurde in Kapitel 3.3 ein Algorithmus entwickelt.

**Lemma 3.15.** *Die Gruppe  $\Gamma_E$  hat folgende Spitzenbreiten:*

<i>Spitze</i>	0	1	3	6	$\infty$
<i>Breite</i>	8	2	8	2	10

*Beweis:* Der in Kapitel 3.3 beschriebene Algorithmus 1 liefert mit Hilfe von Magma und dem Java-Programm `InGruppe.java` diese Ergebnisse.  $\square$

Bei der durchgeführten Konstruktion wird aus jedem Urbild der Verzweigungsstellen des Belyi-Morphismus' eine Spitze. Nun ist es einfach, die Spitzen den Punkten über den Verzweigungsstellen zuzuordnen.

3 Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$

**Lemma 3.16.** *Für das Belyi-Paar  $(E, \beta)$  und die assoziierte Gruppe  $\Gamma_E$  aus Formel (3.9) sind den 5 Urbildern der Verzweigungsstellen folgende Spitzen zugeordnet:*

$$\begin{aligned}(1, 4) &\longmapsto 0 \\(6, -16) &\longmapsto 6 \\(1, -4) &\longmapsto 3 \\(6, 16) &\longmapsto 1 \\ \infty &\longmapsto \infty\end{aligned}$$

*Beweis:* Sei  $\alpha \in \{0, 1, \infty\}$ . Die Urbilder von  $\alpha$  entsprechen Spitzen von  $\Gamma_E$ , die unter der Wirkung von  $\Gamma(2)$  zu  $\alpha$  äquivalent sind.

Da unter der Wirkung von  $\Gamma(2)$  alle geraden Zahlen äquivalent sind, entsprechen die Spitzen 0 und 6 den Punkten über 0. Aufgrund der Äquivalenz der ungeraden Zahlen unter  $\Gamma(2)$  entsprechen die Spitzen 1 und 3 den Punkten über 1. Die Spitze  $\infty$  entspricht  $\infty$ .

Die Verzweigungsordnung der Punkte läßt sich in die Spitzenbreite übersetzen: Spitzenbreite = Verzweigungsordnung  $\cdot 2$  (die 2 ist die Spitzenbreite der Spitzen von  $\Gamma(2)$ ). Mit den Verzweigungsordnungen aus Formel (3.6) und den Spitzenbreiten aus Lemma 3.15 folgt dann die Behauptung.  $\square$

## 4 Eisensteinreihen und Streumatrizen

Nun wollen wir uns der Berechnung von Eisensteinreihen zu Untergruppen der Modulgruppe zuwenden. Zuerst werden die relevanten Definitionen gegeben. Im zweiten und dritten Abschnitt wird als Beispiel die Gruppe  $\Gamma(2)$  betrachtet.

Da eine Formel für die interessanten Größen im Allgemeinen nicht zu finden ist, wird in den folgenden Unterkapiteln ein Algorithmus zur näherungsweisen Berechnung entwickelt. Dabei werden in Kapitel 4.4 die theoretischen Grundlagen gelegt und in Kapitel 4.5 der Algorithmus beschrieben.

In Kapitel 4.6 wird diese Methode dann auf die Gruppe  $\Gamma_E$  aus Kapitel 3 angewendet und im letzten Abschnitt noch einige weitere Beispiele betrachtet.

### 4.1 Definitionen

**Definition 4.1.** Sei  $\Gamma \subseteq \Gamma(1)$  eine Untergruppe von endlichem Index,  $S_j$  eine Spitze zu  $\Gamma$  und  $\Gamma_j$  der Stabilisator der Spitze. Für  $s \in \mathbb{C}$  mit  $\operatorname{Re}(s) > 1$  und  $z \in \mathbb{H}$  ist die Eisensteinreihe zur Spitze  $S_j$  gegeben durch:

$$E_{S_j}(z, s) = \sum_{\gamma \in \Gamma_j \backslash \Gamma} \operatorname{Im}(\sigma_j^{-1} \gamma(z))^s,$$

wobei  $\sigma_j \in SL_2(\mathbb{R})$  so gewählt ist, dass  $\sigma_j^{-1} \Gamma_j \sigma_j = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ .

Für Eisensteinreihen gilt:

**Satz 4.2.** Sei  $\Gamma \subseteq \Gamma(1)$  eine Untergruppe von endlichem Index,  $S_j$  eine Spitze zu  $\Gamma$  und  $\Gamma_j$  der Stabilisator der Spitze. Für  $s \in \mathbb{C}$ ,  $\operatorname{Re}(s) > 1$  und  $z \in \mathbb{H}$  konvergiert  $E_{S_j}(z, s)$  absolut und lokal gleichmäßig. Die Reihe  $E_{S_j}(z, s)$  lässt sich meromorph auf ganz  $\mathbb{C}$  fortsetzen.

Für eine Spitze  $S_k$  von  $\Gamma$  ist die Fourierentwicklung von  $E_{S_j}(z, s)$  in  $S_k$  gegeben durch

$$E_{S_j}(z, s) \Big|_{S_k} = \delta_{jk} \cdot y^s + \pi^{1/2} \frac{\Gamma\left(s - \frac{1}{2}\right)}{\Gamma(s)} \cdot \varphi_{jk}(s) \cdot y^{1-s} + \sum_{m \neq 0} a_m(y, s) e^{2\pi i m x},$$

wobei  $z = x + iy$  und  $\Gamma(\cdot)$  die  $\Gamma$ -Funktion ist.

Für  $\operatorname{Re}(s) > 1$  berechnet sich der Term  $\varphi_{jk}$  wie folgt:

$$\varphi_{jk}(s) = \frac{1}{(b_j b_k)^s} \sum_{c > 0} r_{jk}^\Gamma(c) \frac{1}{c^{2s}}, \quad (4.1)$$

## 4 Eisensteinreihen und Streumatrizen

wobei  $b_j$  und  $b_k$  die Spitzenbreiten von  $S_j$  und  $S_k$  sind sowie

$$r_{jk}^\Gamma(c) = \# \{d \pmod{b_k c} \mid \exists \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \gamma_j^{-1} \Gamma \gamma_k\}. \quad (4.2)$$

*Beweis:* Die Behauptung folgt analog zu dem Beweis in [Ku1] für normierte Spitzen. Ein schöner Beweis dafür ist auch in [vP] Seiten 37-53 zu finden.  $\square$

**Bemerkung 4.3.** In Satz 4.2 ist die Form des ersten Koeffizienten der Fourrierentwicklung als  $\pi^{1/2} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \cdot \varphi_{jk}(s)$  angegeben. Auch für die weiteren Koeffizienten gibt es Formeln, die etwas komplizierter sind.

Die in dieser Arbeit durchgeführten Berechnungen zu  $\varphi_{jk}(s)$  lassen sich ohne großen Aufwand so modifizieren, dass mit ihnen auch die weiteren Koeffizienten der Eisensteinreihen angenähert werden können.

**Bemerkung 4.4.** Die Zahlen  $\varphi_{jk}$  sind symmetrisch in den Spitzen, d.h.

$$\varphi_{jk}(s) = \varphi_{kj}(s).$$

Siehe dazu z.B. [Iw] Seite 88.

Die einfachste Gruppe, zu der sich Eisensteinreihen dieser Art definieren lassen, ist  $\Gamma(1)$ :

**Beispiel 4.5** (Die Eisensteinreihe zu  $\Gamma(1)$ ). Für die volle Modulgruppe  $\Gamma(1)$  ist die Fourrierentwicklung der Eisensteinreihe bekannt. Da  $\Gamma(1)$  nur eine Spitze hat, gibt es nur eine Entwicklung. Für diese gilt

$$\varphi(s) = \sum_{c=1}^{\infty} \phi(c) \frac{1}{c^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)}, \quad (4.3)$$

wobei  $\phi(\cdot)$  die Eulersche  $\phi$ -Funktion und  $\zeta(\cdot)$  die Riemannsche  $\zeta$ -Funktion ist. Demnach ist

$$r(c) = \phi(c).$$

Die rechte Seite der Gleichung (4.3) ist für alle  $s \neq 1$  definiert und gibt somit eine meromorphe Fortsetzung für  $\varphi(s)$  auf ganz  $\mathbb{C}$ .

Ein Beweis ist in [Iw] auf Seite 60 f oder in [vP] auf Seite 42 zu finden.

**Bemerkung 4.6.** Die Euler'sche  $\phi$ -Funktion  $\phi : \mathbb{N} \rightarrow \mathbb{N}$  gibt für  $n$  die Anzahl der natürlichen Zahlen, die kleiner als  $n$  und teilerfremd zu  $n$  sind, an. Die  $\phi$ -Funktion ist multiplikativ für teilerfremde Zahlen, d.h. für  $m, n \in \mathbb{N}$  mit  $(m, n) = 1$  gilt  $\phi(m)\phi(n) = \phi(mn)$ . Für Primzahlpotenzen  $p^k$  ist  $\phi(p^k) = p^k \left(1 - \frac{1}{p}\right)$ . Es ergibt sich für  $n \in \mathbb{N}$

$$\phi(n) = n \prod_{\substack{p|n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right).$$

Zu Eisensteinreihen lassen sich Streumatrix und Streukonstanten definieren. Die Streumatrix ist durch die  $\varphi_{jk}(s)$  gegeben:

**Definition 4.7.** Für eine Untergruppe  $\Gamma \subset \Gamma(1)$  von endlichem Index mit einem Repräsentantensystem  $S = \{S_1, \dots, S_r\}$  für die Spitzen ist die Streumatrix definiert durch die folgende Matrix meromorpher Funktionen:

$$\Phi_\Gamma(s) = \left( \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \varphi_{jk}(s) \right)_{j,k} \quad (4.4)$$

Die Indizes  $j$  sowie  $k$  stehen für zwei nicht notwendigerweise verschiedene Spitzen und  $\varphi_{jk}(s)$  wurde in Formel (4.1) definiert.

Jeder Eintrag der Streumatrix definiert eine Streukonstante.

**Definition 4.8.** Für eine Untergruppe  $\Gamma \subset \Gamma(1)$  von endlichem Index mit einem Repräsentantensystem  $S = \{S_1, \dots, S_r\}$  für die Spitzen lässt sich für jedes Paar  $S_j, S_k$  die Streukonstante  $C_{jk}$  definieren durch

$$C_{jk} = \lim_{s \rightarrow 1} \left( \Phi_\Gamma(s)_{j,k} - \frac{3/(\pi [\Gamma(1) : \Gamma])}{s-1} \right). \quad (4.5)$$

**Beispiel 4.9.** Für  $\Gamma(1)$  ist die Streukonstante (mit Maple berechnet):

$$\begin{aligned} C^{\Gamma(1)} &= \lim_{s \rightarrow 1} \left( \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \frac{\zeta(2s-1)}{\zeta(2s)} - \frac{3}{\pi(s-1)} \right) \\ &= -\frac{6}{\pi} (12\zeta'(-1) - 1 + \log(4\pi)) \end{aligned}$$

## 4.2 Die Streumatrix zu $\Gamma(2)$

Wie für die Modulgruppe  $\Gamma(1)$  lassen sich auch für andere Gruppen die Koeffizienten der Fourierentwicklungen der Eisensteinreihe berechnen. Auf den folgenden Seiten werden die konstanten Koeffizienten zu  $\Gamma(2)$  berechnet. Diese Gruppe ist um einiges komplizierter als  $\Gamma(1)$ . Als Obergruppe aller Gruppen, die über einen Belyi-Morphismus zu algebraischen Kurven konstruiert werden, ist  $\Gamma(2)$  für diese Arbeit besonders interessant.

Aus Lemma 1.26 ist bekannt, dass die Gruppe  $\Gamma(2)$  die drei Spitzen  $0, 1, \infty$  hat, welche alle die Breite 2 haben.

Gesucht werden die Zahlen

$$r_{jk}^{\Gamma(2)}(c) = \#\{d \pmod{b_k c} \mid \exists \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \gamma_j^{-1} \Gamma(2) \gamma_k\},$$

wobei  $j, k \in \{0, 1, \infty\}$ ,  $b_0 = b_1 = b_\infty = 2$  und die Matrizen  $\gamma_j$  sowie  $\gamma_k$  wie in Formel (3.17) gegeben sind.

Die folgenden beiden Lemmata bereiten Satz 4.12 vor, in dem die  $r_{jk}^{\Gamma(2)}(c)$  für alle  $c \in \mathbb{N}$  und  $j, k \in \{0, 1, \infty\}$  berechnet werden.

**Lemma 4.10.** *Seien  $c$  und  $N$  natürliche Zahlen. Dann gilt für die Menge*

$$\mathcal{A}_c^N := \{d \in \mathbb{N} \mid (c, d) = 1 \text{ und } d < Nc\}, \quad (4.6)$$

dass

$$\#\mathcal{A}_c^N = N \cdot \phi(c). \quad (4.7)$$

*Beweis:* Sei  $a \in \mathcal{A}_c^N$  eine natürliche Zahl mit  $0 < a < c$ , so ist auch  $nc + a \in \mathcal{A}_c^N$  für alle  $n \in \{0, \dots, N-1\}$ . Da  $a \not\equiv 0 \pmod{c}$  und  $nc \equiv 0 \pmod{c}$  ist, folgt  $nc + a \not\equiv 0 \pmod{c}$ . So existieren für jede natürliche Zahl  $a$ , die kleiner als  $c$  und zu  $c$  teilerfremd ist, genau  $N$  verschiedenen Lösungen. Es gibt genau  $\phi(c)$  solche  $a$ , also  $N \cdot \phi(c)$  Lösungen.  $\square$

**Lemma 4.11.** *Seien  $c, d$  fest gewählt mit  $(c, d) = 1$ .*

- (i) *Gilt  $c \equiv 0 \pmod{2}$  sowie  $d \equiv 1 \pmod{2}$ , dann existieren  $a, b \in \mathbb{Z}$  mit  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2}$ , so dass  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ .*
- (ii) *Gilt  $c \equiv 1 \pmod{2}$  sowie  $d \equiv 0 \pmod{2}$ , dann existieren  $a, b \in \mathbb{Z}$  mit  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2}$ , so dass  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ .*
- (iii) *Gilt  $c \equiv 1 \pmod{2}$  sowie  $d \equiv 0 \pmod{2}$ , dann existieren  $a, b \in \mathbb{Z}$  mit  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2}$ , so dass  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ .*
- (iv) *Gilt  $c \equiv 1 \pmod{2}$  sowie  $d \equiv 1 \pmod{2}$ , dann existieren  $a, b \in \mathbb{Z}$  mit  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod{2}$ , so dass  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ .*

## 4.2 Die Streumatrix zu $\Gamma(2)$

*Beweis:* Für teilerfremde Paare  $(c, d) \in \mathbb{Z}^2$  gibt es nach dem euklidischen Algorithmus eine Ergänzung  $a, b$ , so dass  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ . Falls die durch den euklidischen Algorithmus konstruierte Lösung nicht schon den Bedingungen entspricht, erfüllt die Matrix  $\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$  in allen vier Fällen des Lemma 4.11 das Gewünschte.  $\square$

**Satz 4.12.** *Für die Gruppe  $\Gamma(2)$  haben die Koeffizienten  $r_{jk}^{\Gamma(2)}(c)$  für  $c \in \mathbb{N}$  und  $j, k \in \{0, 1, \infty\}$  folgende Form:*

$$\begin{aligned} \text{Für } j = k \text{ ist } r_{jk}^{\Gamma(2)}(c) &= \begin{cases} 2\phi(c), & \text{wenn } c \equiv 0 \pmod{2}; \\ 0, & \text{wenn } c \equiv 1 \pmod{2}. \end{cases} \\ \text{Für } j \neq k \text{ ist } r_{jk}^{\Gamma(2)}(c) &= \begin{cases} \phi(c), & \text{wenn } c \equiv 1 \pmod{2}; \\ 0, & \text{wenn } c \equiv 0 \pmod{2}. \end{cases} \end{aligned}$$

*Beweis:* Sei  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  eine beliebige Matrix in  $\Gamma(1)$ . Für  $j, k \in \{0, 1, \infty\}$  betrachte das Produkt  $\gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1}$  und entscheide unter welchen Voraussetzungen an  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  es in  $\Gamma(2)$  liegt.

$$\begin{aligned} (i) \quad j = \infty \quad k = \infty &\Rightarrow \gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ (ii) \quad j = 0 \quad k = 0 &\Rightarrow \gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \\ (iii) \quad j = 1 \quad k = 1 &\Rightarrow \gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} d-b & a+b-c-d \\ -b & a+b \end{pmatrix} \\ (iv) \quad j = \infty \quad k = 0 &\Rightarrow \gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} \\ (v) \quad j = \infty \quad k = 1 &\Rightarrow \gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -b & a+b \\ -d & c+d \end{pmatrix} \\ (vi) \quad j = 0 \quad k = 1 &\Rightarrow \gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_k^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -d & c+d \\ -b & a+b \end{pmatrix} \end{aligned}$$

In den ersten drei Fällen liegt die resultierende Matrix genau dann in  $\Gamma(2)$ , wenn  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ . Die verbliebenen drei Fälle sind etwas unregelmäßiger:

$$\begin{aligned} \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} \in \Gamma(2) &\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2} \\ \begin{pmatrix} -b & a+b \\ -d & c+d \end{pmatrix} \in \Gamma(2) &\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2} \\ \begin{pmatrix} -d & c+d \\ -b & a+b \end{pmatrix} \in \Gamma(2) &\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod{2} \end{aligned}$$

An den Äquivalenzen sofort zu sehen, dass die Hälfte aller Koeffizienten null ist. In die ersten drei Fälle folgt für gerade  $c$  mit Lemma 4.11:

$$r_{jj}^{\Gamma(2)}(c) = \#\{d \pmod{2c} \mid (c, d) = 1 \text{ und } d \equiv 1 \pmod{2}\}$$

## 4 Eisensteinreihen und Streumatrizen

Die zweite Bedingung ist aber für gerade  $c$  immer erfüllt, sofern die erste erfüllt ist. Also gilt

$$\begin{aligned} r_{jj}^{\Gamma(2)}(c) &= \#\{d \pmod{2c} \mid (c, d) = 1\} \\ &\stackrel{\text{(Lemma 4.10)}}{=} 2\phi(c) \end{aligned}$$

Auch bei ungleichen Spitzen folgt aus Lemma 4.11, dass  $r_{jk}^{\Gamma(2)}(c)$  schon durch die Anzahl der möglichen Paare  $(c, d)$  gegeben ist. Doch lässt sich nicht so einfach argumentieren. Im Fall ungleicher Spitzen muss  $c$  ungerade sein und an  $d$  wird eine Kongruenzbedingung gestellt, die bei ungeraden  $c$  nicht automatisch erfüllt ist.

Sei eine gerade Zahl  $a < 2c$  teilerfremd zu  $c$ . Da  $c$  ungerade ist, ist auch  $\frac{a}{2}$  teilerfremd zu  $c$ . Umgekehrt gilt für eine Zahl  $a < \frac{2c}{2}$ , die teilerfremd zu  $c$  ist, dass für  $2a$  sowohl  $(2a, c) = 1$  als auch  $2a < 2c$  gilt. Es gilt für die Fälle (iv) und (v):

$$\begin{aligned} r_{jk}^{\Gamma(2)}(c) &= \#\{d \pmod{2c} \mid (c, d) = 1 \text{ und } d \equiv 0 \pmod{2}\} \\ &= \#\{d \pmod{c} \mid (c, d) = 1\} \\ &= \phi(c) \end{aligned}$$

Jetzt ist nur noch der letzte Fall zu bearbeiten. Es ist bekannt, dass

$$\#\{d \pmod{2c} \mid (c, d) = 1\} = 2\phi(c),$$

Außerdem wurde eben gezeigt, dass die Hälfte der Zahlen in dieser Menge gerade ist. Die verbleibende Hälfte ist also ungerade und es folgt:

$$\begin{aligned} r_{jk}^{\Gamma(2)}(c) &= \#\{d \pmod{2c} \mid (c, d) = 1 \text{ und } d \equiv 1 \pmod{2}\} \\ &= \phi(c), \end{aligned}$$

womit der letzte Fall gezeigt wäre. □

Eine Liste der ersten 38 Koeffizienten ist in Tabelle 2 auf Seite 47 abgebildet.

### 4.3 Die Streukonstanten zu $\Gamma(2)$

Die Reihenentwicklung der Einträge der Streumatrix der Gruppe  $\Gamma(2)$  ist bekannt und durch Vielfache der Euler'schen  $\phi$ -Funktion gegeben. Die Formel findet sich in Satz 4.12.

### 4.3 Die Streukonstanten zu $\Gamma(2)$

$c$	$\phi(c)$	$r_{\infty\infty}^{\Gamma(2)}(c)$	$r_{\infty 0}^{\Gamma(2)}(c)$	$r_{\infty 1}^{\Gamma(2)}(c)$	$r_{00}^{\Gamma(2)}(c)$	$r_{01}^{\Gamma(2)}(c)$	$r_{11}^{\Gamma(2)}(c)$
1	1	0	1	1	0	1	0
2	1	2	0	0	2	0	2
3	2	0	2	2	0	2	0
4	2	4	0	0	4	0	4
5	4	0	4	4	0	4	0
6	2	4	0	0	4	0	4
7	6	0	6	6	0	6	0
8	4	8	0	0	8	0	8
9	6	0	6	6	0	6	0
10	4	8	0	0	8	0	8
11	10	0	10	10	0	10	0
12	4	8	0	0	8	0	8
13	12	0	12	12	0	12	0
14	6	12	0	0	12	0	12
15	8	0	8	8	0	8	0
16	8	16	0	0	16	0	16
17	16	0	16	16	0	16	0
18	6	12	0	0	12	0	12
19	18	0	18	18	0	18	0
20	8	16	0	0	16	0	16
21	12	0	12	12	0	12	0
22	10	20	0	0	20	0	20
23	22	0	22	22	0	22	0
24	8	16	0	0	16	0	16
25	20	0	20	20	0	20	0
26	12	24	0	0	24	0	24
27	18	0	18	18	0	18	0
28	12	24	0	0	24	0	24
29	28	0	28	28	0	28	0
30	8	16	0	0	16	0	16
31	30	0	30	30	0	30	0
32	16	32	0	0	32	0	32
33	20	0	20	20	0	20	0
34	16	32	0	0	32	0	32
35	24	0	24	24	0	24	0
36	12	24	0	0	24	0	24
37	36	0	36	36	0	36	0
38	18	36	0	0	36	0	36

Tabelle 2: Die Koeffizienten der Streumatrix zu  $\Gamma(2)$

#### 4 Eisensteinreihen und Streumatrizen

Für die Berechnung der Streukonstanten benötigen wir eine andere Darstellung der Einträge der Streumatrix. Zuerst werden einige Funktionen eingeführt. Der Dirichlet-Charakter  $\chi_2$  sei definiert durch

$$\chi_2(n) := \begin{cases} 1 & \text{wenn } (n, 2) = 1 \\ 0 & \text{wenn } (n, 2) = 2 \end{cases} \quad \text{für } n \in \mathbb{Z}.$$

Mit Hilfe des Charakters kann eine  $L$ -Reihe definiert werden. Es sei für  $s \in \mathbb{C}$  mit  $\operatorname{Re}(s) > 1$  die  $L$ -Reihe zum Charakter  $\chi_2$  gegeben als

$$L(\chi_2, s) := \sum_{c>0} \chi_2(c) \frac{1}{c^s}.$$

Diese Dirichlet-Reihen lassen sich auch durch Vielfache der Riemannschen  $\zeta$ -Funktion darstellen. Es gilt

$$L(\chi_2, 2s) = \sum_{c>0} \chi_2(c) \frac{1}{c^{2s}} = \sum_{c>0} \frac{1}{(2c-1)^{2s}} = 2^{-2s}(-1 + 2^{2s})\zeta(2s)$$

und dementsprechend

$$L(\chi_2, 2s-1) = 2^{-2s}(-2 + 2^{2s})\zeta(2s-1).$$

Für den Quotienten ergibt sich:

$$\frac{L(\chi_2, 2s-1)}{L(\chi_2, 2s)} = \frac{(-2 + 2^{2s})\zeta(2s-1)}{(-1 + 2^{2s})\zeta(2s)}$$

Es gilt

**Satz 4.13.** *Für die Gruppe  $\Gamma(2)$  gilt für  $j \neq k$*

$$\varphi_{jk}^{\Gamma(2)}(s) = \sum_{c>1} \chi_2(c) \phi(c) \frac{1}{c^{2s}} = \frac{L(\chi_2, 2s-1)}{L(\chi_2, 2s)} \quad (4.8)$$

und für  $j = k$

$$\varphi_{jk}^{\Gamma(2)}(s) = \sum_{c>1} \chi_2(c+1) \cdot 2 \cdot \phi(c) \frac{1}{c^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)} - \frac{L(\chi_2, 2s-1)}{L(\chi_2, 2s)}. \quad (4.9)$$

## 4.4 Doppelnebenklassen und Streumatrizen

*Beweis:* Die jeweils erste Gleichheit in den Formeln (4.8) und (4.9) folgt aus den Ergebnissen von Satz 4.12 und der Definition von  $\varphi_{jk}^{\Gamma(2)}$ . Die zweite Gleichheit ergibt sich durch Ausmultiplizieren der  $L$ -Reihen.  $\square$

Mit Satz 4.13 und der Definition 4.8 und dem Wissen über die Darstellbarkeit der  $L$ -Reihen mit Hilfe der Riemann'schen  $\zeta$ -Funktion lassen sich die Streukonstanten berechnen. Für die Streukonstante von  $\Gamma(2)$  für  $j \neq k$  gilt

$$C_{jk}^{\Gamma(2)} = \lim_{s \rightarrow 1} \left( \frac{\pi^{1/2}}{4^s} \cdot \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \frac{L(\chi_2, 2s-1)}{L(\chi_2, 2s)} - \frac{3}{6\pi(s-1)} \right) \quad (4.10)$$

$$= -\frac{1}{3\pi} (7 \log(2) + 3 \log(\pi) + 36\zeta'(-1) - 3) \quad (4.11)$$

$$\approx 0,07097687113 \quad (4.12)$$

und

$$C_{jj}^{\Gamma(2)} = \lim_{s \rightarrow 1} \left( \frac{2\pi^{1/2}}{4^s} \cdot \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \left( \frac{\zeta(2s-1)}{\zeta(2s)} - \frac{L(\chi_2, 2s-1)}{L(\chi_2, 2s)} \right) - \frac{3}{6\pi(s-1)} \right) \quad (4.13)$$

$$= -\frac{1}{3\pi} (13 \log(2) + 3 \log(\pi) + 36\zeta'(-1) - 3) \quad (4.14)$$

$$\approx -0,3702943296. \quad (4.15)$$

## 4.4 Doppelnebenklassen und Streumatrizen

Untergruppen von  $\Gamma(1)$  von endlichem Index können in Doppelnebenklassen zerlegt werden. Wie diese Zerlegung aussieht wird in Lemma 4.14 gezeigt.

