Die Streumatrix für Untergruppen der Modulgruppe

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

vorgelegt von
Caroline Keil
aus Frankfurt/Main

Dezember 2006

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

Referent: Prof. Dr. Fritz Grunewald
Korreferent: Prof. Dr. Rüdiger Braun
Tag der mündlichen Prüfung: 25. Januar 2007

Zusammenfassung

Die Modulgruppe $\Gamma := \mathrm{PSL}(2,\mathbb{Z})$ der $2\times 2-$Matrizen über $\mathbb{Z}$ mit Determinante 1 operiert auf der oberen Halbebene $\mathbb{H} := \{z = x+iy : x,y \in \mathbb{R}, y > 0\}$. Der Bahnenraum $\Gamma\backslash\mathbb{H}$ ist eine nicht kompakte Riemannsche Fläche und läßt sich durch Hinzunahme der parabolischen Fixpunkte $\mathbb{P}^1(\mathbb{Q})$ kompaktifizieren. Bezüglich der in dieser Arbeit betrachteten Untergruppen $\Delta < \Gamma$ von endlichem Index zerfällt die projektive Gerade in $r < \infty$ Spitzenklassen, so daß wir Δ einen Spitzenvektor $S(\Delta) := [s_1,\ldots,s_r] \in (\mathbb{P}^1(\mathbb{Q}))^r$ als vollständiges Repräsentantensystem der Spitzenklassen zuordnen können und einen kompakten Bahnenraum $\Delta\setminus\mathbb{H}\cup\{s_1,\ldots,s_r\}$ erhalten. Zu jedem Stabilisator $\Delta(s_i)$ eines Repräsentanten $s_i \in \mathbb{P}^1(\mathbb{Q})$ mit Spitzenbreite $w_i := [\Gamma(s_i) : \Delta(s_i)]$ existieren Matrizen $g_i \in \Gamma$ mit $g_i\infty = s_i$ und $g_i^{-1}\Delta(s_i)g_i \subset \Gamma(\infty)$, bzw. $h_i \in \mathrm{PSL}(2,\mathbb{R})$ mit $h_i\infty = s_i$ und $h_i^{-1}\Delta(s_i)h_i = \Gamma(\infty)$. Jedem Repräsentanten s_i ordnen wir eine Eisensteinreihe zu:

$$E_i(z,s) := \sum_{\delta\in\Delta(s_i)\backslash\Delta} \mathrm{Im}(h_i^{-1}\delta z)^s,$$

die für $\mathrm{Re}\, s > 1$ absolut konvergiert und $\Delta-$automorph ist. Jede dieser Eisensteinreihen $E_i(z,s)$ besitzt eine Fourierentwicklung in der Spitze s_j für $1 \le i,j \le r$, deren konstante Terme:

$$\varphi_{ij}(s) := \pi^{\frac{1}{2}}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\sum_{c\in\mathbb{N}}\frac{1}{(w_iw_j)^s c^{2s}}\left|\left\{\left[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)\right] \in g_i^{-1}\Delta(s_i)g_i \setminus g_i^{-1}\Delta g_j / g_j^{-1}\Delta(s_j)g_j\right\}\right|$$

der Streumatrix $\Phi(\Delta,s) := (\varphi_{ij}(s))_{1\le i,j\le r}$ zusammengefasst werden. Im Rahmen dieser Arbeit in GAP entwickelte Programme berechnen zu einer Untergruppe $\Delta <_f \Gamma$ Repräsentanten der Spitzenklasse, die Spitzenbreiten und die Anzahlen b_{ij} der Doppelnebenklassen.

Für Gruppen $\Delta < \Lambda < \Gamma$ führen wir den Begriff der relativen Spitzenbreite einer Spitze s_i^j von Δ in Λ ein und konstruieren die Streumatrix von Λ aus der Streumatrix von Δ.

Diese Überlegungen ermöglichen ein weites Feld von Anwendungen: Zum Einen erhalten wir die Streumatrix einer Kongruenzuntergruppe Δ aus der Streumatrix ihrer Hauptkongruenzuntergruppe $\Gamma(n)$. Daher bestimmen wir zunächst für $\Gamma(p)$ die Struktur der Streumatrix und geben die Einträge in sehr expliziter Form an, bevor wir die Ergebnisse so weit wie möglich auf beliebige Hauptkongruenzuntergruppen $\Gamma(n)$ übertragen.

Zum Anderen können wir auch für solche Nichtkongruenzuntergruppen Δ, die Untergruppen einer Kongruenzuntergruppe Λ sind und eine oder mehrere übereinstimmende Spitzenklassen haben, die Einträge der Streumatrix zumindest teilweise bestimmen. Dann ergeben sich die zu diesen Spitzenrepräsentanten gehörenden Einträge der Streumatrix von Δ aus der Streumatrix von Λ.

Kenntnisse der Struktur der Streumatrix von $\Gamma(p)$ ermöglichen uns auch, die Determinante $\det\Phi(\Gamma(p),s)$ als Quotient von Produkten aus der Riemannschen $\zeta-$Funktion und Dirichletschen L-Reihen zu bestimmen.

Abstract

The modular group $\Gamma := \mathrm{PSL}(2,\mathbb{Z})$ of $2 \times 2-$matrices over $\mathbb{Z}$ with determinant 1 operates on the upper half plain $\mathbb{H} := \{z = x + iy : x, y \in \mathbb{R}, y > 0\}$. The set of orbits $\Gamma \setminus \mathbb{H}$ is a non-compact Riemannian manifold, which can be compactified by adding the parabolic fixed points $\mathbb{P}^1(\mathbb{Q})$. Concerning subgroups $\Delta < \Gamma$ of finite index, the projective line decomposes into $r < \infty$ classes of cusps, thus enabling us to choose a vector of cusps $S(\Delta) := [s_1, \ldots, s_r] \in (\mathbb{P}^1(\mathbb{Q}))^r$ as a complet set of inequivalent cusps obtaining a compact set of orbits $\Delta \setminus \mathbb{H} \cup \{s_1, \ldots, s_r\}$. For the stabilizer $\Delta(s_i)$ of a representative $s_i \in \mathbb{P}^1(\mathbb{Q})$ with cusp width $w_i := [\Gamma(s_i) : \Delta(s_i)]$ there exist matrices $g_i \in \Gamma$ with $g_i\infty = s_i$ and $g_i^{-1}\Delta(s_i)g_i \subset \Gamma(\infty)$ as well as $h_i \in \mathrm{PSL}(2,\mathbb{R})$ with $h_i\infty = s_i$ and $h_i^{-1}\Delta(s_i)h_i = \Gamma(\infty)$. To each cusp s_i we asign the corresponding Eisenstein series:

$$E_i(z,s) := \sum_{\delta \in \Delta(s_i)\setminus\Delta} \mathrm{Im}(h_i^{-1}\delta z)^s,$$

which converges absolutely, if $\mathrm{Re}\, s > 1$, and which is $\Delta-$automorph. Each Eisenstein series $E_i(z,s)$ has a Fourier expansion at the cusp s_j for $1 \le i, j \le r$ with the constant terms:

$$\varphi_{ij}(s) := \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{c \in \mathbb{N}} \frac{1}{(w_i w_j)^s c^{2s}} \left| \left\{ \left[\begin{pmatrix} \star & \star \\ c & \star \end{pmatrix} \right] \in g_i^{-1}\Delta(s_i)g_i \setminus g_i^{-1}\Delta g_j / g_j^{-1}\Delta(s_j)g_j \right\} \right|,$$

which are collected in the scattering matrix $\Phi(\Delta, s) := (\varphi_{ij}(s))_{1 \le i,j \le r}$. We developed programms in GAP, which calculate for a subgroup $\Delta <_f \Gamma$ a complete set of inequivalent cusps, their cusp withs and the numbers b_{ij} of double cosets.

For groups $\Delta < \Lambda < \Gamma$ we introduce the notion of a relative cusp width of a cusp s_i^j of Δ with respect to Λ and construct the scattering matrix of Λ from the scattering matrix of Δ.