Die Berechnung der konstanten Koeffizienten der Eisensteinreihe zu  $\Gamma(2)$  im letzten Abschnitt war recht aufwendig. Bei komplizierteren Gruppen wird das direkte Ausrechnen der Koeffizienten nach Formel (4.2) selten möglich sein. Wie Satz 4.17 zeigt, kann Zerlegung in Doppelnebenklassen die Berechnung vereinfachen. Um dies zu nutzen, wird am Ende des Unterkapitels ein Algorithmus zum Abzählen der Nebenklassen vorgestellt.

**Lemma 4.14.** *Seien  $\Gamma$  eine Untergruppe der  $\Gamma(1)$  von endlichem Index,  $S_j$  und  $S_k$  zwei nicht notwendigerweise verschiedene Spitzen von  $\Gamma$ . Mit  $\Gamma_j$  respektive  $\Gamma_k$  seien die Stabilisatoren der Spitzen benannt und  $b_j, b_k$  seien die Spitzenbreiten. Die Gruppen  $B_j$  und  $B_k$  werden definiert als*

$$\begin{aligned} B_j &:= \gamma_j^{-1} \Gamma_j \gamma_j = \left\langle \begin{pmatrix} 1 & b_j \\ 0 & 1 \end{pmatrix} \right\rangle & \text{und} \\ B_k &:= \gamma_k^{-1} \Gamma_k \gamma_k = \left\langle \begin{pmatrix} 1 & b_k \\ 0 & 1 \end{pmatrix} \right\rangle, \end{aligned} \quad (4.16)$$

wobei  $\gamma_j, \gamma_k \in \Gamma(1)$  so gewählt sind, dass  $\gamma_j^{-1}(S_j) = \gamma_k^{-1}(S_k) = \infty$ .

#### 4 Eisensteinreihen und Streumatrizen

Mit den eben eingeführten Benennungen gilt

$$\gamma_j^{-1}\Gamma\gamma_k = \delta_{jk}B_j \cup \bigcup_{c>0} \bigcup_{d \bmod b_k c} B_j \begin{pmatrix} * & * \\ c & d \end{pmatrix} B_k, \quad (4.17)$$

wobei über alle  $c > 0$  und  $d \bmod b_k c$  summiert wird, so dass  $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \gamma_j^{-1}\Gamma\gamma_k$ .

*Beweis:* Dass  $B_j$  genau dann in  $\gamma_j^{-1}\Gamma\gamma_k$  liegt, wenn  $S_j = S_k$  ist, lässt sich einfach zeigen:

Angenommen in  $\gamma_j^{-1}\Gamma\gamma_k$  liegt ein Element  $\omega$  mit der Eigenschaft  $\omega(\infty) = \infty$ . Dann gibt es ein  $\gamma \in \Gamma$ , so dass  $\omega = \gamma_j^{-1}\gamma\gamma_k$ . Nun ist aber

$$\gamma(S_k) = \gamma_j\omega\gamma_k^{-1}(S_k) = \gamma_j(\infty) = S_j.$$

Dies bedeutet, dass die beiden Spitzen äquivalent sind. Dann gilt auch  $B_j = B_k$ . Damit ist gezeigt, wie es zu dem Anteil  $\delta_{jk}B_j$  in der Vereinigung aus Formel (4.17) kommt.

Betrachten wir nun also die restlichen Elemente. Ein beliebiges Element von  $\gamma_j^{-1}\Gamma\gamma_k$ , das  $\infty$  nicht fixiert, hat die Form  $\begin{pmatrix} a & * \\ c & d \end{pmatrix}$  mit  $c > 0$ . Da für  $b_j|m$  und  $b_k|n$

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & * \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+cm & * \\ c & d+cn \end{pmatrix} \quad (4.18)$$

gilt, bestimmt die Doppelnebenklasse  $B_j \begin{pmatrix} * & * \\ c & d \end{pmatrix} B_k$  den Wert von  $c$  eindeutig und  $d$  bis auf Vielfache von  $b_k c$ .

Seien  $c$  und  $d$  gegeben. Für zwei Matrizen  $\omega = \begin{pmatrix} a & * \\ c & d \end{pmatrix}$  und  $\omega' = \begin{pmatrix} a' & * \\ c & d \end{pmatrix}$  aus  $\gamma_j^{-1}\Gamma\gamma_k$  lässt die Komposition  $\omega'\omega^{-1} = \begin{pmatrix} a' & * \\ c & d \end{pmatrix} \begin{pmatrix} d & * \\ -c & a \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$  die Spitze  $\infty$  invariant. Es existieren  $\gamma$  und  $\gamma'$  mit  $\omega = \gamma_j^{-1}\gamma\gamma_k$  und  $\omega' = \gamma_j^{-1}\gamma'\gamma_k$ . Nun gilt

$$\omega'\omega^{-1} = \gamma_j^{-1}\gamma'\gamma_k\gamma_k^{-1}\gamma^{-1}\gamma_j = \gamma_j^{-1}\gamma'\gamma^{-1}\gamma_j.$$

Also ist

$$\gamma_j\omega'\omega^{-1}\gamma_j^{-1} \in \Gamma$$

und

$$\gamma_j\omega'\omega^{-1}\gamma_j^{-1}(S_j) = \gamma_j\omega'\omega^{-1}(\infty) = \gamma_j(\infty) = S_j.$$

Daraus folgt, dass  $\gamma_j\omega'\omega^{-1}\gamma_j^{-1} \in \Gamma_j$  ist und somit  $\omega'\omega^{-1} \in B_j$ , da es sich um das konjugierte Element zu einem Element aus  $\Gamma_j$  handelt. Die Differenz zweier Matrizen zu festem Paar  $(c, d)$  liegt also in  $B_j$ . Für die Doppelnebenklasse ist somit die obere Zeile der Matrix unerheblich.  $\square$

#### 4.4 Doppelnebenklassen und Streumatrizen

**Korollar 4.15.** Die Zahl  $r_{jk}^\Gamma(c)$  aus Formel (4.2) ist gleich der Anzahl der Doppelnebenklassen zu diesem  $c$ :

Sei  $\kappa \in B_j \setminus \gamma_j^{-1} \Gamma \gamma_k / B_k$ , so gilt für alle  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \kappa$  und  $\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \in \kappa$ , dass  $c = \tilde{c}$ . Es folgt somit aus Lemma 4.14:

$$r_{jk}^\Gamma(c) = \# \{ \kappa \in B_j \setminus \gamma_j^{-1} \Gamma \gamma_k / B_k \mid \exists \begin{pmatrix} * & * \\ c & * \end{pmatrix} \in \kappa \}$$

**Lemma 4.16.** Sei  $\begin{pmatrix} a & * \\ c & d \end{pmatrix} \in \gamma_j^{-1} \Gamma \gamma_k$ , dann gibt es einen eindeutigen Repräsentanten bezüglich der Zerlegung aus Formel (4.17) der Form

$$\begin{pmatrix} \tilde{a} & * \\ c & \tilde{d} \end{pmatrix} \quad \text{mit} \quad 0 \leq \tilde{a} < cb_j \quad \text{und} \quad 0 \leq \tilde{d} < cb_k. \quad (4.19)$$

*Beweis:* Zwei Matrizen liegen in einer Nebenklasse, wenn sie durch Multiplikation mit Elementen aus  $B_j$  von links und  $B_k$  von rechts auseinander hervorgehen.

Es existieren eindeutig bestimmte  $m, n \in \mathbb{Z}$  und  $r, s \in \mathbb{N}$  mit  $0 \leq r < cb_j$  und  $0 \leq s < cb_k$ , so dass

$$a = mcb_j + r \quad \text{und} \quad d = ncb_k + s$$

ist.

Dann ist

$$\begin{pmatrix} 1 & -mb_j \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & * \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -nb_k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a - mcb_j & * \\ c & d - ncb_k \end{pmatrix} = \begin{pmatrix} r & * \\ c & s \end{pmatrix}.$$

Mit  $\tilde{a} = r$  und  $\tilde{d} = s$  leistet  $\begin{pmatrix} \tilde{a} & * \\ c & \tilde{d} \end{pmatrix}$  das Gewünschte. □

**Satz 4.17.** Mit den Voraussetzungen von Lemma 4.14 gilt: Um  $r_{jk}^\Gamma(c)$ , siehe Formel (4.2), zu berechnen, genügt es, alle Matrizen aus

$$\mathcal{M}_c = \left\{ \begin{pmatrix} a & * \\ c & d \end{pmatrix} \in \Gamma(1) \mid 0 \leq a < cb_j \quad \text{und} \quad 0 \leq d < cb_k \right\}$$

dahingehend zu testen, ob sie in  $\gamma_j^{-1} \Gamma \gamma_k$  liegen, denn

$$r_{jk}^\Gamma(c) = \# \{ \gamma \in \mathcal{M}_c \mid \gamma \in \gamma_j^{-1} \Gamma \gamma_k \}.$$

#### 4 Eisensteinreihen und Streumatrizen

*Beweis:* Der Satz folgt aus Korollar 4.15 und Lemma 4.16.  $\square$

Die Menge  $\mathcal{M}_c$  lässt sich noch genauer beschreiben. Aus Formel (4.18) folgt

$$\begin{aligned} \mathcal{M}_c &= \left\{ \begin{pmatrix} a+mc & * \\ c & d+nc \end{pmatrix} \mid \begin{pmatrix} a+mc & * \\ c & d+nc \end{pmatrix} \in \Gamma(1); 0 \leq a, d < c; \right. \\ &\quad \left. 0 \leq m < b_j; 0 \leq n < b_k \right\} \\ &= \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & * \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid \begin{pmatrix} a & * \\ c & d \end{pmatrix} \in \Gamma(1); 0 \leq a, d < c; \right. \\ &\quad \left. 0 \leq m < b_j; 0 \leq n < b_k \right\}. \end{aligned} \tag{4.20}$$

Außerdem muss für eine Matrix  $\begin{pmatrix} a & * \\ c & d \end{pmatrix} \in \mathcal{M}_c$  folgendes gelten:

- (i)  $\text{ggT}(c, a) = 1$
- (ii)  $\text{ggT}(c, d) = 1$
- (iii)  $ad \equiv 1 \pmod{c}$

Wenn  $a, d < c$  angenommen werden, folgt aus diesen drei Eigenschaften, dass schon  $d$  den Wert von  $a$  eindeutig bestimmt, da  $a$  und  $d$  als Elemente aus  $(\mathbb{Z}/c\mathbb{Z})^*$  zueinander invers sein müssen. Also ist

$$\mathcal{M}_c = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & * \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid 0 \leq a, d < c; \text{ggT}(c, d) = 1; \right. \\ \left. ad \equiv 1 \pmod{c}; 0 \leq m < b_j; 0 \leq n < b_k \right\}. \tag{4.21}$$

---

#### **Algorithmus 2** Abzählen der Nebenklassen

---

- 1: **for**  $d$  von 0 bis  $c - 1$  **do**
  - 2:   **if**  $\text{ggT}(c, d) = 1$  **then**
  - 3:     Erstelle eine Matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , bei der die Einträge  $a$  und  $b$  kleiner als  $c$  sind.  
   Diese Matrix ist eindeutig bestimmt.
  - 4:     **for**  $m$  von 0 bis  $b_j - 1$  **do**
  - 5:       **for**  $n$  von 0 bis  $b_k - 1$  **do**
  - 6:         Berechne  $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ . (\*)
  - 7:       **end for**
  - 8:     **end for**
  - 9:   **end if**
  - 10: **end for**
- 

Mit diesen Informationen lässt sich ein Algorithmus finden, um alle Elemente von  $\mathcal{M}_c$  abzuzählen, siehe Algorithmus 2.

## 4.5 Ein Algorithmus zur Berechnung von Streumatrizen

In Zeile 6, die mit  $(*)$  gekennzeichnet ist, des Algorithmus 2 von Seite 52 werden alle Matrizen aus  $\mathcal{M}_c$  genau einmal berechnet.

### 4.5 Ein Algorithmus zur Berechnung von Streumatrizen

Die Vorarbeit aus den Kapiteln 3.3 und 4.4 wird nun genutzt um einen Algorithmus zur Berechnung von Streumatrizen zu entwickeln.

Ausgegangen wird von einer Gruppe  $\Gamma \subset \Gamma(2)$ , die als Urbild einer Stabilisatoruntergruppe zu einem Element  $a$  unter einem Morphismus

$$\varphi : \Gamma(2) \twoheadrightarrow G$$

gegeben ist, wobei  $G$  eine endliche Permutationsgruppe ist. Dies entspricht genau den Daten, die das Vorgehen aus Kapitel 2.3 liefert, wo Äquivalenzen zu Belyi-Paaren betrachtet wurden.

Seien  $S_j$  und  $S_k$  zwei Spitzen von  $\Gamma$  mit Spitzenbreiten  $b_j$  und  $b_k$ . Dann ist der Eintrag der Streumatrix zu  $S_j$  und  $S_k$  gegeben durch

$$\pi^{1/2} \frac{\Gamma(s - 1/2)}{\Gamma(s)} \cdot \frac{1}{(b_j b_k)^s} \sum_{c>0} \frac{r_{jk}^\Gamma(c)}{c^{2s}}.$$

Vergleiche dazu die Definition 4.7 und Formel (4.1). Um einen Eintrag zu berechnen, benötigt man also die Koeffizienten  $r_{jk}^\Gamma(c)$ , wobei

$$r_{jk}^\Gamma(c) = \# \{ d \pmod{b_k c} \mid \exists \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \gamma_j^{-1} \Gamma \gamma_k \}.$$

Der Satz 4.17 reduziert die Berechnung des  $c$ -ten Koeffizienten der Eisensteinreihe zu  $S_j$  entwickelt in  $S_k$  dahingehend, dass nur noch aus einer endlichen Menge  $\mathcal{M}_c$ , siehe Formel (4.21), jene Elemente ausgewählt werden müssen, die in  $\gamma_j^{-1} \Gamma \gamma_k$  liegen. Die Kardinalität dieser Teilmenge ist dann der Koeffizient. Der Algorithmus 2 zählt die Elemente aus  $\mathcal{M}_c$  ab.

Um zu testen, ob die mit dem Algorithmus konstruierten Elemente in  $\gamma_j^{-1} \Gamma \gamma_k$  liegen, kann der Algorithmus 1 von Seite 36 in verallgemeinerter Form benutzt werden.

Der Algorithmus 1 prüft eine Matrix auf ihre Zugehörigkeit zu der in Kapitel 3.3 behandelten Gruppe  $\Gamma_E$ . Er kann auf das Problem, ob ein Element  $\mu$  aus  $\mathcal{M}_c$  in  $\gamma_j^{-1} \Gamma \gamma_k$  liegt, angewendet werden, indem die Frage zu

$$\gamma_j \mu \gamma_k^{-1} \stackrel{?}{\in} \Gamma$$

umformuliert wird. Außerdem müssen natürlich die Daten zu  $\Gamma_E$  mit denen zu  $\Gamma$  ausgetauscht werden.

**Algorithmus 3** Berechnung des  $c$ -ten Koeffizienten zu  $S_j$  und  $S_k$ 


---

```

1: Koeffizient=0
2: for  $d$  von 0 bis  $c - 1$  do
3:   if  $\text{ggT}(c, d) = 1$  then
4:     Erstelle eine Matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  mit Einträgen  $a$  und  $b$  kleiner als  $c$ .
5:     for  $m$  von 0 bis  $b_j - 1$  do
6:       for  $n$  von 0 bis  $b_k - 1$  do
7:         Berechne  $M = \gamma_j \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \gamma_k^{-1}$ .
8:         if  $M \in \Gamma(2)$  then
9:           Finde das Wort von  $M$  in den Erzeugern von  $\Gamma(2)$ .
10:          Bestimme  $\varphi(M)$ .
11:          if  $\varphi(M)(a) = a$  then
12:            Koeffizient = Koeffizient + 1
13:          end if
14:        end if
15:      end for
16:    end for
17:  end if
18: end for
19: return Koeff

```

---

Das Schema für einen Algorithmus zur Berechnung des  $c$ -ten Koeffizienten des Eintrags der Streumatrix zu den Spitzen  $S_j$  und  $S_k$  ist in Algorithmus 3 zu sehen.

**Bemerkung 4.18.** *Mit dem Algorithmus 3 ist die Streumatrix zwar nicht exakt zu berechnen, weil man dafür unendlich viele Koeffizienten bräuchte, doch kann eine Näherung erstellt werden.*

## 4.6 Die Streumatrix zur Gruppe $\Gamma_E$

Die Gruppe  $\Gamma_E$  wurde in Kapitel 3.2 eingeführt. Eine Beschreibung der Gruppe ist in Satz (3.10) auf Seite 30 zu finden.

Zu dieser Gruppe soll nun die Streumatrix berechnet werden. Dazu wurde der Algorithmus 3 von Seite 54 für das Computeralgebraprogramm Magma implementiert. Der Programmcode ist im Anhang unter A.2 auf Seite 101 zu finden. Das Programm berechnet eine Reihe von Koeffizienten zu einem gegebenen Spitzenpaar.

Die mit dem Magma-Programm berechneten Koeffizienten sind in Tabelle 3 auf Seite 56 zu sehen.

**Hinweise zur Flexibilität der Implementierung:** Einige grundlegende Daten werden am Anfang des Programmcodes auf Seite 101 festgelegt. Dies erlaubt es, die Implementierung einfach an unterschiedliche Gruppen und Spitzen anzupassen.

Die Daten sind:

- Der Bereich `cmin` bis `cmax`, in dem die Koeffizienten berechnet werden sollen.
- Die Spitzen `j`, `k` und die Spitzenbreiten `bj`, `bk`, wobei nur ganze Zahlen als Spitzen verstanden werden. Die Eingabe von `-1` wird als  $\infty$  interpretiert.
- Ein Dateiname `datei`, unter welchem die Koeffizienten gespeichert werden sollen.
- Die Gruppe  $\Gamma_E$ . Um die Gruppe zu beschreiben, werden die Symmetriegruppe `P`, das Bild der Erzeuger von  $\Gamma(2)$  `p1` und `p2` sowie das Stabilisatorelement `stab` angegeben.

Diese Implementierung erlaubt es, das Programm für alle Spitzenpaare der Gruppe  $\Gamma_E$  zu nutzen, indem ausschließlich die Daten zu den Spitzen angepasst werden.

Auch die Anpassung an andere Gruppen ist einfach; hierbei muss zusätzlich die Definition der Gruppe angepasst werden. Für den Fall, dass in einer Gruppe Spitzen auftreten, die keinen ganzzahligen Repräsentanten haben, muss das Programm stärker verändert werden. Doch die Erweiterung auf Brüche birgt keine Probleme.

Tabelle 3: Die Koeffizienten zum Belyi-Paar  $(E, \beta)$ 

$c$	$\phi(c)$	$r_{\infty\infty}^{\Gamma_E}$	$r_{\infty 0}^{\Gamma_E}$	$r_{\infty 1}^{\Gamma_E}$	$r_{\infty 3}^{\Gamma_E}$	$r_{\infty 6}^{\Gamma_E}$	$r_{00}^{\Gamma_E}$	$r_{01}^{\Gamma_E}$	$r_{03}^{\Gamma_E}$	$r_{06}^{\Gamma_E}$	$r_{11}^{\Gamma_E}$	$r_{13}^{\Gamma_E}$	$r_{16}^{\Gamma_E}$	$r_{33}^{\Gamma_E}$	$r_{36}^{\Gamma_E}$	$r_{66}^{\Gamma_E}$
1	1	0	4	1	4	1	0	1	3	0	0	0	0	0	1	0
2	1	10	0	0	0	0	6	0	0	2	0	2	0	6	0	0
3	2	0	8	2	8	2	0	2	6	0	0	0	0	0	2	0
4	2	20	0	0	0	0	12	0	0	4	0	4	0	12	0	0
5	4	0	16	4	16	4	0	0	16	0	0	0	4	0	0	0
6	2	20	0	0	0	0	12	0	0	4	0	4	0	12	0	0
7	6	0	24	6	24	6	0	6	18	0	0	0	0	0	6	0
8	4	40	0	0	0	0	26	0	0	6	2	6	0	26	0	2
9	6	0	24	6	24	6	0	6	18	0	0	0	0	0	6	0
10	4	40	0	0	0	0	30	0	0	2	6	2	0	30	0	6
11	10	0	40	10	40	10	0	6	34	0	0	0	4	0	6	0
12	4	40	0	0	0	0	26	0	0	6	2	6	0	26	0	2
13	12	0	48	12	48	12	0	10	38	0	0	0	2	0	10	0
14	6	60	0	0	0	0	40	0	0	8	4	8	0	40	0	4
15	8	0	32	8	32	8	0	4	28	0	0	0	4	0	4	0
16	8	80	0	0	0	0	50	0	0	14	2	14	0	50	0	2
17	16	0	64	16	64	16	0	14	50	0	0	0	2	0	14	0
18	6	60	0	0	0	0	36	0	0	12	0	12	0	36	0	0
19	18	0	72	18	72	18	0	18	54	0	0	0	0	0	18	0
20	8	80	0	0	0	0	56	0	0	8	8	8	0	56	0	8
21	12	0	48	12	48	12	0	8	40	0	0	0	4	0	8	0
22	10	100	0	0	0	0	60	0	0	20	0	20	0	60	0	0
23	22	0	88	22	88	22	0	22	66	0	0	0	0	0	22	0
24	8	80	0	0	0	0	50	0	0	14	2	14	0	50	0	2

Tabelle 3: Die Koeffizienten zum Belyi-Paar  $(E, \beta)$

$c$	$\phi(c)$	$r_{\infty\infty}^{\Gamma_E}$	$r_{\infty 0}^{\Gamma_E}$	$r_{\infty 1}^{\Gamma_E}$	$r_{\infty 3}^{\Gamma_E}$	$r_{\infty 6}^{\Gamma_E}$	$r_{00}^{\Gamma_E}$	$r_{01}^{\Gamma_E}$	$r_{03}^{\Gamma_E}$	$r_{06}^{\Gamma_E}$	$r_{11}^{\Gamma_E}$	$r_{13}^{\Gamma_E}$	$r_{16}^{\Gamma_E}$	$r_{33}^{\Gamma_E}$	$r_{36}^{\Gamma_E}$	$r_{66}^{\Gamma_E}$
25	20	0	80	20	80	20	0	12	68	0	0	0	8	0	12	0
26	12	120	0	0	0	0	72	0	0	24	0	24	0	72	0	0
27	18	0	72	18	72	18	0	10	62	0	0	0	8	0	10	0
28	12	120	0	0	0	0	72	0	0	24	0	24	0	72	0	0
29	28	0	112	28	112	28	0	28	84	0	0	0	0	0	28	0
30	8	80	0	0	0	0	56	0	0	8	8	8	0	56	0	8
31	30	0	120	30	120	30	0	30	90	0	0	0	0	0	30	0
32	16	160	0	0	0	0	102	0	0	26	6	26	0	102	0	6
33	20	0	80	20	80	20	0	20	60	0	0	0	0	0	20	0
34	16	160	0	0	0	0	104	0	0	24	8	24	0	104	0	8
35	24	0	96	24	96	24	0	14	82	0	0	0	10	0	14	0
36	12	120	0	0	0	0	76	0	0	20	4	20	0	76	0	4
37	36	0	144	36	144	36	0	22	122	0	0	0	14	0	22	0
38	18	180	0	0	0	0	116	0	0	28	8	28	0	116	0	8
39	24	0	96	24	96	24	0	20	76	0	0	0	4	0	20	0
40	16	160	0	0	0	0	114	0	0	14	18	14	0	114	0	18
41	40	0	160	40	160	40	0	36	124	0	0	0	4	0	36	0
42	12	120	0	0	0	0	72	0	0	24	0	24	0	72	0	0
43	42	0	168	42	168	42	0	30	138	0	0	0	12	0	30	0
44	20	200	0	0	0	0	126	0	0	34	6	34	0	126	0	6
45	24	0	96	24	96	24	0	14	82	0	0	0	10	0	14	0
46	22	220	0	0	0	0	136	0	0	40	4	40	0	136	0	4
47	46	0	184	46	184	46	0	42	142	0	0	0	4	0	42	0
48	16	160	0	0	0	0	102	0	0	26	6	26	0	102	0	6

4.6 Die Streumatrix zur Gruppe  $\Gamma_E$

## 4.7 Weitere Beispiele

An dieser Stelle sollen noch für einige weitere Kurven die ersten Koeffizienten der Reihen in der Streumatrix berechnet werden, um mehr Daten zu erhalten.