This concept allows for a wide field of applications: Firstly, we derive the scattering matrix of a congruence subgroup Δ from the scattering matrix of its principle congruence subgroup $\Gamma(n)$. Thus we estimate for $\Gamma(p)$ the structure of the scattering matrix and present their entries in an explicit way, before transfering our results as far as possible to principle congruence subgroups $\Gamma(n)$.

Secondly, we are able to determine the entries of the scattering matrix at least for such non-congruence subgroups, which are subgroups of a congruence subgroup and hold one or more analog cusps classes. Then the entries of the scattering matrix of Δ belonging to these cusps arise from the scattering matrix of Λ.

Knowledge of the structure of the scattering matrix enables us to construct the determinant $\det \Phi(\Gamma(p), s)$ as a quotient of products of the Riemannian $\zeta-$function and Dirichlet L-series.

Inhaltsverzeichnis

Einleitung **I**

Danksagung **IX**

1 Die Modulgruppe und ihre Untergruppen **1**
1.1 Die Modulgruppe und die obere Halbebene 1
1.2 Kongruenzuntergruppen 11
1.3 Ein Algorithmus zur Bestimmung der Kongruenzuntergruppen . 13

2 Eisensteinreihen und die Streumatrix **17**
2.1 Einführung in die Theorie der Eisensteinreihen 17
2.2 Die Einträge der Streumatrix 21
2.3 Ein Beispiel: $\Gamma_0(p)$ 27

3 Die Streumatrix für Gruppen $\Delta < \Lambda < \Gamma$ **37**
3.1 Konstruktion der Streumatrix von Λ aus der Streumatrix von Δ 37
3.2 Die Streumatrix der Modulgruppe 42
3.3 Folgerungen 45

4 Die Streumatrix für Hauptkongruenzuntergruppen $\Gamma(p)$ **51**
4.1 Eine Blockstruktur der Spitzenmenge 53
4.2 Bildungsgesetze zu den einzelnen Blöcken 57
4.2.1 Ein Bildungsgesetz für Spitzen aus der Faser von unendlich 57
4.2.2 Ein Bildungsgesetz für Spitzen aus den übrigen Fasern . 60
4.3 Anordnung der Bildungsgesetze in der Streumatrix 63

5 Die Streumatrix für Hauptkongruenzuntergruppen $\Gamma(n)$ **71**
5.1 Die Gruppen $\Gamma(p^k)$ 72
5.1.1 Bildungsgesetze zu den einzelnen Blöcken 74
5.2 Die Gruppen $\Gamma(n)$ 82
5.2.1 Bildungsgesetze zu den einzelnen Blöcken 84

6 Die Determinante der Streumatrix für $\Gamma(p)$ **87**
6.1 Transformation in eine Matrix kleinerer Dimension 87
6.2 Rücktransformation auf die Matrix der Bildungsgesetze 94

6.3 Reihendarstellungen 103

7 Beobachtungen und Ausblick **115**
7.1 Kongruenzuntergruppen 116
7.1.1 Nochmal $\Gamma_0(p)$ 117
7.2 Nichtkongruenzuntergruppen 120

8 Anhang: Programme **123**
8.1 $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$ erzeugen 123
8.2 Darstellung einer Matrix als Produkt aus Erzeugern von Γ und umgekehrt 123
8.3 Die Spitzenmenge $S(\Delta)$ und den Vektor der Spitzenbreiten $W(\Delta)$ bestimmen 125
8.4 Die Anzahlen b_{ij} berechnen 127
8.5 Bestimmen, ob Δ eine Kongruenzuntergruppe ist 129