Auf eine detaillierte Ausführung der Rechnungen ist verzichtet worden. Die Berechnung der Spitzen und der Spitzenbreiten folgt dem Schema aus Kapitel 3.3. Der Algorithmus, der im Anhang unter A.2 abgedruckt ist, wurde mit den entsprechenden Daten benutzt. Die beiden Belyi-Paare sind [KS] entnommen.

**Beispiel 4.19.** Die Kurve  $C_1$  mit dem Morphismus  $\beta_{C_1}$  bilden ein Belyi-Paar vom Grad 3:

$$\begin{aligned} C_1 : y^2 &= x^3 + 4 \\ \beta_{C_1}(x, y) &= \frac{y+2}{4} \end{aligned} \quad (4.22)$$

Der Morphismus  $\beta_{C_1}$  ist dreifach verzweigt über den Stellen  $0, 1$  und  $\infty$ . Schon durch diese Information steht das Dessin fest: Es hat zwei Ecken, drei Kanten und eine Fläche. Es kommt nur das Dessin aus Abbildung 11 in Frage.

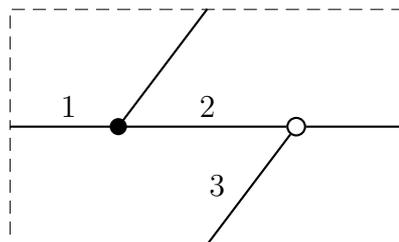


Abbildung 11: Dessin zu  $(C_1, \beta_{C_1})$

Die Permutationen  $\sigma_0, \sigma_1$  und  $\sigma_\infty$  sind alle gleich dem 3-Zykel  $(123)$ . Damit ist die durch die  $\sigma$ 's erzeugte Gruppe  $G_{C_2} := \{id, (123), (132)\} \cong \mathbb{Z}/3\mathbb{Z}$  und der Stabilisator jeder Kante ist trivial. Die entsprechend Formel (2.4) definierte Abbildung  $\varphi_{C_2} : \Gamma(2) \rightarrow G_{C_2}$  bildet beide Erzeuger von  $\Gamma(2)$  auf das gleiche Element ab. Die gesuchte Gruppe ist der Kern der Abbildung.

Die drei Urbilder von  $0, 1, \infty$  entsprechen drei Spitzen, die alle gleich breit sind, nämlich  $3 \cdot 2 = 6$  (Multiplizität der Urbilder mal Breite der Spitzen von  $\Gamma(2)$ ). Dies müssen die selben Spitzen wie die von  $\Gamma(2)$  sein, denn Spitzen, die unter  $\Gamma(2)$  schon nicht äquivalent sind, können dies nicht unter einer Untergruppe sein.

Nun sind alle für das Anwenden des Algorithmus 3 von Seite 54 aus Kapitel 4.5 notwendigen Informationen bekannt. Das Programm aus A.2 kann also mit einigen Modifikationen angewendet werden. Die Ergebnisse sind in Tabelle 4 auf Seite 59 zu sehen.

## 4.7 Weitere Beispiele

$c$	$\phi(c)$	$r_{\infty\infty}^{C_1}(c)$	$r_{\infty 0}^{C_1}(c)$	$r_{\infty 1}^{C_1}(c)$	$r_{00}^{C_1}(c)$	$r_{01}^{C_1}(c)$	$r_{11}^{C_1}(c)$
1	1	0	3	3	0	3	0
2	1	6	0	0	6	0	6
3	2	0	6	6	0	6	0
4	2	12	0	0	12	0	12
5	4	0	12	12	0	12	0
6	2	12	0	0	12	0	12
7	6	0	18	18	0	18	0
8	4	24	0	0	24	0	24
9	6	0	18	18	0	18	0
10	4	24	0	0	24	0	24
11	10	0	30	30	0	30	0
12	4	24	0	0	24	0	24
13	12	0	36	36	0	36	0
14	6	36	0	0	36	0	36
15	8	0	24	24	0	24	0
16	8	48	0	0	48	0	48
17	16	0	48	48	0	48	0
18	6	36	0	0	36	0	36
19	18	0	54	54	0	54	0
20	8	48	0	0	48	0	48
21	12	0	36	36	0	36	0
22	10	60	0	0	60	0	60
23	22	0	66	66	0	66	0
24	8	48	0	0	48	0	48
25	20	0	60	60	0	60	0
26	12	72	0	0	72	0	72
27	18	0	54	54	0	54	0
28	12	72	0	0	72	0	72
29	28	0	84	84	0	84	0
30	8	48	0	0	48	0	48
31	30	0	90	90	0	90	0
32	16	96	0	0	96	0	96
33	20	0	60	60	0	60	0
34	16	96	0	0	96	0	96
35	24	0	72	72	0	72	0
36	12	72	0	0	72	0	72
37	36	0	108	108	0	108	0
38	18	108	0	0	108	0	108

Tabelle 4: Die Koeffizienten zum Belyi-Paar  $(C_1, \beta_{C_1})$

#### 4 Eisensteinreihen und Streumatrizen

**Beispiel 4.20.** Ein weiteres Belyi-Paar von kleinem Grad bildet das Paar

$$\begin{aligned} C_2 : y^2 &= x^3 + Ax, \\ \beta_{C_2}(x, y) &= -\frac{x^2}{A}, \end{aligned} \quad (4.23)$$

für  $A \in \mathbb{Z} \setminus \{0\}$ .

Dieses Paar hat den Grad 4. Verzweigt ist es über den Stellen 0, 1 und  $\infty$  mit folgenden Verzweigungsordnungen:

$$\begin{aligned} \beta_{C_2}^*(0) &= 4 \cdot (0, 0) \\ \beta_{C_2}^*(1) &= 2 \cdot (\sqrt{-A}, 0) + 2 \cdot (-\sqrt{-A}, 0) \\ \beta_{C_2}^*(\infty) &= 4 \cdot \infty. \end{aligned} \quad (4.24)$$

Das Dessin besteht also aus vier Kanten, drei Ecken, von denen zwei die Valenz zwei haben und eine die Valenz vier, sowie einer Fläche. Es gibt nur ein Dessin, das diese Bedingungen erfüllt; es ist in Abbildung 12 zu sehen.

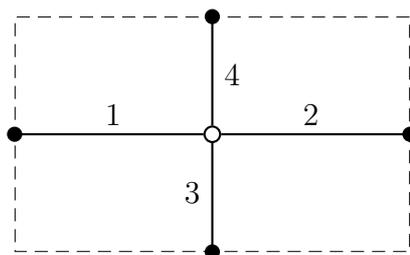


Abbildung 12: Dessin zu  $(C_2, \beta_{C_2})$

Als Permutationen ergeben sich

$$\begin{aligned} \sigma_0 &= (12)(34), \\ \sigma_1 &= (1324) \quad \text{und} \\ \sigma_\infty &= (1324). \end{aligned} \quad (4.25)$$

Diese Permutationen erzeugen die Gruppe  $S_4$ . Als Stabilisator wird jener zur Kante 4 gewählt.

Nun müssen noch die Spitzen und Spitzenbreiten berechnet werden. Die Menge  $\{0, 1, 2, \infty\}$  stellt ein Repräsentantensystem für die Spitzen da. Für die Breiten gilt:

Spitze	0	1	2	$\infty$
Breite	4	8	4	8

Die Ergebnisse, die der Algorithmus 3 mit Implementierung A.2 für diese Gruppe liefert, sind in Tabelle 5 auf Seite 61 zu sehen.

Tabelle 5: Die Koeffizienten zum Belyi-Paar  $(C_2, \beta_{C_2})$

$c$	$\phi(c)$	$r_{\infty\infty}^{C_2}(c)$	$r_{\infty 0}^{C_2}(c)$	$r_{\infty 1}^{C_2}(c)$	$r_{\infty 2}^{C_2}(c)$	$r_{00}^{C_2}(c)$	$r_{01}^{C_2}(c)$	$r_{02}^{C_2}(c)$	$r_{11}^{C_2}(c)$	$r_{12}^{C_2}(c)$	$r_{22}^{C_2}(c)$
1	1	0	2	4	2	0	2	0	0	2	0
2	1	8	0	0	0	0	0	4	8	0	0
3	2	0	4	8	4	0	4	0	0	4	0
4	2	16	0	0	0	8	0	0	16	0	8
5	4	0	8	16	8	0	8	0	0	8	0
6	2	16	0	0	0	0	0	8	16	0	0
7	6	0	12	24	12	0	12	0	0	12	0
8	4	32	0	0	0	16	0	0	32	0	16
9	6	0	12	24	12	0	12	0	0	12	0
10	4	32	0	0	0	0	0	16	32	0	0
11	10	0	20	40	20	0	20	0	0	20	0
12	4	32	0	0	0	16	0	0	32	0	16
13	12	0	24	48	24	0	24	0	0	24	0
14	6	48	0	0	0	0	0	24	48	0	0
15	8	0	16	32	16	0	16	0	0	16	0
16	8	64	0	0	0	32	0	0	64	0	32
17	16	0	32	64	32	0	32	0	0	32	0
18	6	48	0	0	0	0	0	24	48	0	0
19	18	0	36	72	36	0	36	0	0	36	0
20	8	64	0	0	0	32	0	0	64	0	32
21	12	0	24	48	24	0	24	0	0	24	0
22	10	80	0	0	0	0	0	40	80	0	0
23	22	0	44	88	44	0	44	0	0	44	0
24	8	64	0	0	0	32	0	0	64	0	32

4.7 Weitere Beispiele

Tabelle 5: Die Koeffizienten zum Belyi-Paar  $(C_2, \beta_{C_2})$ 

$c$	$\phi(c)$	$r_{\infty\infty}^{C_2}(c)$	$r_{\infty 0}^{C_2}(c)$	$r_{\infty 1}^{C_2}(c)$	$r_{\infty 2}^{C_2}(c)$	$r_{00}^{C_2}(c)$	$r_{01}^{C_2}(c)$	$r_{02}^{C_2}(c)$	$r_{11}^{C_2}(c)$	$r_{12}^{C_2}(c)$	$r_{22}^{C_2}(c)$
25	20	0	40	80	40	0	40	0	0	40	0
26	12	96	0	0	0	0	0	48	96	0	0
27	18	0	36	72	36	0	36	0	0	36	0
28	12	96	0	0	0	48	0	0	96	0	48
29	28	0	56	112	56	0	56	0	0	56	0
30	8	64	0	0	0	0	0	32	64	0	0
31	30	0	60	120	60	0	60	0	0	60	0
32	16	128	0	0	0	64	0	0	128	0	64
33	20	0	40	80	40	0	40	0	0	40	0
34	16	128	0	0	0	0	0	64	128	0	0
35	24	0	48	96	48	0	48	0	0	48	0
36	12	96	0	0	0	48	0	0	96	0	48
37	36	0	72	144	72	0	72	0	0	72	0
38	18	144	0	0	0	0	0	72	144	0	0
39	24	0	48	96	48	0	48	0	0	48	0
40	16	128	0	0	0	64	0	0	128	0	64
41	40	0	80	160	80	0	80	0	0	80	0
42	12	96	0	0	0	0	0	48	96	0	0
43	42	0	84	168	84	0	84	0	0	84	0
44	20	160	0	0	0	80	0	0	160	0	80
45	24	0	48	96	48	0	48	0	0	48	0
46	22	176	0	0	0	0	0	88	176	0	0
47	46	0	92	184	92	0	92	0	0	92	0
48	16	128	0	0	0	64	0	0	128	0	64

Das letzte Beispiel hat eine etwas andere Form. Das Belyi-Paar, zu dem die Gruppe assoziiert ist, ist nicht bekannt. Als Ausgangspunkt ist eine Permutationsgruppe gewählt. Auf diese Art und Weise lassen sich einige Eigenschaften der Gruppe leichter manipulieren.

**Beispiel 4.21.** *Betrachte die Gruppe  $G := \langle (1234567), (1234586) \rangle \subset S_8$  und den Morphismus*

$$\begin{aligned} \varphi_G : \Gamma(2) &\longrightarrow G \\ \gamma_0 &\longmapsto (1234567) \\ \gamma_1 &\longmapsto (1234586). \end{aligned}$$

*Damit sind*

$$\begin{aligned} \sigma_0 &= (1234567) \\ \sigma_1 &= (1234586) \quad \text{und} \\ \sigma_\infty &= \sigma_1^{-1}\sigma_0^{-1} = (17853)(264). \end{aligned}$$

*Als Stabilisator wird jener zum Element 8 gewählt, d.h.  $\Gamma_G = \varphi^{-1}(\text{Stab}_G(8))$ . Ein Repräsentantensystem der Spitzen mit Spitzenbreiten ist:*

<i>Spitze</i>	0	1	2	3	$\frac{3}{2}$	$\infty$
<i>Breite</i>	2	14	14	2	6	10

*Mit diesen Informationen kann der Algorithmus 3 von Seite 54 benutzt werden. Hier muss das Programm aus A.2 etwas stärker verändert werden, da es eine Spitze gibt, in deren Äquivalenzklasse keine ganze Zahl und auch nicht  $\infty$  liegt. Die Ergebnisse, welche das Programm für diese Gruppe liefert, sind in Tabelle 6 auf Seite 64 zu sehen, wobei aus Platzgründen  $a = \frac{3}{2}$  gesetzt wurde.*

**Bemerkung 4.22.** *Die gewählte Gruppe entspricht einem Belyi-Paar mit einem Morphismus vom Grad 8, bei dem über jeder Verzweigungsstelle zwei Punkte liegen, d.h. über jeder Spitze von  $\Gamma(2)$  liegen zwei Spitzen. Aufgrund der Anzahl der Spitzen und der Verzweigungsordnungen lässt sich ablesen, dass die algebraische Kurve des Belyi-Paares Geschlecht 2 hat.*

Tabelle 6: Die Koeffizienten zur Permutationsgruppe  $G$ 

$c$	$\phi(c)$	$r_{\infty\infty}^G$	$r_{\infty 0}^G$	$r_{\infty 1}^G$	$r_{\infty 2}^G$	$r_{\infty 3}^G$	$r_{\infty a}^G$	$r_{00}^G$	$r_{01}^G$	$r_{02}^G$	$r_{03}^G$	$r_{0a}^G$	$r_{11}^G$	$r_{12}^G$	$r_{13}^G$	$r_{1a}^G$	$r_{22}^G$	$r_{23}^G$	$r_{2a}^G$	$r_{33}^G$	$r_{3a}^G$	$r_{aa}^G$
1	1	0	1	4	4	1	0	0	1	0	0	0	0	6	0	3	0	1	3	0	0	0
2	1	4	0	0	0	0	6	0	0	2	0	0	12	0	2	0	12	0	0	0	0	0
3	2	0	0	10	10	0	0	0	1	0	1	2	0	13	0	4	0	1	4	0	2	0
4	2	16	0	0	0	0	4	0	0	4	0	0	24	0	4	0	24	0	0	0	0	8
5	4	0	3	17	17	3	0	0	4	0	0	1	0	24	0	11	0	4	11	0	1	0
6	2	12	0	0	0	0	8	0	0	4	0	0	24	0	4	0	24	0	0	0	0	4
7	6	0	3	27	27	3	0	0	5	0	1	3	0	37	0	15	0	5	15	0	3	0
8	4	26	0	0	0	0	14	0	0	8	0	0	48	0	8	0	48	0	0	0	0	10
9	6	0	3	27	27	3	0	0	4	0	2	3	0	38	0	15	0	4	15	0	3	0
10	4	24	0	0	0	0	16	2	0	6	0	0	50	0	6	0	50	0	0	2	0	8
11	10	0	5	45	45	5	0	0	10	0	0	5	0	60	0	25	0	10	25	0	5	0
12	4	24	0	0	0	0	16	2	0	6	0	0	50	0	6	0	50	0	0	2	0	8
13	12	0	9	51	51	9	0	0	11	0	1	3	0	73	0	33	0	11	33	0	3	0
14	6	40	0	0	0	0	20	4	0	8	0	0	76	0	8	0	76	0	0	4	0	16
15	8	0	5	35	35	5	0	0	8	0	0	3	0	48	0	21	0	8	21	0	3	0
16	8	50	0	0	0	0	30	0	0	16	0	0	96	0	16	0	96	0	0	0	0	18
17	16	0	9	71	71	9	0	0	15	0	1	7	0	97	0	41	0	15	41	0	7	0
18	6	40	0	0	0	0	20	2	0	10	0	0	74	0	10	0	74	0	0	2	0	16
19	18	0	13	77	77	13	0	0	16	0	2	5	0	110	0	49	0	16	49	0	5	0
20	8	44	0	0	0	0	36	2	0	14	0	0	98	0	14	0	98	0	0	2	0	12
21	12	0	8	52	52	8	0	0	9	0	3	4	0	75	0	32	0	9	32	0	4	0
22	10	52	0	0	0	0	48	0	0	20	0	0	120	0	20	0	120	0	0	0	0	12
23	22	0	14	96	96	14	0	0	21	0	1	8	0	133	0	58	0	21	58	0	8	0
24	8	64	0	0	0	0	16	2	0	14	0	0	98	0	14	0	98	0	0	2	0	32
25	20	0	8	92	92	8	0	0	16	0	4	12	0	124	0	48	0	16	48	0	12	0
26	12	68	0	0	0	0	52	2	0	22	0	0	146	0	22	0	146	0	0	2	0	20
27	18	0	10	80	80	10	0	0	17	0	1	8	0	109	0	46	0	17	46	0	8	0
28	12	84	0	0	0	0	36	4	0	20	0	0	148	0	20	0	148	0	0	4	0	36

## 5 Eigenschaften der berechneten Streumatrizen

Nun steht eine ganze Reihe von Beispielen zu Verfügung. An dieser Stelle sollen auffällige Ähnlichkeiten der Ergebnisse zusammengetragen werden und teilweise auch erklärt werden.

Die Streumatrix zu einer Gruppe  $\Gamma \subset \Gamma(1)$  ist durch die konstanten Koeffizienten  $\varphi_{jk}$  der Eisensteinreihen gegeben, vergleiche dazu Definition 4.7. Die  $\varphi_{jk}$  nun wieder werden allein durch die Funktionen  $r_{jk}^\Gamma$  definiert (siehe Satz 4.2). Im Folgenden wird deshalb fast ausschließlich  $r_{jk}(c)$  betrachtet.

### 5.1 Jeder zweite Koeffizient ist null

Bei allen Ergebnissen fällt auf, dass jeder zweite Koeffizient null ist. In Satz 5.2 wird diese Eigenschaft für Gruppen  $\Gamma \subset \Gamma(2)$  bewiesen.

Hierzu müssen erst einmal die Äquivalenzklassen von  $\mathbb{Q} \cup \infty$  unter der Wirkung von  $\Gamma(2)$  genauer betrachtet werden.

**Lemma 5.1.** *Die Äquivalenzklassen von  $\mathbb{Q} \cup \infty$  unter der Wirkung von  $\Gamma(2)$  sind:*

$$\begin{aligned} S_\infty &= \left\{ \frac{s}{t} \in \mathbb{Q} \mid (s, t) = 1, t \equiv 0 \pmod{2} \right\} \cup \infty \\ S_0 &= \left\{ \frac{s}{t} \in \mathbb{Q} \mid (s, t) = 1, s \equiv 0 \pmod{2} \right\} \\ S_1 &= \left\{ \frac{s}{t} \in \mathbb{Q} \mid (s, t) = 1, s \equiv 1 \pmod{2} \text{ und } t \equiv 1 \pmod{2} \right\} \end{aligned}$$

*Beweis:* Aus Lemma 1.26 ist bekannt, dass  $\Gamma(2)$  drei Spitzen hat und die Menge  $\{\infty, 0, 1\}$  ein Repräsentantensystem bildet.

Betrachte nun eine Matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$  und ihre Wirkung auf einen ausgekürzten Bruch  $\frac{s}{t}$ :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \frac{as + bt}{cs + dt}$$

Im weiteren wird erläutert, welche Gestalt ein Bruch  $\frac{s}{t}$  haben muss, um äquivalent zu 0, 1 oder  $\infty$  zu sein.

**Zu  $\infty$ :** Damit  $\frac{s}{t} \sim_{\Gamma(2)} \infty$ , muss  $\frac{as+bt}{cs+dt} = \infty$  gelten:

$$\begin{aligned} \frac{as + bt}{cs + dt} = \infty &\Rightarrow cs + dt = 0 \\ &\Rightarrow cs = -dt \\ &\Rightarrow s \equiv 1 \pmod{2} \quad \text{und} \quad t \equiv 0 \pmod{2} \end{aligned}$$

## 5 Eigenschaften der berechneten Streumatrizen

Die letzte Folgerung gilt, da  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ .

Analog folgt:

**Zu 0:** Damit  $\frac{s}{t} \sim_{\Gamma(2)} 0$ , muss  $\frac{as+bt}{cs+dt} = 0$  gelten:

$$\begin{aligned} \frac{as+bt}{cs+dt} = 0 &\Rightarrow as+bt = 0 \\ &\Rightarrow as = -bt \\ &\Rightarrow s \equiv 0 \pmod{2} \quad \text{und} \quad t \equiv 1 \pmod{2} \end{aligned}$$

**Zu 1:** Damit  $\frac{s}{t} \sim_{\Gamma(2)} 1$ , muss  $\frac{as+bt}{cs+dt} = 1$  gelten:

$$\begin{aligned} \frac{as+bt}{cs+dt} = 1 &\Rightarrow s(a-c) = t(d-b) \\ &\Rightarrow s = d-b \quad \text{und} \quad t = a-c \\ &\Rightarrow s \equiv 1 \pmod{2} \quad \text{und} \quad t \equiv 1 \pmod{2} \end{aligned}$$

Aus diesen Betrachtungen folgt auch schon die Behauptung, denn jeder Bruch erfüllt nur genau eine der drei Bedingungen und jeder Bruch muss zu einer der drei Spitzen äquivalent sein.  $\square$

**Satz 5.2.** Sei  $\Gamma \subset \Gamma(2)$  eine Untergruppe von endlichem Index und  $S = \{S_1, \dots, S_r\}$  ein Repräsentantensystem für die Spitzen von  $\Gamma$ . Dann gilt zu je zwei Spitzen  $S_j, S_k \in S$ :

$$\begin{aligned} \text{Wenn } S_j \sim_{\Gamma(2)} S_k &\Rightarrow r_{jk}(c) = 0, \text{ für } c \in \mathbb{N} \text{ mit } c \equiv 1 \pmod{2}. \\ \text{Wenn } S_j \not\sim_{\Gamma(2)} S_k &\Rightarrow r_{jk}(c) = 0, \text{ für } c \in \mathbb{N} \text{ mit } c \equiv 0 \pmod{2}. \end{aligned} \quad (5.1)$$

*Beweis:* Um diesen Satz zu beweisen, muss die Struktur der Menge  $\gamma_j^{-1}\Gamma\gamma_k$ , welche die  $r$ 's bestimmt, genauer verstanden werden. Das  $c$  in  $r_{jk}(c)$  steht für den Eintrag unten links in den Matrizen aus  $\gamma_j^{-1}\Gamma\gamma_k$ . Betrachte die Projektion

$$\pi : \Gamma(1) \longrightarrow \Gamma(1)/\Gamma(2)$$

und das Bild von  $\gamma_j^{-1}\Gamma\gamma_k$  unter  $\pi$ :

$$\pi(\gamma_j^{-1}\Gamma\gamma_k) = \pi(\gamma_j^{-1})\pi(\Gamma)\pi(\gamma_k) = \pi(\gamma_j^{-1})\text{Id}\pi(\gamma_k) = \pi(\gamma_j^{-1}\gamma_k). \quad (5.2)$$

Ob die Einträge unten links in den Matrizen aus  $\gamma_j^{-1}\Gamma\gamma_k$  gerade oder ungerade sind, hängt also nur von den Spitzen  $S_j$  und  $S_k$  ab.

Für eine Spitze  $S_j$  hat  $\gamma_j$  die Eigenschaft:  $\gamma_j(\infty) = S_j$ . Sei  $S_j = \frac{s}{t}$  ein Bruch, so gilt  $\gamma_j = \begin{pmatrix} s & * \\ t & * \end{pmatrix}$ . Mit  $S_k = \frac{r}{v}$  ist also

$$\gamma_j^{-1}\gamma_k = \begin{pmatrix} * & * \\ -t & s \end{pmatrix} \begin{pmatrix} r & * \\ v & * \end{pmatrix} = \begin{pmatrix} sv & * \\ sv - rt & * \end{pmatrix}.$$

Mit Lemma 5.1 und der Formel (5.2) folgt, dass es in der Menge  $\gamma_j^{-1}\Gamma\gamma_k$ , wenn die Spitzen äquivalent sind, nur Einträge zu geradem  $c$  gibt und, wenn die Spitzen nicht äquivalent sind, nur Einträge zu ungeradem  $c$  gibt.  $\square$

## 5.2 Gleiche Koeffizienten

In allen vier Beispielen kommen Koeffizienten mehrfach vor:

Sei  $\Gamma \subset \Gamma(1)$  eine Gruppe mit Spitzen  $S_j$  und  $S_k$ . Dann ist  $r_{jk}^\Gamma$  eine Abbildung, die einer natürlichen Zahl  $c$  den entsprechenden Koeffizienten des Elements zu  $(S_j, S_k)$  in der Streumatrix zuordnet:

$$\begin{aligned} r_{jk}^\Gamma : \mathbb{N} &\longrightarrow \mathbb{N} \\ c &\longmapsto r_{jk}^\Gamma(c) \end{aligned}$$

### Das Paar $(E, \beta)$

Zu diesem Paar, siehe Formeln (3.5) für das Paar und (3.9) für die Gruppe, legt Tabelle 3 von Seite 56 eine Reihe von Symmetrien nah:

**Frage 5.3.** *Gelten für das Paar  $(E, \beta)$  die Identitäten:*

$$\begin{aligned} r_{\infty 0}^{\Gamma_E} &= r_{\infty 3}^{\Gamma_E} \\ r_{\infty 1}^{\Gamma_E} &= r_{\infty 6}^{\Gamma_E} \\ r_{06}^{\Gamma_E} &= r_{13}^{\Gamma_E} \\ r_{01}^{\Gamma_E} &= r_{36}^{\Gamma_E} \\ r_{00}^{\Gamma_E} &= r_{33}^{\Gamma_E} \\ r_{11}^{\Gamma_E} &= r_{66}^{\Gamma_E} \end{aligned}$$

Die einzigen  $r^{\Gamma_E}$ 's, die nicht doppelt vorkommen, sind  $r_{\infty\infty}^{\Gamma_E}$ ,  $r_{03}^{\Gamma_E}$ ,  $r_{16}^{\Gamma_E}$ .

**Bemerkung 5.4.** *Mit Hilfe des Algorithmus 3 von Seite 54 wurde berechnet, dass die Funktionswerte der Funktionen aus Frage 5.3 bis  $c = 500$  gleich sind. Bis zu dieser Höhe wurden die Koeffizienten berechnet.*

### Die Gruppe $\Gamma(2)$

In Kapitel 4.2 wurde bewiesen:

## 5 Eigenschaften der berechneten Streumatrizen

**Satz 5.5.** *Für die Gruppe  $\Gamma(2)$  gelten die Identitäten:*

$$\begin{aligned} r_{\infty\infty}^{\Gamma(2)} &= r_{00}^{\Gamma(2)} = r_{11}^{\Gamma(2)} \\ r_{\infty 0}^{\Gamma(2)} &= r_{\infty 1}^{\Gamma(2)} = r_{01}^{\Gamma(2)} \end{aligned}$$

*Damit tauchen nur zwei verschiedene Koeffizientenfunktionen auf, diese aber mehrfach.*

*Beweis:* Der Satz folgt aus Satz 4.12 auf Seite 45. □

**Das Paar  $(C_1, \beta_{C_1})$**

Zu diesem Paar, siehe Formel (4.22), legt die Tabelle 4 von Seite 59 eine Reihe von Symmetrien nah:

**Frage 5.6.** *Gelten für das Paar  $(C_1, \beta_{C_1})$  folgende Identitäten:*

$$\begin{aligned} r_{\infty\infty}^{C_1} &= r_{00}^{C_1} = r_{11}^{C_1} \\ r_{\infty 0}^{C_1} &= r_{\infty 1}^{C_1} = r_{01}^{C_1} \end{aligned}$$

*Damit tauchen nur zwei verschiedene Koeffizientenfunktionen auf, diese aber mehrfach.*

**Bemerkung 5.7.** *Mit Hilfe des Algorithmus 3 von Seite 54 wurde berechnet, dass die Funktionswerte der Funktionen aus Frage 5.6 bis  $c = 100$  gleich sind. Bis zu dieser Höhe wurden die Koeffizienten berechnet.*

**Das Paar  $(C_2, \beta_{C_2})$**

Zu diesem Paar, siehe Formel (4.23), legt die Tabelle 5 von Seite 61 eine Reihe von Symmetrien nah:

**Frage 5.8.** *Gelten für das Paar  $(C_2, \beta_{C_2})$  die Identitäten:*

$$\begin{aligned} r_{\infty\infty}^{C_2} &= r_{11}^{C_2} \\ r_{\infty 0}^{C_2} &= r_{\infty 2}^{C_2} = r_{01}^{C_2} = r_{12}^{C_2} \\ r_{00}^{C_2} &= r_{22}^{C_2} \end{aligned}$$

Die einzigen  $r^{\Gamma_E}$ 's, die nicht doppelt vorkommen, sind  $r_{\infty 1}^{C_2}$  und  $r_{02}^{C_2}$ .

**Bemerkung 5.9.** *Mit Hilfe des Algorithmus 3 von Seite 54 wurde berechnet, dass die Funktionswerte der Funktionen aus Frage 5.8 bis  $c = 100$  gleich sind. Bis zu dieser Höhe wurden die Koeffizienten berechnet.*

## Die Permutationsgruppe $G$

Zu dieser Gruppe, siehe Beispiel 4.21, legt die Tabelle 6 von Seite 64 eine Reihe von Symmetrien nah:

**Frage 5.10.** *Gelten für die Permutationsgruppe  $G$  folgende Identitäten:*

$$\begin{aligned} r_{\infty 0}^G &= r_{\infty 3}^G \\ r_{\infty 1}^G &= r_{\infty 2}^G \\ r_{00}^G &= r_{33}^G \\ r_{01}^G &= r_{23}^G \\ r_{02}^G &= r_{13}^G \\ r_{0a}^G &= r_{3a}^G \\ r_{1a}^G &= r_{2a}^G \end{aligned}$$

Die einzigen  $r^{\Gamma_E}$ 's, die nicht doppelt vorkommen, sind  $r_{\infty\infty}^G$ ,  $r_{\infty a}^G$ ,  $r_{03}^G$ ,  $r_{11}^G$ ,  $r_{12}^G$ ,  $r_{1a}^G$ ,  $r_{22}^G$  und  $r_{aa}^G$ .

**Bemerkung 5.11.** *Mit Hilfe des Algorithmus 3 von Seite 54 wurde berechnet, dass die Funktionswerte der Funktionen aus Frage 5.10 bis  $c = 100$  gleich sind. Bis zu dieser Höhe wurden die Koeffizienten berechnet.*

Es sind nur Koeffizienten zu einem Paar von Spitzen  $(S_j, S_k)$  gleich jenen zu  $(S_{j'}, S_{k'})$ , wenn die Mengen  $\{b_j, b_k\}$  und  $\{b_{j'}, b_{k'}\}$  gleich sind. Natürlich muss die Bedingung, die der Satz 5.2 an die Spitzen stellt, damit die Koeffizienten gleich sein können, erfüllt sein. Es fällt auf, dass unter diesen Voraussetzungen die Koeffizienten gleich sind.

Dieses Phänomen lässt sich zu einer allgemeineren Vermutung zusammenfassen:

**Vermutung 5.12.** *Sei  $\Gamma \subset \Gamma(2)$  eine Untergruppe von endlichem Index und  $S = \{S_1, \dots, S_n\}$  ein Repräsentantensystem der Spitzen zu  $\Gamma$ , wobei  $n \in \mathbb{N}$ , dann gilt: Seien  $(S_j, S_k)$  und  $(S_{j'}, S_{k'})$  zwei Paare von Spitzen aus  $S$  mit Spitzenbreiten  $b_j$  und  $b_k$ , respektive  $b_{j'}$  und  $b_{k'}$ , so dass gilt  $b_j = b_{j'}$  und  $b_k = b_{k'}$ , dann:*

$$\text{Wenn } S_j \sim_{\Gamma(2)} S_k \text{ und } S_{j'} \sim_{\Gamma(2)} S_{k'} \implies r_{jk}(c) = r_{j'k'}(c) \quad \forall c \in \mathbb{N}.$$

$$\text{Wenn } S_j \not\sim_{\Gamma(2)} S_k \text{ und } S_{j'} \not\sim_{\Gamma(2)} S_{k'} \implies r_{jk}(c) = r_{j'k'}(c) \quad \forall c \in \mathbb{N}.$$

**Bemerkung 5.13.** *Aufgrund der Symmetrie  $r_{jk}(c) = r_{kj}(c)$  für alle  $c \in \mathbb{N}$  gelten die Folgerungen aus Vermutung 5.12 auch für  $b_j = b_{k'}$  und  $b_k = b_{j'}$ .*

### Antworten auf die Fragen

Wenn die Vermutung 5.12 gilt, sind die Fragen 5.3, 5.6, 5.8 und 5.10 positiv zu beantworten.

Die Vermutung 5.12 wurde an allen hier berechneten Beispielen getestet. Für  $\Gamma(2)$  gilt sie allgemein. Für das Paar  $(E, \beta)$  ist sie bis  $c = 500$  verifiziert; bei den anderen Beispielen bis  $c = 100$ .

Einige der Identitäten der Koeffizientenfunktionen folgen aus den Sätzen in Unterkapitel 5.6 über total verzweigte Spitzen. Bezüglich Frage 5.3 folgen die ersten beiden Identitäten aus Satz 5.32. Die Frage 5.6 ist vollständig positiv zu beantworten, wie Satz 5.34 zeigt. Auch die Frage 5.8 ist weitgehend positiv zu beantworten, denn alle Identitäten bis auf die letzte folgen aus Satz 5.35. Da die Gruppe  $G$  keine total verzweigten Spitzen hat, lassen sich keine der Identitäten aus Frage 5.10 mit Hilfe von Kapitel 5.6 beantworten.

### 5.3 Lineare Abhängigkeiten

In allen Beispielen sind einige Spalten gleich, wie schon in Kapitel 5.2 dargestellt worden ist. Es lassen sich noch weitere lineare Abhängigkeiten finden.

#### Das Paar $(E, \beta)$

Neben den in Frage 5.3 angesprochenen Gleichheiten, legen die Listen noch weitere Abhängigkeiten nah. Insgesamt ergibt sich:

**Vermutung 5.14.** *Folgende lineare Relationen bestehen:*

$$\begin{array}{ll}
 r_{\infty\infty}^{\Gamma_E} & r_{06}^{\Gamma_E} \\
 r_{\infty 0}^{\Gamma_E} & r_{11}^{\Gamma_E} = r_{\infty\infty}^{\Gamma_E} - r_{00}^{\Gamma_E} - 2r_{06}^{\Gamma_E} \\
 r_{\infty 1}^{\Gamma_E} = \frac{1}{4}r_{\infty 0}^{\Gamma_E} & r_{13}^{\Gamma_E} = r_{06}^{\Gamma_E} \\
 r_{\infty 3}^{\Gamma_E} = r_{\infty 0}^{\Gamma_E} & r_{16}^{\Gamma_E} = \frac{1}{4}r_{\infty 0}^{\Gamma_E} - r_{01}^{\Gamma_E} \\
 r_{\infty 6}^{\Gamma_E} = \frac{1}{4}r_{\infty 0}^{\Gamma_E} & r_{33}^{\Gamma_E} = r_{00}^{\Gamma_E} \\
 r_{00}^{\Gamma_E} & r_{36}^{\Gamma_E} = r_{01}^{\Gamma_E} \\
 r_{01}^{\Gamma_E} & r_{66}^{\Gamma_E} = r_{\infty\infty}^{\Gamma_E} - r_{00}^{\Gamma_E} - 2r_{06}^{\Gamma_E} \\
 r_{03}^{\Gamma_E} = r_{\infty 0}^{\Gamma_E} - r_{01}^{\Gamma_E} &
 \end{array}$$

*Es gibt insgesamt 5 linear unabhängige Funktionen:  $r_{\infty\infty}^{\Gamma_E}$ ,  $r_{\infty 0}^{\Gamma_E}$ ,  $r_{00}^{\Gamma_E}$ ,  $r_{01}^{\Gamma_E}$  und  $r_{06}^{\Gamma_E}$ .*

**Die Gruppe  $\Gamma(2)$** 

Wie schon im Satz 4.12 bewiesen gibt es nur zwei verschiedene Ergebnisse. Die beiden sind linear unabhängig von einander.

**Das Paar  $(C_1, \beta_{C_1})$** 

Da die Frage 5.6 positiv zu beantworten ist, gibt es nur zwei verschiedene Ergebnisse. Die beiden sind linear unabhängig von einander.

**Das Paar  $(C_2, \beta_{C_2})$** 

Neben den in Frage 5.8 angesprochenen Gleichheiten, legen die Listen noch weitere Abhängigkeiten nah. Insgesamt ergibt sich:

**Vermutung 5.15.** *Folgende lineare Relationen bestehen:*

$$\begin{array}{ll}
 r_{\infty\infty}^{C_2} & r_{01}^{C_2} = r_{\infty 0}^{C_2} \\
 r_{\infty 0}^{C_2} & r_{02}^{C_2} = \frac{1}{2}r_{\infty\infty}^{C_2} - r_{00}^{C_2} \\
 r_{\infty 1}^{C_2} = 2r_{\infty 0}^{C_2} & r_{11}^{C_2} = r_{\infty\infty}^{C_2} \\
 r_{\infty 2}^{C_2} = r_{\infty 0}^{C_2} & r_{12}^{C_2} = r_{\infty 0}^{C_2} \\
 r_{00}^{C_2} & r_{22}^{C_2} = r_{00}^{C_2}
 \end{array}$$

*Es gibt insgesamt 3 linear unabhängige Funktionen:  $r_{\infty\infty}^{C_2}$ ,  $r_{\infty 0}^{C_2}$  und  $r_{00}^{C_2}$ .*

**Die Permutationsgruppe  $G$** 

Neben den in Frage 5.8 angesprochenen Gleichheiten, legen die Listen noch weitere Abhängigkeiten nah. Insgesamt ergibt sich:

## 5 Eigenschaften der berechneten Streumatrizen

**Vermutung 5.16.** *Folgende lineare Relationen bestehen, wobei  $a = \frac{3}{2}$  ist:*

$$\begin{array}{ll}
 r_{\infty\infty}^G & r_{11}^G = \frac{6}{5}(r_{\infty\infty}^G + r_{\infty a}^G) + r_{00}^G \\
 r_{\infty 0}^G & r_{12}^G = \frac{7}{5}(r_{\infty 0}^G + r_{\infty 1}^G) - r_{01}^G \\
 r_{\infty 1}^G & r_{13}^G = r_{02}^G \\
 r_{\infty 2}^G = r_{\infty 1}^G & r_{1a}^G = \frac{7}{5}r_{\infty 0}^G + \frac{2}{5}r_{\infty 1}^G \\
 r_{\infty 3}^G = r_{\infty 0}^G & r_{22}^G = \frac{6}{5}(r_{\infty\infty}^G + r_{\infty a}^G) - r_{00}^G \\
 r_{\infty a}^G & r_{23}^G = r_{01}^G \\
 r_{00}^G & r_{2a}^G = r_{1a}^G \\
 r_{01}^G & r_{33}^G = r_{00}^G \\
 r_{02}^G = \frac{1}{5}(r_{\infty\infty}^G + r_{\infty a}^G) - r_{00}^G & r_{3a}^G = r_{0a}^G \\
 r_{03}^G = \frac{1}{5}(r_{\infty 0}^G + r_{\infty 1}^G) - r_{01}^G & r_{aa}^G = \frac{3}{5}r_{\infty\infty}^G - \frac{2}{5}r_{\infty a}^G \\
 r_{0a}^G = -\frac{4}{5}r_{\infty 0}^G + \frac{1}{5}r_{\infty 1}^G &
 \end{array}$$

*Es gibt insgesamt 6 linear unabhängige Funktionen*

$r_{\infty\infty}^G, r_{\infty 0}^G, r_{\infty 1}^G, r_{\infty 3/2}^G, r_{00}^G$  und  $r_{01}^G$ .

**Feststellung:** Die Dimension des Raumes, der von den  $r_{jk}^\Gamma$  zu einer Gruppe  $\Gamma$  aufgespannt wird, ist in den behandelten Beispielen immer kleiner gleich der Anzahl der Spitzen.

Naheliegender ist es zu folgende Frage zu formulieren:

**Frage 5.17.** *Gilt allgemein, dass die Dimension des Raumes, der von den  $r_{jk}^\Gamma$  zu einer Gruppe  $\Gamma$  aufgespannt wird kleiner gleich der Anzahl der Spitzen ist?*

**Bemerkung 5.18.** *Ein beachtlicher Teil der linearen Abhängigkeiten aus diesem Kapitel folgt aus Satz 5.24 von Seite 78.*

## Matrizen

Nun werden die ersten Koeffizienten für das Belyi-Paar  $(E, \beta)$  aus Formel 3.7 in Matrizen dargestellt, um Regelmäßigkeiten und lineare Abhängigkeiten zu

### 5.3 Lineare Abhängigkeiten

finden. Zu jeder natürlichen Zahl  $c$  lässt sich eine Matrix wie folgt definieren:

$$\begin{pmatrix} r_{\infty\infty}(c) & r_{\infty 0}(c) & r_{\infty 1}(c) & r_{\infty 3}(c) & r_{\infty 6}(c) \\ r_{\infty 0}(c) & r_{00}(c) & r_{01}(c) & r_{03}(c) & r_{06}(c) \\ r_{\infty 1}(c) & r_{01}(c) & r_{11}(c) & r_{13}(c) & r_{16}(c) \\ r_{\infty 3}(c) & r_{03}(c) & r_{13}(c) & r_{33}(c) & r_{36}(c) \\ r_{\infty 6}(c) & r_{06}(c) & r_{16}(c) & r_{36}(c) & r_{66}(c) \end{pmatrix}$$

Da jeder zweite Koeffizient null ist, zeigen die Matrizen starke Regelmäßigkeiten und es tauchen nur die beiden Typen auf.

$$\text{Für gerades } c : \begin{pmatrix} * & 0 & 0 & 0 & 0 \\ 0 & * & 0 & 0 & * \\ 0 & 0 & * & * & 0 \\ 0 & 0 & * & * & 0 \\ 0 & * & 0 & 0 & * \end{pmatrix} \quad \text{Für ungerades } c : \begin{pmatrix} 0 & * & * & * & * \\ * & 0 & * & * & 0 \\ * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ * & 0 & * & * & 0 \end{pmatrix}$$

Die ersten 12 Matrizen, die sich ergeben, sind:

$c = 1 :$

$$\begin{pmatrix} 0 & 4 & 1 & 4 & 1 \\ 4 & 0 & 1 & 3 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 4 & 3 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$c = 2 :$

$$\begin{pmatrix} 10 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 6 & 0 \\ 0 & 2 & 0 & 0 & 0 \end{pmatrix}$$

$c = 3 :$

$$\begin{pmatrix} 0 & 8 & 2 & 8 & 2 \\ 8 & 0 & 2 & 6 & 0 \\ 2 & 2 & 0 & 0 & 0 \\ 8 & 6 & 0 & 0 & 2 \\ 2 & 0 & 0 & 2 & 0 \end{pmatrix}$$

$c = 4 :$

$$\begin{pmatrix} 20 & 0 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 4 & 12 & 0 \\ 0 & 4 & 0 & 0 & 0 \end{pmatrix}$$

$c = 5 :$

$$\begin{pmatrix} 0 & 16 & 4 & 16 & 4 \\ 16 & 0 & 0 & 16 & 0 \\ 4 & 0 & 0 & 0 & 4 \\ 16 & 16 & 0 & 0 & 4 \\ 4 & 0 & 4 & 4 & 0 \end{pmatrix}$$

$c = 6 :$

$$\begin{pmatrix} 20 & 0 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 4 & 12 & 0 \\ 0 & 4 & 0 & 0 & 0 \end{pmatrix}$$

$c = 7 :$

$$\begin{pmatrix} 0 & 24 & 6 & 24 & 6 \\ 24 & 0 & 6 & 18 & 0 \\ 6 & 6 & 0 & 0 & 0 \\ 24 & 18 & 0 & 0 & 6 \\ 6 & 0 & 0 & 6 & 0 \end{pmatrix}$$

$c = 8 :$

$$\begin{pmatrix} 40 & 0 & 0 & 0 & 0 \\ 0 & 26 & 0 & 0 & 6 \\ 0 & 0 & 2 & 6 & 0 \\ 0 & 0 & 6 & 26 & 0 \\ 0 & 6 & 0 & 0 & 2 \end{pmatrix}$$

$c = 9 :$

$$\begin{pmatrix} 0 & 24 & 6 & 24 & 6 \\ 24 & 0 & 6 & 18 & 0 \\ 6 & 6 & 0 & 0 & 0 \\ 24 & 18 & 0 & 0 & 6 \\ 6 & 0 & 0 & 6 & 0 \end{pmatrix}$$

$c = 10 :$

$$\begin{pmatrix} 40 & 0 & 0 & 0 & 0 \\ 0 & 30 & 0 & 0 & 2 \\ 0 & 0 & 6 & 2 & 0 \\ 0 & 0 & 2 & 30 & 0 \\ 0 & 2 & 0 & 0 & 6 \end{pmatrix}$$

$c = 11 :$

$$\begin{pmatrix} 0 & 40 & 10 & 40 & 10 \\ 40 & 0 & 6 & 34 & 0 \\ 10 & 6 & 0 & 0 & 4 \\ 40 & 34 & 0 & 0 & 6 \\ 10 & 0 & 4 & 6 & 0 \end{pmatrix}$$

$c = 12 :$

$$\begin{pmatrix} 40 & 0 & 0 & 0 & 0 \\ 0 & 26 & 0 & 0 & 6 \\ 0 & 0 & 2 & 6 & 0 \\ 0 & 0 & 6 & 26 & 0 \\ 0 & 6 & 0 & 0 & 2 \end{pmatrix}$$

## 5 Eigenschaften der berechneten Streumatrizen

Alle diese Matrizen haben vollen Rang 5 (mit Maple getestet).

In den Beispielen zu  $\Gamma(2)$ ,  $C_1$  bzw.  $G$  haben die Matrizen vollen Rang 3 respektive 6. Zu  $C_2$  haben die Matrizen zu geradem  $c$  vollen Rang 4 und die zu ungeradem  $c$  haben Rang 3 (Tabelle 5 auf Seite 61 zeigt, dass für ungerades  $c$  in der zweiten und in der vierten Spalte genau die gleichen Werte stehen).

### 5.4 Die Summe der Koeffizientenfunktionen zu einer Spitze

Betrachtet man in den Tabellen die Summe der Koeffizientenfunktionen zu einer fixierten Spitze  $S_k$  so gilt in allen Beispielen:

$$\frac{1}{b_k} \sum_{S_j \in S} r_{jk}^\Gamma(c) = \phi(c) \quad \text{für alle } c. \quad (5.3)$$

Da die Euler'sche  $\phi$ -Funktion nach Beispiel 4.5 die Koeffizienten für die Gruppe  $\Gamma(1)$  beschreibt, lässt sich die Formel (5.3) umformulieren zu

$$\frac{1}{b_k} \sum_{S_j \in S} r_{jk}^\Gamma(c) = r^{\Gamma(1)}(c) \quad \text{für alle } c. \quad (5.4)$$

Dieses Ergebnis folgt aus einer allgemeinen Gleichung über die Beziehung zwischen der Eisensteinreihe für eine Gruppe  $\Gamma$  und Eisensteinreihen zu einer Untergruppe  $\Gamma' \subset \Gamma$ . Die Gleichung wird in Satz 5.20 bewiesen, doch dafür wird ein Lemma benötigt, welches vorangestellt wird.

**Lemma 5.19.** *Sei  $\Gamma \subset \Gamma(1)$  eine Untergruppe von endlichem Index und  $S_j$  eine Spitze von  $\Gamma$  mit Spitzenbreite  $b_j$ . Dann gilt für die Eisensteinreihe:*

$$E_{S_j}(z, s) = b_j^{-1} \sum_{-\frac{d}{c} \in S_j} \frac{\text{Im}(z)^s}{|cz - d|^{2s}} \quad (5.5)$$

*Beweis:* Die Eisensteinreihe zur Gruppe  $\Gamma$  mit Spitze  $S_j$  ist definiert als

$$E_{S_j}(z, s) = \sum_{\gamma \in \Gamma_j \setminus \Gamma} \text{Im}(\sigma_j^{-1} \gamma(z))^s.$$

Mit

$$\sigma_j = \gamma_j \begin{pmatrix} \sqrt{b_j} & 0 \\ 0 & 1/\sqrt{b_j} \end{pmatrix}$$

## 5.4 Die Summe der Koeffizientenfunktionen zu einer Spitze

gilt

$$\sum_{\gamma \in \Gamma_j \setminus \Gamma} \operatorname{Im}(\sigma_j^{-1} \gamma(z))^s = \sum_{\gamma \in \Gamma_j \setminus \Gamma} b_j^{-s} \operatorname{Im}(\gamma_j^{-1} \gamma(z))^s.$$

Sei  $\gamma_j^{-1} \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , so ist  $\operatorname{Im}(\gamma_j^{-1} \gamma(z)) = \frac{\operatorname{Im}(z)}{|cz-d|^2}$ . Außerdem gilt, dass das Paar  $(c, d)$  genau dann untere Zeile einer Matrix  $\gamma_j^{-1} \gamma$  mit  $\gamma \in \Gamma_j \setminus \Gamma$  ist, wenn  $-\frac{d}{c} \in S_j$  ist:

Sei  $\frac{s}{t} \in S_j$  ein Repräsentant für  $S_j$ , so kann  $\gamma_j^{-1} = \begin{pmatrix} * & * \\ -t & s \end{pmatrix}$  gewählt werden.

Einerseits: Für  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$  ist dann  $\gamma_j^{-1} \Gamma_j \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ sc-at & sd-bt \end{pmatrix}$  und mit  $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \frac{s}{t} = \frac{bt-sd}{sc-at}$ , wobei  $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \Gamma$ , ist  $\frac{bt-sd}{sc-at} \in S_j$ .

Andererseits: Sei  $-\frac{d}{c} \in S_j$ , so existiert  $\gamma \in \Gamma$  mit  $\gamma \begin{pmatrix} -q \\ p \end{pmatrix} = \frac{s}{t}$  und somit gilt  $\gamma_j^{-1} \gamma \begin{pmatrix} -q \\ p \end{pmatrix} = \infty$ , also  $\gamma_j^{-1} \gamma = \begin{pmatrix} * & * \\ p & q \end{pmatrix}$ .

Mit diesem Ergebnis folgt:

$$E_{S_j}(z, s) = b_j^{-s} \sum_{\gamma \in \Gamma_j \setminus \Gamma} \operatorname{Im}(\gamma_j^{-1} \gamma(z))^s = b_j^{-s} \sum_{-\frac{d}{c} \in S_j} \frac{\operatorname{Im}(z)^s}{|cz-d|^{2s}}.$$

□

**Satz 5.20.** *Seien die Gruppen  $\Gamma$  und  $\Gamma'$  Untergruppen von  $\Gamma(1)$  von endlichem Index mit  $\Gamma' \subset \Gamma \subset \Gamma(1)$ . Sei  $S_j$  eine Spitze von  $\Gamma$  mit Spitzenbreite  $b_j$ . So lässt sich diese Spitze unter der Wirkung von  $\Gamma'$  zerlegen und es gilt*

$$S = \bigcup_{i=1}^r S_{j_i},$$

wobei die  $\{S_{j_i}\}_{i=1, \dots, r}$  Spitzen von  $\Gamma'$  sind mit Spitzenbreiten  $b_{j_i}$ .

Für die Eisensteinreihen gilt:

$$\sum_{i=1}^r b_{j_i}^s E_{S_{j_i}}^{\Gamma'}(z, s) = b_j^s E_{S_j}^{\Gamma}(z, s) \quad (5.6)$$

*Beweis:* Mit Lemma 5.19 lässt sich schreiben

$$\begin{aligned} b_j^s E_{S_j}^{\Gamma}(z, s) &= \sum_{-\frac{d}{c} \in S_j} \frac{\operatorname{Im}(z)^s}{|cz-d|^{2s}} \\ &= \sum_{i=1}^r \sum_{-\frac{d}{c} \in S_{j_i}} \frac{\operatorname{Im}(z)^s}{|cz-d|^{2s}} \\ &= \sum_{i=1}^r b_{j_i}^s E_{S_{j_i}}^{\Gamma'}(z, s), \end{aligned}$$

## 5 Eigenschaften der berechneten Streumatrizen

wobei die erste und die letzte Gleichheit aus Lemma 5.19 folgt.  $\square$

Aus der Beziehung zwischen den Eisensteinreihen lässt sich eine Relation für die Koeffizientenfunktionen der Streumatrizen folgern.

**Satz 5.21.** *Gelten die Benennungen aus Satz 5.20. Seien außerdem  $S_k$  eine weitere Spitze von  $\Gamma$  und  $S_{k'}$  eine Spitze von  $\Gamma'$  mit  $S_{k'} \subset S_k$ . Die dazu gehörenden Spitzenbreiten seien  $b_k$  und  $b_{k'}$ .*

*Dann gilt für die Koeffizienten:*

$$\frac{1}{b_{k'}} \sum_{i=1}^r r_{j_i k'}^{\Gamma'}(c) = \frac{1}{b_k} r_{j k}^{\Gamma}(c) \quad \forall c \in \mathbb{N} \quad (5.7)$$

*Beweis:* An dieser Stelle werden Fourierentwicklungen von Eisensteinreihen zu unterschiedlichen Spitzen verglichen. Dabei muss beachtet werden, dass bei der Fourierentwicklung mit der Spitzenbreite der Spitze, in der entwickelt wird, skaliert wird. Für die Fourierentwicklungen der Eisensteinreihe zur Spitze  $S_j$  in der Spitze  $S_k$  gilt

$$E_{S_j}(z, s)|_{S_k} = E_{S_j}(\sigma_k(z), s) = E_{S_j}(\gamma_k(b_k z), s).$$

Beim Vergleich der konstanten Koeffizienten von Eisensteinreihen zu verschiedenen Spitzen muss diese Skalierung berücksichtigt werden.

In Satz 4.2 wurde der konstante Koeffizient von  $E_{S_j}(z, s)|_{S_k}$  eingeführt als

$$\pi^{1/2} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \cdot \varphi_{jk}(s) \cdot y^{1-s}$$

mit

$$\varphi_{jk}(s) = \frac{1}{(b_j b_k)^s} \sum_{c>0} r_{jk}(c) \frac{1}{c^{2s}}.$$

Aus der Gleichheit der Eisensteinreihen aus Satz 5.20 folgt die Gleichheit der konstanten Koeffizienten:

$$\begin{aligned} b_{k'}^{s-1} \sum_{i=1}^r b_{j_i}^s \pi^{1/2} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \cdot \varphi_{j_i k'}^{\Gamma'}(s) \cdot \text{Im}(b_{k'} z)^{1-s} \\ = b_k^{s-1} b_j^s \pi^{1/2} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \cdot \varphi_{jk}^{\Gamma}(s) \cdot \text{Im}(b_k z)^{1-s}, \end{aligned}$$

wobei die Faktoren  $b_{k'}^{s-1}$  und  $b_k^{s-1}$  die unterschiedlichen Skalierungen aufheben. Also ist

$$b_{k'}^{s-1} \sum_{i=1}^r b_{j_i}^s \varphi_{j_i k'}^{\Gamma'}(s) = b_k^{s-1} b_j^s \varphi_{jk}^{\Gamma}(s), \quad (5.8)$$

## 5.4 Die Summe der Koeffizientenfunktionen zu einer Spitze

woraus über

$$\sum_{i=1}^r \frac{b_{j_i}^s b_k^{1-s}}{(b_{j_i} b_{k'})^s} \sum_{c>0} r_{j_i k'}^{\Gamma'}(c) \frac{1}{c^{2s}} = \frac{b_{j_i}^s b_{k'}^{1-s}}{(b_j b_k)^s} \sum_{c>0} r_{jk}^{\Gamma}(c) \frac{1}{c^{2s}}$$

folgt, dass

$$\frac{b_k}{(b_k b_{k'})^s} \sum_{i=1}^r r_{j_i k'}^{\Gamma'}(c) = \frac{b_{k'}}{(b_k b_{k'})^s} r_{jk}^{\Gamma}(c)$$

gilt. Aus der letzten Formel folgt durch Umstellen die Behauptung.  $\square$

Die Formel 5.4 vom Anfang des Kapitels ist ein Spezialfall von Satz 5.21 und es kann folgender Satz formuliert werden:

**Satz 5.22.** *Sei  $\Gamma \in \Gamma(1)$  eine Untergruppe von endlichem Index mit Repräsentantensystem  $S = \{S_1, \dots, S_r\}$  für die Spitzen. Benenne  $b_i$  die Spitzenbreite von  $S_i$ ,  $i \in \{1, \dots, r\}$ . So gilt für die Koeffizientenfunktionen*

$$\frac{1}{b_k} \sum_{S_j \in S} r_{jk}(c) = r^{\Gamma(1)}(c) = \phi(c) \quad \text{für alle } c. \quad (5.9)$$

*Beweis:* Die Behauptung folgt aus Satz 5.21 und den Ergebnissen zur Streumatrix der Gruppe  $\Gamma(1)$  aus Beispiel 4.5.  $\square$

**Bemerkung 5.23.** *Die Motivation zu einer solchen Gleichung kommt auch aus der Arakelov-Theorie. Dort kann man zeigen, dass die Summe*

$$\frac{1}{b_k} \sum_{S_j \in S} r_{jk}^{\Gamma}(c)$$

*unabhängig von der gewählten Spitze ist.*

*Hier stellt sich sogar heraus, dass die Summe unabhängig von der Gruppe  $\Gamma \subset \Gamma(1)$  ist.*

Über die in dieser Arbeit behandelten Gruppen ist noch mehr bekannt, was die Struktur der Koeffizientenfunktionen noch genauer zu beschreiben hilft.

Mit Satz 5.2, in dem gezeigt wurde, dass jeder zweite Koeffizient null ist, lässt sich die Formel (5.9) in zwei Teile zerlegen. Aus Formel (5.9) folgt, dass für gerade  $c$  gilt:

$$\frac{1}{b_k} \sum_{\substack{S_j \in S \\ S_j \sim_{\Gamma(2)} S_k}} r_{jk}(c) = \phi(c) \quad (5.10)$$

## 5 Eigenschaften der berechneten Streumatrizen

Für ungerade  $c$  gilt:

$$\frac{1}{b_k} \sum_{\substack{S_j \in S \\ S_j \not\sim_{\Gamma(2)} S_k}} r_{jk}(c) = \phi(c) \quad (5.11)$$

Diese Zerlegung ist Resultat der Tatsache, dass alle hier behandelten Gruppen Untergruppen von  $\Gamma(2)$  sind. Ausgehend von dieser Tatsache kann mit Satz 5.21 noch mehr Information gewonnen werden:

**Satz 5.24.** *Sei  $\Gamma \subset \Gamma(2)$  eine Untergruppe von endlichem Index und  $S = \{S_1, \dots, S_r\}$  ein Repräsentantensystem der Spitzen von  $\Gamma$ . Für jede Spitze  $S_k \in S$  mit Spitzenbreite  $b_k$  gilt für gerades  $c$ :*

$$\begin{aligned} \frac{2}{b_k} \sum_{\substack{S_j \in S \\ S_j \sim_{\Gamma(2)} S_k}} r_{jk}^{\Gamma}(c) &= r_{jk}^{\Gamma(2)}(c) = 2\phi(c) \\ \sum_{\substack{S_j \in S \\ S_j \not\sim_{\Gamma(2)} S_k}} r_{jk}^{\Gamma}(c) &= r_{jk}^{\Gamma(2)}(c) = 0 \end{aligned}$$

Für ungerades  $c$  wird zur Vereinfachung der Schreibweise angenommen, dass  $S_k \sim_{\Gamma(2)} \infty$  gilt, dann ergeben sich folgende Formeln:

$$\begin{aligned} \sum_{\substack{S_j \in S \\ S_j \sim_{\Gamma(2)} \infty}} r_{jk}^{\Gamma}(c) &= r_{jk}^{\Gamma(2)}(c) = 0 \\ \frac{2}{b_k} \sum_{\substack{S_j \in S \\ S_j \sim_{\Gamma(2)} 0}} r_{jk}^{\Gamma}(c) &= r_{jk}^{\Gamma(2)}(c) = \phi(c) \\ \frac{2}{b_k} \sum_{\substack{S_j \in S \\ S_j \sim_{\Gamma(2)} 1}} r_{jk}^{\Gamma}(c) &= r_{jk}^{\Gamma(2)}(c) = \phi(c) \end{aligned}$$

Diese Formeln bedeuten, dass die Spitzen, die äquivalent zu 0 sind, und jene, die äquivalent zu 1 sind, jeweils die Hälfte des Gesamtergebnis bilden. Für die anderen beiden Fälle  $S_k \sim_{\Gamma(2)} 0$  und  $S_k \sim_{\Gamma(2)} 1$  vertauschen sich die Spitzen entsprechend, so dass in der ersten Formel immer jene Spitze steht, zu der  $S_k$  unter der Wirkung von  $\Gamma(2)$  äquivalent ist und in den unteren beiden Zeilen die Spitzen stehen, zu denen  $S_k$  unter der Wirkung von  $\Gamma(2)$  nicht äquivalent ist.

## 5.5 Abschätzungen und Approximationen

*Beweis:* Der Satz folgt aus Satz 5.21 und den Ergebnissen zur Streumatrix von  $\Gamma(2)$  aus Satz 4.12 von Seite 45. Die Breite aller Spitzen von  $\Gamma(2)$  ist 2. Die Koeffizienten für  $\Gamma(2)$  haben genau die in der Behauptung aufgeführte Form. □

**Bemerkung 5.25.** *An Satz 5.24 ist zu erkennen, dass Satz 5.2, in dem gezeigt wurde, dass jeder zweite Koeffizient null ist, aus Satz 5.21 über die Relationen der Koeffizientenfunktionen folgt.*

### 5.5 Abschätzungen und Approximationen

Mit den Ergebnissen aus Kapitel 5.4 können die Koeffizienten abgeschätzt werden. Im Folgenden wird eine Abschätzung vorgestellt.

Für eine Gruppe  $\Gamma \subset \Gamma(2)$  und zwei ihrer Spitzen  $S_j$  und  $S_k$  lassen sich die Koeffizienten  $r_{jk}(c)$  mit  $c \in \mathbb{N}$  abschätzen. Es gilt

**Satz 5.26.** *Sei  $\Gamma \subset \Gamma(2)$  eine Untergruppe und  $S_j$  sowie  $S_k$  zwei ihrer Spitzen mit Spitzenbreiten  $b_j$  und  $b_k$ , so gilt für  $r_{jk}(c)$  mit  $c \in \mathbb{N}$ :*

*Wenn  $S_j \sim_{\Gamma(2)} S_k$ , ist*

$$0 \leq r_{jk}^{\Gamma}(c) \leq \chi_2(c+1) \min(b_j, b_k) \phi(c). \quad (5.12)$$

*Wenn  $S_j \not\sim_{\Gamma(2)} S_k$ , ist*

$$0 \leq r_{jk}^{\Gamma}(c) \leq \chi_2(c) \frac{1}{2} \min(b_j, b_k) \phi(c). \quad (5.13)$$

*Beweis:* Dass  $r_{jk}^{\Gamma}(c)$  mit  $c \in \mathbb{N}$  nicht negativ ist, folgt unmittelbar aus der Definition in Satz 4.2 als Kardinalität einer Menge. Der Rest folgt, indem die Aussagen aus Satz 5.24 mit fixierter Spitze  $S_j$  mit denen zu fixierter Spitze  $S_k$  verglichen werden. □

Aus Satz 5.26 kann eine Aussage zum Wachstum der Koeffizienten abgeleitet werden:

**Korollar 5.27.** *Die Koeffizienten  $r_{jk}^{\Gamma}(c)$  wachsen höchstens linear. Die Euler'sche  $\phi$ -Funktion wächst linear, vergleiche dazu Bemerkung 4.6. Nach Satz 5.26 kann  $r_{jk}^{\Gamma}(c)$  nicht schneller wachsen, d.h.*

$$r_{jk}^{\Gamma}(c) \leq O(c). \quad (5.14)$$

## 5 Eigenschaften der berechneten Streumatrizen

Diese Abschätzung für die Koeffizienten ist recht grob. Nach unten wird mit der offensichtlichen Schranke Null abgeschätzt. Auch nach oben ist die Abschätzung sehr großzügig. Dies führt zum Beispiel dazu, dass die Polordnung der  $L$ -Reihe der Abschätzung nicht die der ursprünglichen Funktion ist. Infolge dessen ergibt das Einsetzen der Abschätzung in die Formel 4.5 der Streukonstanten kein vernünftiges Ergebnis mehr.

Um sich eine Vorstellung vom Wert der Streukonstante zu machen, wird nun eine Approximation der Koeffizientenfunktion gegeben, die dies erlaubt:

**Definition 5.28.** Sei  $\Gamma \subset \Gamma(2)$  eine Untergruppe und  $S_j$  sowie  $S_k$  zwei ihrer Spitzen mit Spitzenbreiten  $b_j$  und  $b_k$ , dann sei die Funktion  $\xi_{jk}^\Gamma : \mathbb{N} \rightarrow \mathbb{Q}$  definiert wie folgt:

Für  $c \in \mathbb{N}$  ist

$$\xi_{jk}^\Gamma(c) := \begin{cases} \chi_2(c+1) \cdot \frac{b_j b_k}{2[\Gamma(2):\Gamma]} \phi(c) & \text{wenn } S_j \sim_{\Gamma(2)} S_k \\ \chi_2(c) \cdot \frac{b_j b_k}{4[\Gamma(2):\Gamma]} \phi(c) & \text{wenn } S_j \not\sim_{\Gamma(2)} S_k. \end{cases}$$

Die Funktion  $\xi_{jk}^\Gamma$  lässt sich mit Benutzung der Ergebnisse für die Gruppe  $\Gamma(2)$  darstellen. Es gilt:

$$\xi_{jk}^\Gamma(c) = \frac{b_j b_k}{4[\Gamma(2) : \Gamma]} r_{j'k'}^{\Gamma(2)}(c) \quad \forall c \in \mathbb{N}, \quad (5.15)$$

wobei die Indizes  $j'$  und  $k'$  zu Spitzen  $S_{j'}$  und  $S_{k'}$  aus  $\{0, 1, \infty\}$  gehören mit den Eigenschaften:

$$S_{j'} \sim_{\Gamma(2)} S_j \quad \text{und} \quad S_{k'} \sim_{\Gamma(2)} S_k$$

(Vergleiche dazu die Ergebnisse für die Gruppe  $\Gamma(2)$  aus Satz 4.12 auf Seite 45.)

Für die Funktion  $\xi_{jk}^\Gamma$  stellen wir fest:

**Satz 5.29.** Für eine Funktion  $\xi_{jk}^\Gamma$  nach Definition 5.28 gilt

(i) Die approximierte Streukonstante  $\tilde{C}_{jk}^\Gamma$ , wobei  $\xi_{jk}^\Gamma$  anstatt  $r_{jk}^\Gamma$  eingesetzt wird, konvergiert.

(ii) Für die Summe zu einer Spitze gilt analog zu Satz 5.22:

$$\frac{1}{b_k} \sum_{S_j \in S} \xi_{jk}^\Gamma(c) = \frac{1}{b_k} \sum_{S_j \in S} r_{jk}^\Gamma(c) = \phi(c)$$

Auch der Satz 5.24 gilt analog.

## 5.5 Abschätzungen und Approximationen

*Beweis:* Der Punkt (i) folgt aus dem Zusammenhang von  $\xi_{jk}^\Gamma$  mit den Koeffizientenfunktionen von  $\Gamma(2)$ , siehe Formel (5.15). Für den approximierten konstanten Koeffizienten  $\tilde{\varphi}_{jk}^\Gamma$  folgt:

$$\begin{aligned}\tilde{\varphi}_{jk}^\Gamma &= \frac{1}{(b_j b_k)^s} \frac{b_j b_k}{4 [\Gamma(2) : \Gamma]} \sum_{c>0} r_{j'k'}^{\Gamma(2)}(c) \\ &= \left(\frac{4}{b_j b_k}\right)^s \frac{b_j b_k}{4 [\Gamma(2) : \Gamma]} \frac{1}{4^s} \sum_{c>0} r_{j'k'}^{\Gamma(2)}(c) \\ &= \left(\frac{4}{b_j b_k}\right)^s \frac{b_j b_k}{4 [\Gamma(2) : \Gamma]} \varphi_{j'k'}^{\Gamma(2)}\end{aligned}$$

Der konstante Term von  $\left(\frac{4}{b_j b_k}\right)^s \frac{b_j b_k}{4 [\Gamma(2) : \Gamma]}$  bei Betrachtung der Reihe in  $s = 1$  ist  $\frac{1}{[\Gamma(2) : \Gamma]}$ . Das Residuum des konstanten Terms einer Eisensteinreihe zu  $\Gamma(2)$  ist  $\frac{3}{\pi [\Gamma(1) : \Gamma(2)]}$ , siehe dazu Definition 4.8. Durch Multiplikation ergibt sich das Residuum der Funktion  $\pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \tilde{\varphi}_{jk}^\Gamma$  als

$$\frac{1}{[\Gamma(2) : \Gamma]} \cdot \frac{3}{\pi [\Gamma(1) : \Gamma(2)]} = \frac{3}{\pi [\Gamma(1) : \Gamma]}.$$

Dies ist genau das benötigte Residuum.

Der Punkt (ii) folgt durch einfaches Aufsummieren sowie den Sätzen 5.22 und 5.24. □

Experimente zeigen, siehe z.B. Tabelle 9 auf Seite 97, dass die Abweichung  $\xi_{jk}^\Gamma(c) - r_{jk}^\Gamma(c)$  nicht groß ist und die Differenz mal positiv, mal negativ ist, so dass die Fehler sich gegenseitig relativieren.

Mit der Funktion  $\xi_{jk}^\Gamma$  aus Definition 5.28 lassen sich die Streumatrix und die Streukonstanten approximieren.

**Frage 5.30.** Gilt für die Differenz  $\xi_{jk}^\Gamma(c) - r_{jk}^\Gamma(c)$

**a)** die Differenz wächst sublinear, also  $|\xi_{jk}^\Gamma(c) - r_{jk}^\Gamma(c)| = O(c^{1-\varepsilon})$ ?

Wenn die Antwort auf diese Frage positiv ist, gilt dann

**b)** die in  $O(c^{1-\varepsilon})$  auftretende Konstante  $K(\Gamma)$  ist unabhängig von der Gruppe  $\Gamma$ ?

Falls beide Fragen mit „ja“ zu beantworten sind, so lässt sich auch die Differenz der exakten und approximierten Streukonstanten abschätzen mit:

$$|C_{jk}^\Gamma - \tilde{C}_{jk}^\Gamma| \leq K \cdot \zeta(1 + \varepsilon) \tag{5.16}$$

Da die  $\zeta$ -Funktion in  $s = 1$  einen Pol hat, sollten, für eine bessere Abschätzung, die Vorzeichenwechsel mit beachtet werden.

## 5.6 Total verzweigte Spitzen

Eng mit den Sätzen aus Kapitel 5.4 hängt auch die Tatsache zusammen, dass an vielen Stellen die Einzelergebnisse Vielfache der Euler'schen  $\phi$ -Funktion sind. Für total verzweigte Spitzen sind die Ergebnisse sehr regelmäßig, so dass für diese Fälle konkrete Formeln angegeben werden können. Es lassen sich also Aussagen über die Gestalt der Streumatrix zu einer Gruppe  $\Gamma \subset \Gamma(2)$  und ihrer Einträge  $\varphi_{jk}(s)$  machen.

Der Satz 5.24 impliziert allgemein:

**Satz 5.31.** *Sei  $(K, \beta)$  ein Belyi-Paar. Ist der Morphismus  $\beta$  an einer Stelle total verzweigt und sei  $S_k$  die zugehörige Spitze, dann folgt: In der assoziierten Streumatrix  $\Phi_{(K, \beta)}(s)$  sind die Einträge in der Zeile und der Spalte  $k$  von der Form*

$$\Phi_{(K, \beta)}(s)_{j,k} = \pi^{1/2} \frac{\Gamma(s - 1/2)}{\Gamma(s)} \cdot \frac{1}{a^s} \sum_{c>0} \chi_2(c + \iota) \frac{b \phi(c)}{c^{2s}},$$

wobei  $a, b \in \mathbb{N}$  und  $\iota \in \{0, 1\}$ . Die Werte von  $a, b$  und  $\iota$  ergeben sich direkt aus den Spitzen.

*Beweis:* Die Behauptung folgt aus Satz 5.24: Es folgt sofort, dass in den Zeilen und Spalten Vielfache der  $\phi$ -Funktion auftauchen müssen, wenn der Belyi-Morphismus über einer Stelle total verzweigt ist, weil dann wird für jede Spitze eine Summe aus Satz 5.24 nur über einen Summanden gebildet.

Die Werte für  $a, b$  und  $\iota$  sind einfach zu bestimmen: Das Produkt der Spitzenbreiten der beteiligten Spitzen bildet  $a$ . Ist  $S_j \sim_{\Gamma(2)} S_k$ , so ist  $\iota = 1$  und  $b = b_j$ . Andernfalls ist  $\iota = 0$  und  $b = \frac{b_j}{2}$ .  $\square$

Konkret auf die Beispiele angewandt, lassen sich die folgenden Berechnungsformeln angeben.

### Das Paar $(E, \beta)$

Bei diesem Paar, siehe Formeln (3.5) für das Paar und (3.9) für die Gruppe, ist nur Spitze  $\infty$  total verzweigt:

**Satz 5.32.** *Für das Paar  $(E, \beta)$  bestehen folgende exakten Formeln:*

$$\begin{aligned} \varphi_{\infty\infty}^{\Gamma_E}(s) &= \frac{1}{b_\infty^{2s}} \sum_{c>0} \chi_2(c + 1) \frac{b_\infty \phi(c)}{c^{2s}} \\ \varphi_{\infty k}^{\Gamma_E}(s) &= \frac{1}{(b_\infty b_k)^s} \sum_{c>0} \chi_2(c) \frac{b_k \phi(c)}{2c^{2s}} \end{aligned}$$

Das  $k$  in der zweiten Formel steht für  $S_k \in \{0, 1, 3, 6\}$ .

*Beweis:* Die Behauptung folgt aus Satz 5.31.  $\square$

### Die Gruppe $\Gamma(2)$

In Kapitel 4.2 wurde bewiesen:

**Satz 5.33.** *Für die Gruppe  $\Gamma(2)$  bestehen folgende exakten Formeln. Für alle  $S_j$  und  $S_k$  aus  $\{0, 1, \infty\}$  gilt:*

$$\begin{aligned}\varphi_{jj}^{\Gamma(2)}(s) &= \frac{1}{b_j^{2s}} \sum_{c>0} \chi_2(c+1) \frac{2\phi(c)}{c^{2s}} \\ \varphi_{jk}^{\Gamma(2)}(s) &= \frac{1}{(b_j b_k)^s} \sum_{c>0} \chi_2(c) \frac{\phi(c)}{c^{2s}}\end{aligned}$$

*Beweis:* Der Satz folgt aus Satz 4.12 auf Seite 45.  $\square$

### Das Paar $(C_1, \beta_{C_1})$

Auch bei diesem Paar, siehe Formel (4.22), lassen sich alle Entwicklungen als Vielfache der  $\phi$ -Funktion darstellen:

**Satz 5.34.** *Für das Paar  $(C_1, \beta_{C_1})$  bestehen folgende exakten Formeln. Seien  $S_j$  und  $S_k$  aus  $\{0, 1, \infty\}$  und sei  $b = b_0 = b_1 = b_\infty = 6$  die Spitzenbreite, dann gilt:*

$$\begin{aligned}\varphi_{jj}^{C_1}(s) &= \frac{1}{b^{2s}} \sum_{c>0} \chi_2(c+1) \frac{b\phi(c)}{c^{2s}} \\ \varphi_{jk}^{C_1}(s) &= \frac{1}{b^{2s}} \sum_{c>0} \chi_2(c) \frac{b\phi(c)}{2c^{2s}}\end{aligned}$$

*Beweis:* Die Behauptung folgt aus Satz 5.31.  $\square$

### Das Paar $(C_2, \beta_{C_2})$

Beim Paar  $(C_2, \beta_{C_2})$ , siehe Formel (4.23), sind ebenfalls alle Entwicklungen als Vielfache der  $\phi$ -Funktion darstellbar. Als neues Phänomen gibt es hier Spitzenpaare, bei denen nur jeder vierte Koeffizient auftaucht.

## 5 Eigenschaften der berechneten Streumatrizen

**Satz 5.35.** *Folgende exakte Formeln gelten zu  $(C_2, \beta_{C_2})$ :*

$$\varphi_{jk}^{C_2}(s) = \frac{1}{(b_j b_k)^s} \sum_{c>0} \chi_2(c+1) \frac{8\phi(c)}{c^{2s}} \quad \text{mit } (j, k) \in \{(\infty, \infty), (1, 1)\}$$

$$\varphi_{\infty 1}^{C_2}(s) = \frac{1}{(b_\infty b_1)^s} \sum_{c>0} \chi_2(c) \frac{4\phi(c)}{c^{2s}}$$

$$\varphi_{jk}^{C_2}(s) = \frac{1}{(b_j b_k)^s} \sum_{c>0} \chi_2(c) \frac{2\phi(c)}{c^{2s}} \quad \text{mit } (j, k) \in \{(\infty, 0), (\infty, 2), (0, 1), (1, 2)\}$$

*Beweis:* Die Behauptung folgt aus Satz 5.31. □

Außer den Regelmäßigkeiten aus Satz 5.35 legt die Tabelle 5 auf Seite 61 noch zwei weitere Formeln nah:

**Vermutung 5.36.** *Folgende Formeln gelten zu  $(C_2, \beta_{C_2})$ :*

$$\varphi_{jk}^{C_2}(s) = \frac{1}{(b_j b_k)^s} \sum_{c>0} \chi_4(c) \frac{4\phi(c)}{c^{2s}} \quad \text{mit } (j, k) \in \{(0, 0), (2, 2)\}$$

$$\varphi_{02}^{C_2}(s) = \frac{1}{(b_0 b_2)^s} \sum_{c>0} \chi_4(c+3) \frac{4\phi(c)}{c^{2s}}$$

Hierbei ist

$$\chi_4(n) := \begin{cases} 1 & \text{wenn } 4|n \\ 0 & \text{sonst} \end{cases} \quad \text{für } n \in \mathbb{Z}.$$

**Bemerkung 5.37.** *Die Formeln aus Vermutung 5.36, folgen nicht aus Satz 5.31, da es sich bei denen um Entwicklungen handelt, bei denen keine total verzweigte Spitze beteiligt ist. Vermutung 5.36 ist für die ersten 100 Koeffizienten verifiziert.*

### Die Gruppe $G$

Bei der Gruppe  $G$ , siehe Beispiel 4.21, zeigt sich ein deutlich anderes Verhalten. In keiner Entwicklung taucht ein Vielfaches der  $\phi$ -Funktion auf. Dies ist auch das einzige Beispiel, bei dem über jeder Spitze von  $\Gamma(2)$  mehr als eine Spitze liegt.

### Veranschaulichung: Koeffizienten $r_{\infty\infty}$ für über $\infty$ total verzweigte Morphismen

In dem Fall eines über  $\infty$  total verzweigten Morphismus', wie er hier in den meisten Beispielen vorkommt, ist die Berechnung nach Algorithmus 3 besonders übersichtlich. Darum soll hier am Beispiel  $(E, \beta)$  aus Formel (3.5) mit Gruppe  $\Gamma_E$  nach Formel (3.9) genauer ausgeführt werden, wie es zu dem Ergebnis für  $\varphi_{\infty\infty}^{\Gamma_E}$  aus Satz 5.32 kommt: Es ist

$$r_{\infty\infty}^{\Gamma_E}(c) = \begin{cases} b_{\infty} \phi(c), & \text{wenn } c \equiv 0 \pmod{2}; \\ 0, & \text{wenn } c \equiv 1 \pmod{2}. \end{cases}$$

wobei  $r_{\infty\infty}^{\Gamma_E}(c)$  definiert ist wie folgt:

$$r_{\infty\infty}^{\Gamma_E}(c) = \# \{d \pmod{b_{\infty}c} \mid \exists \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma_E\}$$

Dass zu ungeradem  $c$  der Koeffizient immer null ist, wurde in Satz 5.2 bewiesen. Diese Tatsache ist darauf zurück zu führen, dass es keine Matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$  gibt, mit  $c$  ungerade.

Um zu verdeutlichen, wie es zu dem Ergebnis  $b_{\infty} \phi(c)$  für gerade  $c$  kommt, wird folgendes Lemma benötigt.

**Lemma 5.38.** *Sei die Gruppe  $\Gamma_E$  wie in Formel (3.9) gegeben. Es findet sich immer eine Matrix  $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma_E$ , wenn  $c \equiv 0 \pmod{2}$  und  $\text{ggT}(c, d) = 1$ .*

*Beweis:* Für teilerfremde  $c$  und  $d$  mit geradem  $c$  existiert nach Lemma 4.11 auf Seite 44 eine Matrix  $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma(2)$ .

Eine beliebige Matrix  $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma(2)$  kann durch Multiplikation mit  $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^a$  von rechts in die Gruppe  $\Gamma_E$  verschoben werden, wobei  $a \in \{1, \dots, 5\}$ : Die Gruppe  $\Gamma(2)$  wird nach Lemma 1.28 erzeugt von

$$\gamma_0 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \quad \text{und} \quad \gamma_1 = \begin{pmatrix} -1 & 2 \\ 2 & 3 \end{pmatrix}.$$

Die Matrix  $\begin{pmatrix} * & * \\ c & d \end{pmatrix}$  hat in den Erzeugern von  $\Gamma(2)$  die Darstellung  $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \gamma_1^{-1} \gamma_0^{-1}$ . Eine Matrix ist genau dann in  $\Gamma_E$ , wenn sie unter der Abbildung

$$\begin{aligned} \varphi : \Gamma(2) &\longrightarrow S_5 \\ \gamma_0 &\longmapsto (1235) \\ \gamma_1 &\longmapsto (1234) \end{aligned}$$

den Fixpunkt 5 hat.

Nun ist  $\varphi\left(\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\right) = \varphi(\gamma_1^{-1} \gamma_0^{-1}) = (15243)$ , d.h. für eine der fünf Potenzen gilt

$$\varphi(\gamma_1^{-1} \gamma_0^{-1})^a \varphi\left(\begin{pmatrix} * & * \\ c & d \end{pmatrix}\right)(5) = 5.$$

## 5 Eigenschaften der berechneten Streumatrizen

Für diese Potenz  $a'$  liegt  $(\gamma_1^{-1}\gamma_0^{-1})^{a'} \begin{pmatrix} * & * \\ c & d \end{pmatrix}$  in  $\Gamma_E$ . □

Sei nun also  $c$  gerade. Die Spitzenbreite in  $\infty$  ist 10. Mit Lemma 5.38 und der Definition von  $r_{\infty\infty}$  folgt

$$\begin{aligned} r_{\infty\infty}(c) &= \# \{d \pmod{10c} \mid \exists \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma_E\} \\ &= \# \{d \pmod{10c} \mid (c, d) = 1\} \\ &= \# \{0 \leq d < 10c \text{ und } (c, d) = 1\} \\ &= 10\phi(c), \end{aligned}$$

wobei die letzte Gleichheit nach Lemma 4.10 auf Seite 44 gilt.

An diesem Beispiel ist zu sehen, dass die schöne Form der Koeffizienten auf die Tatsache zurückzuführen ist, dass die Permutation, die zu  $\infty$  gehört, ein Zykel maximaler Länge ist.

## 5.7 Berechnung von Streukonstanten

Die Streukonstante wurde im Kapitel 4 in Definition 4.8 eingeführt. Mit den in dieser Arbeit berechneten endlich vielen Koeffizienten der Streumatrizen lassen sich Streukonstanten im Allgemeinen nicht berechnen. Jedoch lassen sich für einige Fälle Aussagen über die Streukonstanten machen.

### Streukonstanten zu total verzweigten Spitzen

Sei  $\Gamma \subset \Gamma(2)$  eine Untergruppe von endlichem Index, die eine total verzweigte Spitze habe. Zu total verzweigten Spitzen tauchen nach Satz 5.31 Einträge in der Streumatrix auf, welche die Form

$$\Phi_{\Gamma}(s)_{j,k} = \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \frac{b}{(b_j b_k)^s} \sum_{c>0} \chi_2(c+\iota) \frac{\phi(c)}{c^{2s}} \quad (5.17)$$

haben, wobei  $b_j$  und  $b_k$  die Spitzenbreite der beteiligten Spitzen ist,  $\iota \in \{0, 1\}$  und  $b \in \mathbb{N}$  ist.

Schon im Kapitel 4.3, welches die Streukonstanten zur Gruppe  $\Gamma(2)$  thematisierte, wurde erläutert, wie ähnlich strukturierte Formeln derart umgeschrieben werden können, dass die Streukonstante mit Computeralgebrasystemen zu berechnen ist.

So gilt:

$$\begin{aligned} \sum_{c>0} \chi_2(c) \frac{\phi(c)}{c^{2s}} &= \frac{(-2 + 2^{2s})\zeta(2s-1)}{(-1 + 2^{2s})\zeta(2s)} \quad \text{und} \\ \sum_{c>0} \chi_2(c+1) \frac{\phi(c)}{c^{2s}} &= \frac{\zeta(2s-1)}{\zeta(2s)} - \frac{(-2 + 2^{2s})\zeta(2s-1)}{(-1 + 2^{2s})\zeta(2s)} \end{aligned}$$

Mit dieser Manipulation ist die Streukonstante

$$C_{jk}^\Gamma(\iota) = \lim_{s \rightarrow 1} \left( \Phi_\Gamma(s, \iota)_{j,k} - \frac{3/(\pi [\Gamma(1) : \Gamma])}{s-1} \right)$$

zu  $\Phi_\Gamma(s, \iota)_{j,k}$ , die von der in Formel (5.17) aufgeführten Form sind, berechenbar.

Für den Fall  $\iota = 1$ , d.h. für den Fall wo die Spitzen  $S_j$  und  $S_k$ , zu denen die Streukonstante berechnet wird,  $\Gamma(2)$ -äquivalent sind, gilt

$$C_{jk}(1) = -\frac{1}{3\pi} \cdot \frac{b}{b_j b_k} (20 \log(2) + 6 \log(\pi) + 3 \log(b_j b_k) + 72\zeta'(-1) - 6).$$

Im anderen Fall ist

$$C_{jk}(0) = -\frac{2}{3\pi} \cdot \frac{b}{b_j b_k} (8 \log(2) + 6 \log(\pi) + 3 \log(b_j b_k) + 72\zeta'(-1) - 6).$$

### Die Summe der Streukonstanten zu einer Spitze

Auch in den Fällen, wo über die einzelnen Streukonstanten nichts ausgesagt werden kann, ist es möglich, die Summe der Streukonstanten zu einer Spitze zu berechnen:

**Satz 5.39.** *Sei  $\Gamma \subset \Gamma(1)$  eine Untergruppe von endlichem Index,  $S = \{S_1, \dots, S_r\}$  ein Repräsentantensystem für die Spitzen mit Spitzenbreiten  $b_1, \dots, b_r$  und  $S_k$  eine fixierte Spitze, dann gilt für die Summe der Streukonstanten*

$$\sum_{S_j \in S} b_j C_{jk} + \frac{3}{\pi} \log(b_k) = C^{\Gamma(1)} - \frac{3}{\pi [\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j), \quad (5.18)$$

wobei der Wert der Streukonstanten  $C^{\Gamma(1)}$  bekannt ist.

*Beweis:* Die Streukonstante ist folgendermaßen definiert:

$$\begin{aligned} C_{jk} &= \lim_{s \rightarrow 1} \left( \Phi_\Gamma(s)_{j,k} - \frac{3/(\pi [\Gamma(1) : \Gamma])}{s-1} \right) \\ &= \lim_{s \rightarrow 1} \left( \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \varphi_{jk}(s) - \frac{3/(\pi [\Gamma(1) : \Gamma])}{s-1} \right) \\ &= \lim_{s \rightarrow 1} \left( \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \frac{1}{(b_j b_k)^s} \sum_{c>0} r_{jk}(c) \frac{1}{c^{2s}} - \frac{3/(\pi [\Gamma(1) : \Gamma])}{s-1} \right) \end{aligned}$$

## 5 Eigenschaften der berechneten Streumatrizen

Betrachte nun für eine fest gewählte Spitze  $S_k$  die Summe  $\sum_{S_j \in S} b_j C_{jk}$ .  
Es ergibt sich:

$$\begin{aligned} \sum_{S_j \in S} b_j C_{jk} &= \lim_{s \rightarrow 1} \left( \sum_{S_j \in S} \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \frac{b_j}{(b_j b_k)^s} \sum_{c>0} r_{jk}(c) \frac{1}{c^{2s}} - \frac{3}{\pi(s-1)} \right) \\ &= \lim_{s \rightarrow 1} \left( \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \sum_{S_j \in S} \frac{b_j}{(b_j b_k)^s} \sum_{c>0} r_{jk}(c) \frac{1}{c^{2s}} - \frac{3}{\pi(s-1)} \right) \end{aligned}$$

wobei

$$\frac{3}{\pi(s-1)} = \sum_{S_j \in S} b_j \frac{3/(\pi [\Gamma(1) : \Gamma])}{s-1}$$

ist, da die Summe der Breite aller Spitzen genau der Index der Gruppe ist.

Die Terme, die in den einzelnen Summanden auftauchen, können jeweils in  $s = 1$  in eine Reihe entwickelt werden. Es ergeben sich

$$\frac{b_j}{(b_j b_k)^s} = \frac{1}{b_k} - \frac{\log(b_j b_k)}{b_k} (s-1) + O((s-1)^2) \quad (5.19)$$

$$\pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} = \pi - \pi \log(4)(s-1) + O((s-1)^2) \quad (5.20)$$

$$\sum_{c>0} r_{jk}(c) \frac{1}{c^{2s}} = \frac{c_j}{s-1} + K_j + O(s-1), \quad (5.21)$$

wobei  $c_j$  und  $K_j$  von den Koeffizienten  $r_{jk}(c)$  abhängen.

Die Konstante  $c_j$  lässt sich bestimmen, da die Polordnung der Streukonstanten zu  $S_j$  und  $S_k$  bekannt ist. Mit den Reihenentwicklungen der einzelnen Terme folgt dann, dass

$$c_j \cdot \pi \cdot \frac{1}{b_j b_k} = \frac{3}{\pi [\Gamma(1) : \Gamma]} \quad \Rightarrow \quad c_j = \frac{3b_j b_k}{\pi^2 [\Gamma(1) : \Gamma]}. \quad (5.22)$$

Auch über die  $K_j$ 's lässt sich einiges aussagen. Hier ist der Wert für ein eine einzelne Konstante  $K_j$  nicht bekannt. Doch die Summe  $\sum_{S_j \in S} K_j$  lässt sich bestimmen, da sie eng mit der Streukonstanten zur Gruppe  $\Gamma(1)$  verbunden ist.

## 5.7 Berechnung von Streukonstanten

Es ist

$$\begin{aligned}
 C^{\Gamma(1)} &= \pi^{1/2} \frac{\Gamma(2s-1)}{\Gamma(2s)} \varphi^{\Gamma(1)} - \frac{3}{\pi(s-1)} \\
 &= \pi^{1/2} \frac{\Gamma(2s-1)}{\Gamma(2s)} \sum_{c>0} r^{\Gamma(1)} - \frac{3}{\pi(s-1)} \\
 &= \pi^{1/2} \frac{\Gamma(2s-1)}{\Gamma(2s)} \sum_{S_j \in S} \frac{1}{b_k} \sum_{c>0} r_{jk}^{\Gamma} - \frac{3}{\pi(s-1)} \\
 &= \sum_{S_j \in S} \left( \frac{\pi c_j}{b_k(s-1)} + \frac{\pi}{b_k} K_j - \frac{\pi}{b_k} \log(4) c_j \right) - \frac{3}{\pi(s-1)}.
 \end{aligned}$$

Damit folgt für die Summe der  $K_j$ :

$$\sum_{S_j \in S} K_j = \frac{b_k}{\pi} C^{\Gamma(1)} + \frac{3b_k}{\pi^2} \log(4)$$

Mit diesen Informationen kann die Summe berechnet werden. Mittels

$$\begin{aligned}
 &\sum_{S_j \in S} \frac{b_j}{(b_j b_k)^s} \sum_{c>0} r_{jk}(c) \frac{1}{c^{2s}} \\
 &= \sum_{S_j \in S} \left( \frac{1}{b_k} - \frac{\log(b_j b_k)}{b_k} (s-1) + O((s-1)^2) \right) \left( \frac{c_j}{s-1} + K_j + O(s-1) \right) \\
 &= \sum_{S_j \in S} \frac{1}{b_k} \cdot \frac{c_j}{s-1} - c_j \frac{\log(b_j b_k)}{b_k} + \frac{K_j}{b_k} + O(s-1) \\
 &= \frac{3}{\pi^2(s-1)} - \frac{3}{\pi^2 [\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j) - \frac{3}{\pi^2} \log(b_k) \\
 &\quad + \frac{C^{\Gamma(1)}}{\pi} + \frac{3}{\pi^2} \log(4) + O(s-1)
 \end{aligned}$$

ergibt sich

$$\begin{aligned}
\sum_{S_j \in S} b_j C_{jk} &= \lim_{s \rightarrow 1} \left( (\pi - \pi \log(4)(s-1) + O((s-1)^2)) \cdot \right. \\
&\quad \left. \left( \frac{3}{\pi^2(s-1)} - \frac{3}{\pi^2 [\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j) - \frac{3}{\pi^2} \log(b_k) + \frac{C^{\Gamma(1)}}{\pi} + \frac{3}{\pi^2} \log(4) + O(s-1) \right) - \frac{3}{\pi(s-1)} \right) \\
&= \lim_{s \rightarrow 1} \left( \frac{3}{\pi(s-1)} - \frac{3}{\pi [\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j) - \frac{3}{\pi} \log(b_k) + C^{\Gamma(1)} + \frac{3}{\pi} \log(4) - \frac{3}{\pi} \log(4) - \frac{3}{\pi(s-1)} \right) \\
&= C^{\Gamma(1)} - \frac{3}{\pi} \left( \log(b_k) + \frac{1}{[\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j) \right)
\end{aligned}$$

□

**Bemerkung 5.40.** Wenn der Wert für  $C^{\Gamma(1)}$  eingesetzt wird, so gilt

$$\sum_{S_j \in S} b_j C_{jk} = -\frac{3}{\pi} \left( 24\zeta'(-1) - 2 + 2 \log(4\pi) + \log(b_k) + \frac{1}{[\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j) \right).$$

## 6 Eine arithmetische Anwendung der Streukonstanten

In seinem Artikel [Kü2] zeigt U. Kühn eine Anwendung von Streukonstanten für die Arakelov-Theorie. Hier sollen Ergebnisse aus den Kapiteln 4 und 5 auf die Berechnung von Höhenpaarungen angewendet werden.

### 6.1 Néron-Tate-Höhenpaarungen und Streukonstanten

Ist  $K$  eine über  $\overline{\mathbb{Q}}$  definierte Kurve, dann lässt sich für Divisoren  $D$  vom Grad 0 auf  $K$  eine Néron-Tate-Höhenpaarung  $\langle \cdot \rangle_{NT}$  definieren. Für elliptische Kurven ist wegen des Isomorphismus  $E \simeq \text{Pic}^0(E)$  eine Verträglichkeit mit Definition 1.15 gewährleistet. Mit Hilfe der Streukonstante zu Eisensteinreihen, siehe Definition 4.8, die zu Belyi-Paaren  $(K, \beta)$  assoziiert sind, lassen sich Néron-Tate-Höhenpaarungen von Grad 0 Divisoren auf der Kurve  $K$  auf eine neue Art berechnen.

**Satz 6.1** (Kühn). *Sei  $\beta : K \rightarrow \mathbb{P}^1$  ein Belyi-Morphismus für eine algebraische Kurve über  $\mathbb{Q}$  mit induzierter Belyi-Uniformisierung  $K(\mathbb{C}) \equiv \overline{\Gamma_K \backslash \mathbb{H}}$ . Seien  $D_1 = \sum_j n_j S_j$  und  $D_2 = \sum_k m_k S_k$  zwei Spitzendivisoren vom Grad 0. Dann gilt für die Néron-Tate-Höhenpaarung von  $D_1$  und  $D_2$ :*

$$\langle D_1, D_2 \rangle_{NT} = - \sum_{p \text{ prim}} \delta_p \log(p) - 2\pi \sum_{j,k} n_j m_k C_{jk}^{\Gamma_K}, \quad (6.1)$$

wobei die  $\delta_p$  rationale, explizit berechenbare<sup>1</sup> Zahlen sind und  $C_{jk}^{\Gamma_K}$  die Streukonstante zu  $S_j$  und  $S_k$  bezüglich  $\Gamma_K$  ist.

*Beweis:* Siehe [Kü2], Seite 402. □

**Definition 6.2.** *Mit Satz 6.1 lässt sich die Höhenpaarung zweier Grad Null Divisoren  $D_1$  und  $D_2$  in einen algebraischen und einen analytischen Teil aufteilen:*

$$\langle D_1, D_2 \rangle_{NT} = h_{NT}^{alg}(D_1, D_2) + h_{NT}^{analyt}(D_1, D_2), \quad (6.2)$$

wobei

$$h_{NT}^{alg}(D_1, D_2) = - \sum_{p \text{ prim}} \delta_p \log(p) \quad (6.3)$$

---

<sup>1</sup>Der Aufwand zur Berechnung dieser Zahlen ist vermutlich ähnlich dem der in dieser Arbeit vollzogenen Berechnungen zu  $C_{jk}^{\Gamma_K}$ .

## 6 Eine arithmetische Anwendung der Streukonstanten

und

$$h_{NT}^{analyt}(D_1, D_2) = -2\pi \sum_{j,k} n_j m_k C_{jk}^{\Gamma_K} \quad (6.4)$$

ist. Die Benennung der Teile ist durch den Beweis zu Satz 6.1 motiviert.

Gegeben sei eine elliptische Kurve  $E$  und der Divisor  $0_E - P$ , mit  $0_E$  und  $P \in E$ . Da  $E$  isomorph zu ihrer Picardgruppe ist, d.h. es gilt:  $E \simeq Pic^0(E)$ , ist in diesem Fall die Néron-Tate-Paarung auf  $Pic^0(E)$  aus Formel (6.1) des Divisors  $0_E - P$  mit sich selbst durch die Formel

$$\langle 0_E - P, 0_E - P \rangle_{NT} = \langle P, P \rangle_{NT} \quad (6.5)$$

gegeben, wobei die rechte Seite der Formel (6.5) bereits im Kapitel 1.1 in Satz 1.16 eingeführt worden ist.

### 6.2 Der analytische Anteil der Höhe von $P = (1, 4) \in E$

Sei für die elliptische Kurve  $E$  ein Belyi-Morphismus  $\beta : E \rightarrow \mathbb{P}^1$  gegeben und sei  $E(\mathbb{C}) = \overline{\Gamma_E \backslash \mathbb{H}}$ . Weiter gelte, dass  $0_E$  und  $P$  Spitzen  $S_j$  und  $S_k$  entsprechen, also dass  $\{0_E, P\} \subset \beta^{-1}(\text{Verzweigungspunkte})$  gelte. Dann ist

$$\begin{aligned} \langle P, P \rangle_{NT} &= \langle 0_E - P, 0_E - P \rangle_{NT} \\ &= - \sum_{p \text{ prim}} \delta_p \log(p) - 2\pi \sum_{j,k} C_{jk}^{\Gamma_E}. \end{aligned}$$

Nun soll für den Punkt  $P = (1, 4)$ , der auf der Kurve  $E$  aus Kapitel 3 liegt, siehe dazu Satz 3.8, der analytische Anteil von  $\langle D_P, D_P \rangle_{NT}$  nach Formel (6.3) berechnet werden. Die in Kapitel 4.6 berechneten Koeffizienten der Streumatrix von  $\Gamma_E$  sollen dafür verwendet werden. Da nur endlich viele Koeffizienten bekannt sind, kann der analytische Anteil der Höhe nur näherungsweise bestimmt werden.

Sei  $D_P$  der Divisor  $P - 0_E$ . Der Punkt  $P = (1, 4)$  liegt nach Lemma 3.16 über der Spitze Null, welche die Breite 8 hat;  $0_E$  liegt über  $\infty$ , einer Spitze mit Breite 10. Mit der Definition 4.8 für die Streukonstante folgt für  $D_P$ :

$$\begin{aligned} h_{NT}^{analyt}(D_P, D_P) &= h_{NT}^{analyt}(0_E - P, 0_E - P) \\ &= -2\pi (C_{\infty\infty}^{\Gamma_E} - 2C_{\infty 0}^{\Gamma_E} + C_{00}^{\Gamma_E}) \\ &= -2\pi \lim_{s \rightarrow 1} (\Phi_{\Gamma_E}(s)_{\infty, \infty} - 2\Phi_{\Gamma_E}(s)_{\infty, 0} + \Phi_{\Gamma_E}(s)_{0, 0}) \end{aligned} \quad (6.6)$$

## 6.2 Der analytische Anteil der Höhe von $P = (1, 4) \in E$

Nun werden die Definitionen von  $\Phi_{\Gamma_E}(s)$ , siehe Formel (4.4), und  $\varphi_{jk}(s)$  aus Formel (4.1) eingesetzt und man erhält:

$$h_{NT}^{analyt}(D_P, D_P) = -2\pi \lim_{s \rightarrow 1} \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \sum_{c=1}^{\infty} \left( \frac{r_{\infty\infty}^{\Gamma_E}(c)}{b_{\infty}^{2s}} - 2 \frac{r_{\infty 0}^{\Gamma_E}(c)}{(b_{\infty} b_0)^s} + \frac{r_{00}^{\Gamma_E}(c)}{b_0^{2s}} \right) \frac{1}{c^{2s}}. \quad (6.7)$$

**A) (Direkte Berechnung):** Da nur endlich viele Koeffizienten bekannt sind, wird nur über eine endliche Reihe summiert. In diesem Fall gibt es keine Konvergenzprobleme, d.h. der Limes kann weggelassen und  $s = 1$  gesetzt werden. Zu berechnen ist dann folgende Formel:

$$h_{NT}^{analyt}(D_P, D_P) \approx -2\pi^2 \sum_{c=1}^N \left( \frac{r_{\infty\infty}^{\Gamma_E}(c)}{100} - 2 \frac{r_{\infty 0}^{\Gamma_E}(c)}{80} + \frac{r_{00}^{\Gamma_E}(c)}{64} \right) \frac{1}{c^2}. \quad (6.8)$$

In der Tabelle 7 auf Seite 94 sind die Ergebnisse für einige  $N \leq 500$  aufgelistet. Da die Ergebnisse sich nicht monoton verhalten, wird, um eine gute Näherung zu bekommen, über die Ergebnisse von  $N = 497$  bis  $N = 500$  gemittelt. Der angegebene Fehler ist der Betrag, um den das gemittelte Ergebnis von den Einzelergebnissen variieren, also  $\max |\text{gemittelter Wert} - \text{Einzelwert}|$ .

$$\begin{aligned} h_{NT}^{analyt}(D_P, D_P) &\approx -2\pi^2 \cdot \frac{1}{4} (-0,05815 - 0,05802 - 0,05822 - 0,05805) \\ &= 1,14705 \pm 0,002. \end{aligned} \quad (6.9)$$

Aufgrund der Struktur der Koeffizienten, siehe Tabelle 3 auf Seite 56, tauchen in der Summe in Formel (6.8) für gerade  $c$  nur die beiden positiven Summanden  $r_{\infty\infty}^{\Gamma_E}(c)$  und  $r_{00}^{\Gamma_E}(c)$  auf. Bei ungeradem  $c$  ist nur der mittlere Summand  $r_{\infty 0}^{\Gamma_E}(c)$ , welcher abgezogen wird, nicht null. Die unterschiedlichen Vorzeichen in Formel (6.8) sorgen also nicht für kleine Summanden. Die Summe wächst nicht monoton und das Ergebnis verändert sich mit jedem neuen Reihenglied recht stark. In der Tabelle 7 auf Seite 94 ist zu sehen, dass der Wert ab der dritten Nachkommastellen noch variiert.

Auf den folgenden Seiten wird der Versuch unternommen, die Konvergenz zu verbessern, indem die Ergebnisse für die Gruppe  $\Gamma(2)$  bei der Berechnung mit benutzt werden. Außerdem wird ein Versuch unternommen, das Ergebnis abzuschätzen.

**B) (Berechnung mit Hilfe von  $\Gamma(2)$ ):** Für die Gruppe  $\Gamma(2)$  tauchen nur zwei verschiedene Streukonstanten auf. Diese wurden in den Formeln (4.11)

## 6 Eine arithmetische Anwendung der Streukonstanten

N	$C_{\infty\infty} - 2C_{\infty 0} + C_{00}$	$h_{NT}^{analyt}(D_P, D_P)$
100	-0,05743	1,13362
200	-0,05810	1,14684
300	-0,05800	1,14487
400	-0,05793	1,14349
491	-0,05820	1,14882
492	-0,05807	1,14625
493	-0,05825	1,14981
494	-0,05807	1,14625
495	-0,05817	1,14822
496	-0,05798	1,14447
497	-0,05815	1,14783
498	-0,05802	1,14526
499	-0,05822	1,14921
500	-0,05805	1,14586

Tabelle 7: Summen zur Höhenberechnung von  $P = (1, 4)$

und (4.14) berechnet. Jetzt wird versucht, die Höhe für den Punkt  $P = (1, 4)$  mit einigen Abwandlungen der Formel (6.8) genauer zu berechnen.

Zunächst wird folgende Umformung betrachtet:

$$\begin{aligned}
 & C_{\infty\infty}^{\Gamma_E} - 2C_{\infty 0}^{\Gamma_E} + C_{00}^{\Gamma_E} \\
 = & (C_{\infty\infty}^{\Gamma_E} + C_{00}^{\Gamma_E} - 2C_{\infty\infty}^{\Gamma(2)}) + (2C_{\infty 0}^{\Gamma(2)} - 2C_{\infty 0}^{\Gamma_E}) \\
 & + (2C_{\infty\infty}^{\Gamma(2)} - 2C_{\infty 0}^{\Gamma(2)})
 \end{aligned}$$

Welchen Vorteil hat diese Summe?

Im ersten Teil

$$C_g := C_{\infty\infty}^{\Gamma_E} + C_{00}^{\Gamma_E} - 2C_{\infty\infty}^{\Gamma(2)}$$

kommen in der Reihenentwicklung nur Koeffizienten zu geradem  $c$  vor.

Im zweiten Teil

$$C_u := 2C_{\infty 0}^{\Gamma(2)} - 2C_{\infty 0}^{\Gamma_E}$$

treten in der Reihenentwicklung nur Koeffizienten zu ungeradem  $c$  auf.

Der letzte Teil

$$C_{\Gamma(2)} := 2C_{\infty\infty}^{\Gamma(2)} - 2C_{\infty 0}^{\Gamma(2)}$$

ist durch die Formeln (4.11) und (4.14) gegeben.

Durch die unterschiedlichen Vorzeichen ist zu hoffen, dass die Summanden in der Reihe zu  $C_g$  und  $C_u$  klein werden und die Summe gut konvergiert.

6.2 Der analytische Anteil der Höhe von  $P = (1, 4) \in E$

N	Wert der Summe	$h_{NT}^{analyt}(D_P, D_P)$
100	0,22026	1,19741
200	0,22274	1,14846
300	0,22241	1,15498
400	0,22218	1,15952
491	0,22319	1,13958
492	0,22266	1,15004
493	0,22340	1,13543
494	0,22269	1,14945
495	0,22308	1,14175
496	0,22230	1,15715
497	0,22298	1,14372
498	0,22245	1,15419
499	0,22325	1,13839
500	0,22261	1,15082

Tabelle 8: modifizierte Summen zur Höhenberechnung von  $P = (1, 4)$

$$\begin{aligned}
C_g + C_u &= (C_{\infty\infty}^{\Gamma_E} + C_{00}^{\Gamma_E} - 2C_{\infty\infty}^{\Gamma(2)}) + (2C_{\infty 0}^{\Gamma(2)} - 2C_{\infty 0}^{\Gamma_E}) \\
&= \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \left( \varphi_{\infty\infty}^{\Gamma_E} + \varphi_{00}^{\Gamma_E} - 2\varphi_{\infty\infty}^{\Gamma(2)} - 2\varphi_{\infty 0}^{\Gamma_E} + 2\varphi_{\infty 0}^{\Gamma(2)} \right) \\
&= \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \left( \sum_{c>0} \chi_2(c+1) \left( \frac{r_{\infty\infty}^{\Gamma_E}(c)}{100^s} + \frac{r_{00}^{\Gamma_E}(c)}{64^s} - \frac{4}{4^s} \phi(c) \right) \frac{1}{c^{2s}} \right. \\
&\quad \left. + \sum_{c>0} \chi_2(c) \left( \frac{2}{4^s} \phi(c) - \frac{2r_{\infty 0}^{\Gamma_E}(c)}{80^s} \right) \frac{1}{c^{2s}} \right)
\end{aligned}$$

Die große Klammer aus der letzten Formel mit Maple berechnet führt zu den Ergebnissen in Spalte zwei der Tabelle 8. Bedauerlicherweise ist zu sehen, dass die Konvergenz nicht sichtlich besser geworden ist.

Mit  $\frac{1}{4}(0, 22298+0, 22245+0, 22325+0, 22261) = 0, 22282$  ist das Ergebnis

$$\begin{aligned}
h_{NT}^{analyt}(D_P, D_P) &= -2\pi (C_g + C_u + C_{\Gamma(2)}) \\
&\approx -2\pi \left( \pi \cdot (0, 22282) - \frac{4 \log(2)}{\pi} \right) \\
&= 1, 14689 \pm 0, 008.
\end{aligned}$$

In der dritten Spalte von Tabelle 8 ist  $h_{NT}^{analyt}(D_P, D_P)$ , berechnet über  $\Gamma(2)$ , zu sehen.

**C) (Berechnung mit Hilfe von Satz 5.32):** Eine weitere Möglichkeit, die Rechengenauigkeit zu verbessern, ist, den Satz aus Kapitel 5.2 mit zu berücksichtigen. In Satz 5.32 wurde eine Bildungsvorschrift für  $r_{\infty\infty}^{\Gamma_E}$  und  $r_{\infty 0}^{\Gamma_E}$  angegeben. Mit diesem Satz ergibt sich:

$$C_{\infty\infty}^{\Gamma_E} - 2C_{\infty 0}^{\Gamma_E} + C_{00}^{\Gamma_E} \stackrel{\text{Satz 5.32}}{=} \pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \left( \sum_{c>0} \chi_2(c+1) \left( \frac{10\phi(c)}{100^s} + \frac{r_{00}^{\Gamma_E}(c)}{64^s} \right) \frac{1}{c^{2s}} - \sum_{c>0} \chi_2(c) \frac{8\phi(c)}{80^s} \frac{1}{c^{2s}} \right)$$

Um jetzt präziser Rechnen zu können, müssen zu  $r_{00}^{\Gamma_E}$  noch mehr Koeffizienten berechnet werden. Damit wurde der Rechenaufwand von der Berechnung von Koeffizienten zu drei Entwicklungen auf die Berechnung der Koeffizienten zu einer einzigen Entwicklung reduziert.

Für die Entwicklung zur Spitze 0 in der Spitze 0 wurden noch 100 weitere Koeffizienten berechnet, so dass die Summe über die ersten 600 Koeffizienten betrachtet werden kann. Das Ergebnis ändert sich dadurch leicht und es ergibt sich

$$\begin{aligned} h_{NT}^{analyt}(D_P, D_P) &\approx -2\pi^2 \cdot \frac{1}{4}(-0,05801 - 0,05798 - 0,05798 - 0,05805) \\ &= 1,14497 \pm 0,002. \end{aligned} \tag{6.10}$$

**D) (Abschätzung mit Hilfe von Kapitel 5.5):** Als Alternative zum Ausrechnen weitere Koeffizienten, wird die Funktion  $\xi_{jk}^{\Gamma_E}$  aus Definition 5.28 von Seite 80 benutzt, um das Ergebnis zu nähern. Der Beginn der Reihe kann mit den berechneten Koeffizienten bestimmt werden. Für die höheren Koeffizienten, die nicht mehr bekannt sind, wird die Funktion  $\xi_{jk}^{\Gamma_E}$  als Koeffizientenfunktion gewählt.

Für die Gruppe  $\Gamma_E$  mit Spitzen 0 und 0 ist

$$\begin{aligned} \xi_{00}^{\Gamma_E} : \mathbb{N} &\longrightarrow \mathbb{Q} \\ c &\longmapsto \chi_2(c+1) \cdot \frac{64}{10} \phi(c). \end{aligned}$$

Beim Vergleich der Werte von  $r_{00}^{\Gamma_E}$  und  $\xi_{00}^{\Gamma_E}$  liegt der relative Fehler  $\left| \frac{r_{00}^{\Gamma_E}(c) - \xi_{00}^{\Gamma_E}(c)}{c} \right|$  bei größerem  $c$  bei unter 5%, wie in der Tabelle 9 auf Seite 97 zu sehen ist. Außerdem ist der Fehler mal positiv und mal negativ, so dass sich die Fehler ausgleichen und die Summe über alle Fehler bei 500 Summanden nur bei 20 liegt. Die wichtigste Eigenschaft dieser Reihe ist aber,

## 6.2 Der analytische Anteil der Höhe von $P = (1, 4) \in E$

dass sie genau das fehlende Residuum hat, welches notwendig ist, damit die Reihe

$$\pi^{1/2} \frac{\Gamma(s - 1/2)}{\Gamma(s)} \sum_{c>0} \left( \chi_2(c+1) \left( \frac{10\phi(c)}{100^s} + \frac{6,4\phi(c)}{64^s} \right) - \chi_2(c) \frac{8\phi(c)}{80^s} \right) \frac{1}{c^{2s}}$$

konvergiert.

c	$r_{00}^{\Gamma E}(c)$	$\xi^{\Gamma E}(c)$	abs. Fehler	rel. Fehler
480	856	819,2	-36,8	-0,043
481	0	0	0	0
482	1516	1536	20	0,013
483	0	0	0	0
484	1384	1408	24	0,017
485	0	0	0	0
486	1028	1036,8	8,8	0,009
487	0	0	0	0
488	1526	1536	10	0,007
489	0	0	0	0
490	1128	1075,2	-52,8	-0,047
491	0	0	0	0
492	1012	1024	12	0,012
493	0	0	0	0
494	1380	1382,4	2,4	0,002
495	0	0	0	0
496	1516	1536	20	0,013
497	0	0	0	0
498	1048	1049,6	1,6	0,002
499	0	0	0	0
500	1324	1280	-44	-0,033

Tabelle 9: Näherung an die Koeffizienten von  $\varphi_{00}^{\Gamma E}$

Mit dieser Funktion lässt sich recht einfach eine Summe über beliebig viele Summanden berechnen. Die Genauigkeit des Ergebnisses wird damit natürlich nicht wirklich erhöht, da die weiteren Koeffizienten falsch sind. Aber die Berechnung wird einen Eindruck vermitteln, wie weit sich das Ergebnis, welches durch die ersten 500 Koeffizienten gegeben ist, noch verändert.

In diesem Fall kann eine Summe  $\sum_{jk} n_j n_k \tilde{C}_{jk}^{\Gamma E}$  nach Formel (6.7) berech-

## 6 Eine arithmetische Anwendung der Streukonstanten

net werden, indem angenommen wird:

$$\begin{aligned} r_{\infty\infty}^{\Gamma_E}(c) &= \chi_2(c+1)10\phi(c) \\ r_{\infty 0}^{\Gamma_E}(c) &= \chi_2(c)4\phi(c) \\ \tilde{r}_{00}^{\Gamma_E}(c) &= \xi_{00}^{\Gamma_E}(c) \end{aligned}$$

Mit Mathematica folgt:

$$C_{\infty\infty}^{\Gamma_E} - 2C_{\infty 0}^{\Gamma_E} + \tilde{C}_{00}^{\Gamma_E} = -\frac{4 \log(2)}{5\pi} \approx -0,17650$$

Werden nun die ersten 500 Reihenglieder wieder abgezogen, verbleibt ein Rest, der einen Eindruck vermittelt, wie weit das Ergebnis aus Formel (6.9) sich noch verändert. Für die ersten 500 Reihenglieder ergibt sich

$$\pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \sum_{c=1}^{500} \left( \frac{r_{\infty\infty}^{\Gamma_E}(c)}{100^s} + \frac{\tilde{r}_{00}^{\Gamma_E}(c)}{64^s} - 2 \frac{r_{\infty 0}^{\Gamma_E}(c)}{80^s} \right) \frac{1}{c^{2s}} \approx -0,17635.$$

Die Differenz ist dann  $-0,00015$ . Mit diesen Ergebnissen ist davon auszugehen, dass der Fehler der Berechnung nach Formel (6.8) in der Größenordnung von  $10^{-4}$  liegt.

**Über den geometrischen Anteil der Höhe von  $P = (1, 4)$ :** Nun ist der analytische Anteil der Höhe näherungsweise bekannt. Betrachte nun den algebraischen Anteil, vergleiche dazu Formel (6.4):

$$h_{NT}^{alg}(D_1, D_2) = - \sum_{p \text{ prim}} \delta_p \log(p)$$

Die Berechnung des algebraischen Anteils ist in dieser Arbeit nicht zu leisten, doch eine mögliche Form kann angegeben werden.

In Kapitel 3 wurde in Formel (3.1) die Höhe von  $P$  als  $\langle P, P \rangle_{NT} \approx 0,12838$  angegeben. Nach Formel (6.5) ist diese gleich der Höhe des Divisors  $D_P$ . Zusammen mit dem Ergebnis für den analytischen Anteil der Höhe aus Formel (6.10), ist eine Näherung für den algebraischen Teil wie folgt zu finden:

$$\begin{aligned} h_{NT}^{alg}(D_P, D_P) &= \langle D_P, D_P \rangle_{NT} - h_{NT}^{analyt}(D_P, D_P) \\ &\approx 0,12838 - 1,14497 \\ &= -1,01659 \end{aligned}$$

Der Beweis von Satz 6.1 lässt erwarten, dass die Primzahlen 2 und 5 im algebraischen Anteil auftauchen und eine mögliche Darstellung ist

$$h_{NT}^{alg}(D_P, D_P) = -\frac{1}{5} \log(2) - \frac{6}{11} \log(5) \approx -1,01650$$

## 6.2 Der analytische Anteil der Höhe von $P = (1, 4) \in E$

mit

$$-1,01659 - 10^{-4} < -1,01650 < -1,01659 + 10^{-4},$$

wobei  $10^{-4}$  die erwartete Genauigkeit des Ergebnisses für den analytischen Anteil der Höhe ist.

Eine andere Darstellung hat die Form

$$h_{NT}^{alg}(D_P, D_P) = -\frac{17}{9} \log(2) + \frac{2}{11} \log(5) \approx -1,01665.$$

Auch hier gilt

$$-1,01659 - 10^{-4} < -1,01665 < -1,01659 + 10^{-4}.$$

So lange die Höhe der Koeffizienten unbeschränkt ist, vergleiche Definition 1.14, lässt sich eine beliebig gute Näherung finden.

## A Anhang

### A.1 InGruppe.java

Hier ist der Programmcode eines Java-Programmes abgedruckt, mit dem für ein Wort getestet wird, ob die zugehörige Matrix in der Gruppe  $\Gamma_E$  aus Kapitel 3.2 liegt. Im Programm InGruppe.java ist der Algorithmus 1 implementiert.

Eine Erklärung der Befehle ist zum Beispiel im Internet bei [Ja] zu finden.

```

import java.io.*;
import java.awt.*;

class InGruppe
{
    /* verknuepft zwei Permutationen.
     * Permutationen sigma werden so gegeben:
     * Als Integer-Array von der Laenge 5,
     * an i-ter Position steht sigma(i)
     */
    public static int[] verkn (int [] a, int [] b)
    {
        int [] perm= {1,2,3,4,5};
        for (int i=0; i<5; i++)
            perm[i]= b[a[i]-1];
        return perm;
    }

    // berechnet das Bild unter der Abbildung phi_E in S_5
    public static int[] bild (String l)
    {
        int [] perm = {1,2,3,4,5};
        int [] P1 = {5,1,2,4,3};
        int [] P2 = {4,1,2,3,5};
        int [] P3 = {2,3,5,4,1};
        int [] P4 = {2,3,4,1,5};
        String vergl ="1234";

        for (int i=0; i< l.length (); i++)
        {
            char nun = l.charAt(i);
            if ( vergl.charAt(0) == nun )
                perm = verkn(perm,P1);
            else
            if ( vergl.charAt(1) == nun)
                perm = verkn(perm,P2);
            else
            if ( vergl.charAt(2) == nun)

```

## A.2 Magma-Algorithmus

```
        perm = verkn(perm,P3);
    else
    if (vergl.charAt(3) == nun)
        perm = verkn(perm,P4);
    }
    return perm;
}

/* Testet ob ein Element von Gamma(2) in der Untergruppe ist.
 * Dabei muss das Element als String in 1,2,3,4 gegeben werden,
 * wobei 1 und 2 die Erzeuger von Gamma(2)
 * repraesentieren und 3 bzw. 4 ihre Inversen.
 */
public static boolean inUG (String a)
{
    boolean drin = false;
    if (bild(a)[4]==5) drin=true;
    return drin;
}

public static void main (String arg[]) throws IOException
{
    // Einlesen von der Konsole
    String zeile;
    BufferedReader stdin =
        new BufferedReader(new InputStreamReader( System.in ) );
    System.out.println("Geben Sie Ihren Input ein:");
    zeile = stdin.readLine();
    boolean wasis= inUG(zeile);
    System.out.println(wasis);
}
}
```

## A.2 Magma-Algorithmus

An dieser Stelle ist der vollständige Programmcode der Magma-Implementierung des Algorithmus 3 von Seite 54 zu sehen. Der Programmtext ist nur minimal erläutert. Wie der Algorithmus prinzipiell funktioniert, wurde in den vorhergehenden Kapiteln 3.3, 4.5 und 4.6 ausführlich erklärt.

Beschreibungen der einzelnen verwendeten Befehle finden sich im Magma-Handbuch, das auf der Homepage von [Co] zu finden ist.

```
/* In die naechsten Zeilen muessen die benoetigten
 * Daten eingegeben werden.
 */
```

## A Anhang

```
cmin:=1;      //Koeffizienten
cmax:=100;
j:=1;        //Spitzen
k:=6;
bj:=2;       //Breiten
bk:=2;

datei:= "Sp16K100";

P:=Sym(5);
p1:=P!(1,2,3,5); //Bild des 1. Erzeugers von Gamma2
p2:=P!(1,2,3,4); //Bild des 2. Erzeugers von Gamma2
stab:=5;

/* Nun folgen Definitionen und eine Prozedur,
 * die das Bild eines Wortes berechnet.
 */

G2:=CongruenceSubgroup(2);

Koeffs:=[0: i in [1..(cmax+2)]];

bild:=function(w)
  p:=P!1;
  for i:=0 to #w-1 do
    if w[#w-i] eq 1 then
      p:= p*p1;
    elif w[#w-i] eq 2 then
      p:=p*p2^(-1);
    elif w[#w-i] eq -1 then
      p:=p*p1^(-1);
    elif w[#w-i] eq -2 then
      p:=p*p2;
    end if;
  end for;
return p;
end function;

F:= Open("/u/posingie/Belyi/JavaMagma/3Versuch/Daten/"\
         *datei, "w");
fprintf F, "Die Koeffizienten \n";
```

## A.2 Magma-Algorithmus

```

// Die Matrizen fuer die Konjugation werden erstellt.

if j ne -1 then
    Gj:=Matrix(IntegerRing(), 2,2, [j,-1,1,0]);
    else
    Gj:=Matrix(IntegerRing(), 2,2, [1,0,0,1]);
end if;
if k ne -1 then
    Gk:=Matrix(IntegerRing(), 2,2, [0,1,-1,k]);
    else
    Gk:=Matrix(IntegerRing(), 2,2, [1,0,0,1]);
end if;

// Der Fall d=0 wird behandelt.

for m:=0 to bj-1 do
for n:=0 to bk-1 do

    evtl:=Matrix(IntegerRing(), 2,2, [0,-1,1,0]);
    Mm:=Matrix(IntegerRing(), 2,2, [1,m,0,1]);
    Mn:=Matrix(IntegerRing(), 2,2, [1,n,0,1]);
    weiter:=Gj*Mm*evtl*Mn*Gk;

    if weiter[1][1] mod 2 eq 1 and\
       weiter[1][2] mod 2 eq 0 and\
       weiter[2][1] mod 2 eq 0 and\
       weiter[2][2] mod 2 eq 1 then

        g:=G2![weiter[1][1], weiter[1][2],\
               weiter[2][1], weiter[2][2]];
        wi:=FindWord(G2,g);

        if Image(bild(wi),stab) eq stab then
            Koeffs[1]:=Koeffs[1]+1;
        end if;
    end if;
end for;
end for;

// Die geforderten Koeffizienten werden berechnet.

```

## A Anhang

```
for c:=cmin to cmax do
for d:=1 to c-1 do

    if GCD(c,d) eq 1 then
        a:= 0;
        while a*d mod c ne 1 do a:=a+1; end while;
        b:= (a*d-1)/c;
        evtl:=Matrix(IntegerRing(), 2,2, [a,b,c,d]);

        for m:=0 to bj-1 do
        for n:=0 to bk-1 do

            Mm:=Matrix(IntegerRing(), 2,2, [1,m,0,1]);
            Mn:=Matrix(IntegerRing(), 2,2, [1,n,0,1]);
            weiter:=Gj*Mm*evtl*Mn*Gk;

            if weiter[1][1] mod 2 eq 1 and\
               weiter[1][2] mod 2 eq 0 and\
               weiter[2][1] mod 2 eq 0 and\
               weiter[2][2] mod 2 eq 1 then

                g:=G2![weiter[1][1], weiter[1][2],\
                       weiter[2][1], weiter[2][2]];
                wi:=FindWord(G2,g);

                if Image(bild(wi),stab) eq stab then
                    Koeffs[c]:=Koeffs[c]+1;
                end if;
            end if;
        end for;
        end for;
    end if;
end for;
fprintf F, "%o\n", Koeffs[c];
end for;

delete F;

quit;
```

## Software

**Java:** Java 2

**Magma:** Magma V2.10-17

**Maple:** Version 10

**Mathematica:** Mathematica 5

**Pari:** Pari/GP, integriert in das online SAGE Notebook:

<http://sage.math.washington.edu:8100/> (Stand Dezember 2006)

## Literatur

- [Be] *G. V. Belyĭ*: Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.* **43** (1979), 267–276, 479.
- [Bi] *B. Birch*: Noncongruence subgroups, covers and drawings. *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*. London Math. Soc. Lecture Note Ser. **200**. Cambridge Univ. Press, Cambridge, 1994, 25–46.
- [Bo] *J.-B. Bost*: Introduction to compact Riemann surfaces, Jacobians, and abelian varieties. *From number theory to physics (Les Houches, 1989)*. Springer, Berlin, 1992, 64–211.
- [Co] *Computational Algebra Group*: Magma on-line help. University of Sydney, <http://magma.maths.usyd.edu.au/>, 2006.
- [Cr] *J. E. Cremona*: Algorithms for modular elliptic curves. Second ed.. Cambridge University Press, Cambridge, 1997.
- [DD] *R. Douady, A. Douady*: Algèbre et théories galoisiennes. Cassini, Paris, 2005.
- [El1] *N. D. Elkies*: ABC implies Mordell. *International Mathematics Research Notices* **1991** (1991), 99–109.

- [El2] *R. Elkik*: Le théorème de Manin-Drinfel'd. Astérisque (1990), 59–67, Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).
- [Gr] *A. Grothendieck*: Esquisse d'un programme. Geometric Galois actions, 1. London Math. Soc. Lecture Note Ser. **242**. Cambridge Univ. Press, Cambridge, 1997, 5–48, With an English translation on pp. 243–283.
- [He] *D. A. Hejhal*: The Selberg trace formula for  $\mathrm{PSL}(2, \mathbf{R})$ . Vol. 2. Lecture Notes in Mathematics **1001**. Springer-Verlag, Berlin, 1983.
- [Iw] *H. Iwaniec*: Spectral methods of automorphic forms. Second ed.. Graduate Studies in Mathematics **53**. American Mathematical Society, Providence, RI, 2002.
- [Ja] *Java*: Standard Edition Documentation. Sun Microsystems, Inc., <http://java.sun.com/j2se/1.4.2/docs/api/index.html>, 2006.
- [JS] *G. Jones, D. Singerman*: Belyi functions, hypermaps and Galois groups. Bull. London Math. Soc. **28** (1996), 561–590.
- [Kn] *A. W. Knap*: Elliptic curves. Mathematical Notes **40**. Princeton University Press, Princeton, NJ, 1992.
- [KS] *L. Khadjavi, V. Scharaschkin*: Belyi Maps and Elliptic Curves. <http://myweb.lmu.edu/lkhadjavi/>.
- [Ku1] *T. Kubota*: Elementary theory of Eisenstein series. Halstad Press, New York, 1973.
- [Kü2] *U. Kühn*: Néron-Tate heights on algebraic curves and subgroups of the modular group. Manuscripta Math. **116** (2005), 401–419.
- [La] *K. Lamotke*: Riemannsche Flächen. Springer-Verlag, Berlin, 2005.
- [Li] *R. Ličcanu*: Propriétés du degré des morphismes de Belyi. Monatsh. Math. **142** (2004), 327–340.
- [LZ] *S. Lando, A. Zvonkin*: Graphs on Surfaces and Their Applications. Encyclopedia of Mathematical Sciences **141**. Springer-Verlag, Berlin, 2004.

- [Ma] *B. Mazur*: Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44** (1978), 129–162.
- [MR] *V. K. Murty, D. Ramakrishnan*: The Manin-Drinfel'd theorem and Ramanujan sums. *Proc. Indian Acad. Sci. Math. Sci.* **97** (1987), 251–262 (1988).
- [Si] *J. H. Silverman*: The arithmetic of elliptic curves. Graduate Texts in Mathematics **106**. Springer-Verlag, 1986.
- [Ve] *A. B. Venkov*: On essentially cuspidal noncongruence subgroups of  $\mathrm{PSL}(2, \mathbf{Z})$ . *J. Funct. Anal.* **92** (1990), 1–7.
- [vP] *A. von Pippich*: Elliptische Eisensteinreihen. Diplomarbeit. Humboldt Universität zu Berlin, 2005.
- [Wo] *J. Wolfart*: Kinderzeichnungen und Uniformisierungstheorie. <http://www.math.uni-frankfurt.de/wolfart/wolfart.html>.



## Abbildungsverzeichnis

1	Addition auf einer elliptischen Kurve . . . . .	11
2	Fundamentalebene zu $\Gamma(1)$ . . . . .	14
3	Fundamentalebene zu $\Gamma(2)$ . . . . .	15
4	Ein Dessin auf der Ebene . . . . .	24
5	Graph auf der Ebene . . . . .	31
6	Bestandteile des Dessins zu $(E, \beta)$ . . . . .	32
7	Dessin zu $A: \sigma_1 = (1235)$ . . . . .	32
8	Dessin zu $B: \sigma_1 = (1523)$ . . . . .	33
9	Dessin zu $C: \sigma_1 = (1253)$ . . . . .	33
10	Dessin zu $(E, \beta)$ auf dem Torus . . . . .	35
11	Dessin zu $(C_1, \beta_{C_1})$ . . . . .	58
12	Dessin zu $(C_2, \beta_{C_2})$ . . . . .	60

## Tabellenverzeichnis

1	Mögliche Permutationen zu $(E, \beta)$ . . . . .	32
2	Koeffizienten zu $\Gamma(2)$ . . . . .	47
3	Koeffizienten zu $(E, \beta)$ . . . . .	56
4	Koeffizienten zu $(C_1, \beta_{C_1})$ . . . . .	59
5	Koeffizienten zu $(C_2, \beta_{C_2})$ . . . . .	61
6	Koeffizienten zu $G$ . . . . .	64
7	Summen zur Höhenberechnung von $P = (1, 4)$ . . . . .	94
8	modifizierte Summen zur Höhenberechnung von $P = (1, 4)$ . . . . .	95
9	Näherung an die Koeffizienten von $\varphi_{00}^{\Gamma_E}$ . . . . .	97



## Thesen

Belyi-Morphismen geben einen Zusammenhang zwischen über  $\overline{\mathbb{Q}}$  definierten algebraischen Kurven und nicht-holomorphen Eisensteinreihen zu Untergruppen  $\Gamma$  von  $SL_2(\mathbb{Z})$ . In der vorliegenden Arbeit wurden mehrere Aspekte in diesem Themenkreis behandelt.

**Belyi-Morphismen zu elliptischen Kurven:** Für elliptischen Kurven  $E$  wurde eine Konstruktion von Belyi-Morphismen, d.h Morphismen  $\beta : E \rightarrow \mathbb{P}^1$ , die nur über  $0, 1, \infty$  verzweigt sind, unter Einbeziehung von rationalen Punkten der Kurve durchgeführt (Satz 2.11):

Für eine elliptische Kurve  $E$  definiert über  $\mathbb{Q}$  affin gegeben durch  $y^2 = x^3 + Ax + B$  mit  $A, B \in \mathbb{Z}$  und einer endlichen Menge  $P = \{P_1, \dots, P_r\}$  von Punkten aus  $E(\mathbb{Q})$  gibt einen einfach zu konstruierenden Belyi-Morphismus  $\beta$  mit der Eigenschaft, dass  $P \subset \beta^{-1}\{0, 1, \infty\}$ .

Für den Grad dieses Morphismus' gilt

$$\deg(\beta) \leq \left( K \cdot \max_{i=1 \dots r} H(P_i)^4 \right)^{(r+2)(r+5)},$$

wobei

$$K = \max(4A^3, 3^4|B| + |\Delta_E|)$$

mit  $\Delta_E = 4A^3 + 27B^2$  und  $H\left(\left(\frac{p}{q}, \frac{s}{t}\right)\right) = \max(|s|, |t|)$ .

**Die elliptische Kurve  $E : y^2 = x^3 + 5x + 10$ :** Zur Bestimmung einer Untergruppe  $\Gamma \subset \Gamma(2)$  zu einem Belyi-Paar gibt es einen theoretischen Algorithmus. Praktisch ist das Vorgehen im allgemeinen aber nicht auszuführen. In Einzelfällen lässt sich die Gruppe aber bestimmen (Satz 3.10):

Zu dem Belyi-Paar

$$E : y^2 = x^3 + 5x + 10, \quad \beta(x, y) = \frac{y(x-5) + 16}{32}$$

ist die assoziierte Gruppe  $\Gamma_E \subset \Gamma(2)$  gegeben durch den Morphismus

$$\begin{aligned} \varphi_E : \Gamma(2) &\longrightarrow S_5 \\ \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} &\longmapsto (1235) \\ \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix} &\longmapsto (1234) \end{aligned}$$

als

$$\Gamma_E = \{\gamma \in \Gamma(2) \mid \varphi_E(\gamma) \in \text{Stab}(5)\}.$$

**Ein Algorithmus zur Berechnung der Streumatrix:** Ein wesentliches Ergebnis dieser Arbeit ist ein Algorithmus zur Berechnung der Koeffizienten von Streumatrizen (Kapitel 4.4 und 4.5):

Seien  $\Gamma \subset \Gamma(1)$  eine Untergruppe von endlichem Index,  $S_j$  und  $S_k$  zwei nicht notwendigerweise verschiedene Spitzen von  $\Gamma$  mit Spitzenbreiten  $b_j$  und  $b_k$ . Der Zahl  $r_{jk}(c)$  ist der  $c$ -te Koeffizient in der  $L$ -Reihe, die den Eintrag der Streumatrix zu den Spitzen  $S_j$  und  $S_k$  definiert.

Um  $r_{jk}(c)$  zu erhalten, genügt es, alle Matrizen aus

$$\mathcal{M}_c = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & * \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid 0 \leq a, d < c; \text{ggT}(c, d) = 1; \right. \\ \left. ad \equiv 1 \pmod{c}; 0 \leq m < b_j; 0 \leq n < b_k \right\}.$$

dahingehend zu testen, ob sie in  $\gamma_j^{-1}\Gamma\gamma_k$  liegen, denn es gilt (Satz 4.17):

$$r_{jk}(c) = \# \{ \gamma \in \mathcal{M}_c \mid \gamma \in \gamma_j^{-1}\Gamma\gamma_k \}$$

Damit ist die Berechnung eines Koeffizienten auf einen endlichen Test reduziert. Der Algorithmus 3 auf Seite 54 führt diesen Test für Gruppen  $\Gamma$  gegeben durch Permutationen aus. So wird  $r_{jk}(c)$  berechnet. Die Zahlen, die der Algorithmus für eine Reihe von Beispielen lieferte, sind in den Tabellen 2 bis 6 in Kapitel 4 zu sehen. So lieferte der Algorithmus für die Gruppe  $\Gamma_E$  bezüglich der Spitzen 0 und 3 folgende Reihe:

$$\varphi_{03}^{\Gamma_E}(s) = \frac{1}{64^s} \left( \frac{3}{1^{2s}} + \frac{6}{3^{2s}} + \frac{16}{5^{2s}} + \frac{18}{7^{2s}} + \frac{18}{9^{2s}} + \frac{34}{11^{2s}} + \frac{38}{13^{2s}} + \frac{28}{15^{2s}} + \frac{50}{17^{2s}} + \dots \right)$$

**Eigenschaften der Streumatrix:** Die Rechenergebnisse erlauben eine Reihe von Beobachtungen zu Streumatrizen und motivierten einige Untersuchungen. Es konnte einiges gezeigt werden.

- Jeder zweite Koeffizient in den Einträgen der Streumatrix ist null (Satz 5.2).
- Für die Summe der Koeffizienten zu einer Spitze gilt (Satz 5.22):

$$\frac{1}{b_k} \sum_{S_j \in S} r_{jk}(c) = \phi(c).$$

Damit ist die Summe unabhängig von Spitze und Gruppe.

- Für Untergruppen  $\Gamma' \subset \Gamma \subset \Gamma(1)$  von endlichem Index gelten Relationen zwischen den Koeffizientenfunktionen (Satz 5.21):

$$\frac{1}{b_{k'}} \sum_{i=1}^r r_{ji k'}^{\Gamma'}(c) = \frac{1}{b_k} r_{jk}^{\Gamma}(c) \quad \forall c \in \mathbb{N},$$

wobei  $S_j = \bigcup_{i=1}^r S_{ji}$  und  $S_{k'} \subset S_k$ .

- Eine Abschätzung für die Größe der Koeffizienten (Satz 5.26). Insbesondere wachsen die Koeffizienten höchstens linear.
- Ist der Belyi-Morphismus an einer Stelle total verzweigt, so hat die Streumatrix Einträge der Form (Satz 5.31)

$$\pi^{1/2} \frac{\Gamma(s-1/2)}{\Gamma(s)} \cdot \frac{1}{a^s} \sum_{c>0} \chi_2(c+\iota) \frac{b\phi(c)}{c^{2s}},$$

mit leicht bestimmbaren  $a, b \in \mathbb{N}$  und  $\iota \in \{0, 1\}$ .

- Die Summe der Streukonstanten zu einer fixierten Spitze ist immer berechenbar und es gilt (Satz 5.39)

$$\sum_{S_j \in S} b_j C_{jk} + \frac{3}{\pi} \log(b_k) = C^{\Gamma(1)} - \frac{3}{\pi [\Gamma(1) : \Gamma]} \sum_{S_j \in S} b_j \log(b_j),$$

wobei  $C^{\Gamma(1)} = -\frac{6}{\pi} (12\zeta'(-1) - 1 + \log(4\pi)) \approx -2,60811$ .

Darüber hinaus fielen noch eine Reihe weiterer interessanter Dinge auf, die zu beweisen aber den Rahmen dieser Arbeit gesprengt hätten. Dazu gehören, dass unter gewissen Bedingungen die Koeffizienten zu zwei Spitzenpaaren gleich sind und dass immer nur sehr wenige linear unabhängige Koeffizientenfunktionen auftreten.

**Höhenberechnung über Streukonstanten:** Die Höhenpaarung von rationalen Punkten auf elliptischen Kurven kann in einen algebraischen und einen analytischen Anteil zerlegt werden. Der analytischen Anteil ist durch Streukonstanten gegeben und diese lassen sich durch die Koeffizienten  $r_{jk}(c)$  approximieren:

Auf der Kurve  $E : y^2 = x^3 + 5x + 10$  gilt für den analytischen Anteil des rationalen Punktes  $P = (1, 4) \in E(\mathbb{Q})$  (Formel (6.10)):

$$h_{NT}^{analyt}(P, P) \approx 1,14497.$$



## **Selbstständigkeitserklärung**

Ich erkläre, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Berlin, den 16. Februar 2007

Anna Posingies

## **Einverständniserklärung**

Hiermit erkläre ich mich einverstanden, dass ein Exemplar meiner Diplomarbeit in der Bibliothek des Institutes für Mathematik verbleibt.

Berlin, den 16. Februar 2007

Anna Posingies