Literaturverzeichnis **135**

Einleitung

Die Modulgruppe:

$$\Gamma := \mathrm{PSL}(2,\mathbb{Z}) < \mathrm{PSL}(2,\mathbb{R})$$

der $2 \times 2-$Matrizen über $\mathbb{Z}$ mit Determinante 1 operiert als Fuchssche Gruppe erster Art auf der oberen Halbebene:

$$\mathbb{H} := \{z = x + iy : x, y \in \mathbb{R}, y > 0\}$$

mittels Möbiustransformationen.Vermutlich war Gauss der erste, der diese Gruppe studierte und mit seinen Untersuchungen die klassische Periode der Theorie der automorphen Funktionen begründete, die ein großes Interesse an dieser Theorie hervorrief und in Arbeiten von Klein, Fricke und Poincaré gipfelte.
Einen zweiten Aufschwung erlebte die Theorie der automorphen Funktionen durch einen Artikel von Selberg [Sel56], der den Begriff der automorphen Funktion verallgemeinerte auf Funktionen, die automorph bezüglich einer endlichdimensionalen unitären Darstellung einer diskreten Untergruppe von $\mathrm{PSL}(2,\mathbb{R})$ sind. Unabhängig davon erschien ein Artikel von Maass [Maa49], der ähnliche nicht-analytische automorphe Formen, sogenannte Maass-Wellenformen, definierte. Durch diese Ideen wurden neue, bisher nicht in der Theorie der automorphen Funktionen verwendete Techniken herangezogen und dies führte zu der Spektraltheorie der automorphen Funktionen.

In dieser Arbeit wollen wir spezielle $\Gamma-$automorphe Funktionen untersuchen und geben dazu im ersten Kapitel dieser Arbeit einen Einstieg in die klassische Theorie. Der Bahnenraum $\Gamma \setminus \mathbb{H}$ ist eine nicht kompakte Riemannsche Fläche, die wir folgendermaßen kompaktifizieren können: Wir betrachten die projektiven Geraden $\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{P}^1(\mathbb{R})$, wobei wir $\mathbb{P}^1(\mathbb{Q})$ als die Menge:

$$\mathbb{P}^1(\mathbb{Q}) := \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Q}^2 \setminus \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\} \right\} / \sim .$$

der gekürzten Brüche modulo ± 1 von $\mathbb{Q}^2 \setminus \{(0,0)\}$ modulo der Äquivalenzrelation $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right] :\Longleftrightarrow \exists \lambda \in \mathbb{Q}^\star : \lambda \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] = \left[\begin{smallmatrix} c \\ d \end{smallmatrix}\right]$ auffassen, und $\mathbb{P}^1(\mathbb{R})$ als Rand von $\mathbb{H}$ ansehen. Die Modulgruppe Γ operiert dann in natürlicher Weise auf $\mathbb{P}^1(\mathbb{Q})$ und $\mathbb{P}^1(\mathbb{R})$ und die unipotenten (parabolischen) Elemente aus Γ haben Fixpunkte auf $\mathbb{P}^1(\mathbb{Q})$, die *Spitzen*. Γ permutiert die Menge der Spitzen $\mathbb{P}^1(\mathbb{Q})$ transitiv und

die Vereinigung $\Gamma\backslash\mathbb{H} \cup \{\infty\}$ läß sich mit der horosphärischen Topologie zu einer kompakten Fläche machen. Bezüglich der in dieser Arbeit betrachteten Untergruppen $\Delta < \Gamma$ von endlichem Index zerfällt die projektive Gerade in $r < \infty$ Spitzenklassen, so daß wir Δ einen *Spitzenvektor* $S(\Delta) := [s_1, \ldots, s_r] \in (\mathbb{P}^1(\mathbb{Q}))^r$ als vollständiges Repräsentantensystem der Spitzenklassen zuordnen können und einen kompakten Bahnenraum $\Delta \setminus \mathbb{H} \cup \{s_1, \ldots, s_r\}$ erhalten. Der *Stabilisator*

$$\Delta(s_i) := \mathrm{Stab}_\Delta(s_i) := \{\delta \in \Delta \colon \delta s_i = s_i\}$$

eines Repräsentanten $s_i \in \mathbb{P}^1(\mathbb{Q})$ einer Spitzenklasse von Δ läßt sich durch eine Matrix $g_i \in \Gamma$ mit $g_i\infty = s_i$ in den Stabilisator $\Gamma_\infty = \Gamma(\infty)$ der vollen Modulgruppe einbetten:

$$g_i^{-1}\Delta(s_i)g_i \subset \Gamma_\infty,$$

wobei wir den Index $w_i := [\Gamma(s_i) : \Delta(s_i)]$ als *Spitzenbreite* von s_i definieren und Δ den *Vektor der Spitzenbreiten* $S(\Delta) \in \mathbb{N}^r$ zuordnen. In obiger Inklusion können wir die Gleichheit erreichen, wenn wir statt $g_i \in \Gamma$ eine Matrix aus $h_i \in \mathrm{PSL}(2, \mathbb{R})$ wählen mit $h_i := g_i\hat{w}_i$ für:

$$\hat{w}_i := \begin{pmatrix} \sqrt{w}_i & 0 \\ 0 & \frac{1}{\sqrt{w}_i} \end{pmatrix}.$$

Ein Ziel dieser Arbeit war es, ein Programm zu entwickeln, das zu einer gegebenen Untergruppe $\Delta <_f \Gamma$ den Spitzenvektor $S(\Delta)$ und den Vektor $W(\Delta)$ der Spitzenbreiten bestimmt. Die meisten Programme wurden in GAP (Groups, Algorithms, Programming [GAP]) realisiert, einem frei verfügbaren Computeralgebrasystem mit dem Schwerpunkt Gruppentheorie. Wenn nötig, wurden zusätzliche Programmteile in MAGMA oder Maple implementiert. Die wichtigsten im Rahmen dieser Arbeit entwickelten Programme sind im Anhang angefügt.

Im zweiten Kapitel ordnen wir einer Untergruppe $\Delta <_f \Gamma$ eine Familie von Eisensteinreihen zu, indem wir die *Eisensteinreihe* $E_i(z, s)$ zu einer Spitze s_i für $z \in \mathbb{H}, s \in \mathbb{C}$ definieren als:

$$E_i(z, s) := \sum_{\delta \in \Delta(s_i)\backslash\Delta} \mathrm{Im}(h_i^{-1}\delta z)^s.$$

Die Eisensteinreihen konvergieren absolut für $\mathrm{Re}\, s > 1$ und sind Δ-automorphe Funktionen. Selberg [Sel89, Sel91] hat gezeigt, daß sie eine Fortsetzung auf die ganze obere Halbebene besitzen und über eine Funktionalgleichung $E_i(z, s)$ und $E_i(z, 1-s)$ miteinander in Beziehung setzen, genau wie viele Zetafunktionen. Die Fourierentwicklung der Eisensteinreihe $E_i(z, s)$ in der Spitze s_j ist für $\mathrm{Re}\, s > 1$ ist definiert als:

$$E_i(h_j z, s) = \sum_{m=-\infty}^{\infty} a_{ij,m}(y, s)e^{2\pi imx}$$

mit $a_{ij,m}(y,s) := \int_0^1 E_i(h_j z, s) e^{-2\pi i m x} dx$, die sich in expliziterer Form angeben lassen und für die konstanten Terme der Fourierentwicklung folgende Gestalt haben:

$$a_{ij,0}(y,s) = \delta_{ij} y^s + \varphi_{ij}(s) y^{1-s}$$

mit:

$$\begin{aligned} \varphi_{ij}(s) &= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{\tilde{c}\in\mathbb{R}^+} \frac{1}{\tilde{c}^{2s}} \sum_{d \bmod \tilde{c}\ \left(\begin{smallmatrix}\star & \star\\ \tilde{c} & d\end{smallmatrix}\right)\in h_i^{-1}\Delta h_j} 1 \\ &= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{\tilde{c}\in\mathbb{R}^+} \frac{1}{\tilde{c}^{2s}} \left| \left\{ [\left(\begin{smallmatrix}\star & \star\\ \tilde{c} & \star\end{smallmatrix}\right)] \in \Gamma(\infty) \setminus h_i^{-1}\Delta h_j/\Gamma(\infty) \right\} \right|, \end{aligned}$$

die wir in der *Streumatrix*:

$$\Phi(\Delta, s) := (\varphi_{ij}(s))_{1\le i,j\le r}$$

für $\operatorname{Re} s > 1$ zusammenfassen. Die Streumatrix ist eine symmetrische Matrix, die sich wegen der Fortsetzbarkeit der Eisensteinreihen auf ganz $\mathbb{H}$ fortsetzen läßt und von der Selberg [Sel89, Sel91] gezeigt hat, daß sie folgende Funktionalgleichung erfüllt:

$$\Phi(\Delta, s)\Phi(\Delta, 1-s) = \mathrm{Id}_r.$$

Damit ergibt sich für die Determinate der Streumatrix die Funktionalgleichung:

$$\det(\Phi(\Delta, s)) \det(\Phi(\Delta, 1-s)) = 1.$$

Für $\tilde{c} \in \mathbb{R}^+$ läßt sich die Anzahl der entsprechenden Doppelnebenklassen von Matrizen mit festem Eintrag $\tilde{c}$ links unten:

$$a_{ij}(\tilde{c}) := \left| \left\{ [\left(\begin{smallmatrix}\star & \star\\ \tilde{c} & \star\end{smallmatrix}\right)] \in \Gamma(\infty) \setminus h_i^{-1}\Delta h_j/\Gamma(\infty) \right\} \right|$$

umformulieren zu einer entsprechenden Anzahl über $c \in \mathbb{N}$:

$$b_{ij}(c) := \left| \left\{ [\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \{T^{w_i n} : n \in \mathbb{Z}\} \setminus g_i^{-1}\Delta g_j/\{T^{w_j n} : n \in \mathbb{Z}\} \right\} \right|$$

mit $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und:

$$a_{ij}(\tilde{c}) = \sqrt{w_i}\sqrt{w_j} b_{ij}(c).$$

Ein im Rahmen dieser Arbeit entwickeltes Programm berechnet zu einer beliebigen Untergruppe $\Delta <_f \Gamma$ diese Anzahlen b_{ij} der Doppelnebenklassen und damit die Einträge der Streumatrix bis zu einer beliebigen Grenze.

Im dritten Kapitel konstruieren wir die Streumatrix einer beliebigen Untergruppe $\Lambda <_f \Gamma$ aus der Streumatrix einer Untergruppe $\Delta < \Lambda$. Dazu führen wir den Begriff der *relativen Spitzenbreite* einer Spitze s_i^j von Δ in Λ ein, indem wir

ein Repräsentantensystem der Spitzen von Δ bezüglich eines Repräsentantensystems $S(\Lambda) := [s_1, \ldots, s_{r(\Lambda)}]$ der Spitzen von Λ ein Repräsentantensystem der Spitzen von Δ nach unter Λ äquivalent werdenden Spitzen sortieren:

$$S(\Delta) = [\underbrace{s_1^1 = s_1, s_1^2, \ldots, s_1^{r_1}}_{\sim_\Lambda s_1}, \underbrace{s_2^1 = s_2, s_2^2, \ldots, s_2^{r_2}}_{\sim_\Lambda s_2}, \ldots, \underbrace{s_{r(\Lambda)}^1 = s_{r(\Lambda)}, s_{r(\Lambda)}^2, \ldots, s_{r(\Lambda)}^{r_{r(\Lambda)}}}_{\sim_\Lambda s_{r(\Lambda)}}].$$

Die *relative Spitzenbreite* einer Spitze s_i^j von $\Delta < \Lambda$ in Λ wird definiert als:

$$v_i^j := [\Lambda(s_i^j) : \Delta(s_i^j)].$$

Der bisherige Begriff der Spitzenbreite gibt die relative Spitzenbreite einer Spitze in Bezug auf die ganze Modulgruppe Γ an und wird hier in Bezug auf eine Gruppe $\Lambda < \Gamma$ erweitert. Dann bestimmen wir die Anzahl b_{ik} der Doppelnebenklassen von Λ aus den entsprechenden Anzahlen b_{ik}^{jl} der Doppelnebenklassen von Δ:

1. Satz: *Für $c \in \mathbb{N}$ gilt:*

$$v_i^j b_{ik}(c) = \sum_{l=1}^{r_k} b_{ik}^{jl}(c).$$

Dieser Satz ermöglicht ein weites Feld von Anwendungen:
Für *Kongruenzuntergruppen*, das sind solche Gruppen Δ, die für ein $n \in \mathbb{N}$ eine *Hauptkongruenzuntergruppe*

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod n \right\}$$

enthalten, können wir mit Satz 1 die Streumatrix von Δ durch die Einträge der Streumatrix von $\Gamma(n)$ angeben. Daher untersuchen wir im vierten Kapitel dieser Arbeit die Streumatrix von $\Gamma(p)$ für eine Primzahl p und bestimmen die Einträge der Streumatrix, indem wir zunächst ihre Spitzen nach den Fasern folgender Abbildung anordnen:

$$\begin{aligned} \lambda \colon \ \Gamma(p) \setminus \mathbb{P}^1(\mathbb{Q}) \ &\longrightarrow \ \mathbb{P}^1(\mathbb{F}_p) \\ \overline{\begin{bmatrix} x \\ y \end{bmatrix}} \ &\longmapsto \ \begin{bmatrix} x \\ y \end{bmatrix}_p := \begin{bmatrix} x \bmod p \\ y \bmod p \end{bmatrix} \end{aligned}$$

und anschließend für die Spitzenklassen jeder Faser die Anzahl der Doppelnebenklassen für $c \in \mathbb{N}$ durch einfache Kongruenzen angeben. Wir erhalten so weitreichende Informationen über die Streumatrix. Insbesondere können wir die

Gesetze zur Bestimmung der Anzahl der Doppelnebenklassen aufzählen und damit eine Abbildung konstruieren:

$$F : \Delta \setminus \mathbb{P}^1(\mathbb{Q}) \times \Delta \setminus \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{F}_p/\{\pm 1\},$$

die jeweils zwei Spitzen die Nummer ihres zugehörigen Gesetzes zuordnet.
Im nächsten Kapitel erweitern wir diese Überlegungen in zwei Schritten zunächst auf $\Gamma(p^k)$ für $k \in \mathbb{N}$ und dann auf beliebiges $n \in \mathbb{N}$, indem wir eine ähnliche Abbildung λ konstruieren und für die Elemente ihrer Fasern explizite Bildungsgesetze für die Anzahl der entsprechenden Doppelnebenklassen bestimmen. In anderer Form sind diese Ergebnisse teilweise schon bekannt, so gibt Hejhal [Hej83] allgemeine Formeln für Hauptkongruenzgruppen an, ohne auf die Struktur der Streumatrix näher einzugehen.
Die tiefergehende Kenntniss über die Struktur der Streumatrix ermöglicht uns Untersuchungen ihrer Determinante. In Kapitel 6 zeigen wir diese Überlegungen an dem Beispiel $\Gamma(p)$ zunächst für eine durch spezielle Zuordnungen reduzierte Matrix und übertragen die dabei gefundenen Ergebnisse auf die Streumatrix.

2. Satz: *Die Determinante der Streumatrix von* $\Gamma(p)$ *hat die Gestalt:*

$$\det(\Phi(\Gamma(p), s))$$

$$= G(s)C \left(\frac{p^2 - p^{2s}}{p^{2s} - 1}\right)^{p-1} \left(\frac{p^{2s+1} - 2p + p^2}{p^{2s} - 1}\right)^2 \left(\frac{\zeta(2s-1)}{\zeta(2s)}\right)^{p+1} \left(\prod_{\chi_j \in V} \frac{L_{\chi_j}(2s-1)}{L_{\chi_j}(2s)}\right)^{p+1}$$

wobei das Produkt über alle Charaktere $\chi \in V := \{\chi \in \widehat{\mathbb{F}}_p^\star/\{\pm 1\} : \chi \neq \chi_0\}$ *läuft mit:*

$$G(s) := \left(\pi^{\frac{1}{2}} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)}\right)^{(p+1)\frac{p-1}{2}}$$

und:

$$C \;=\; \begin{cases} \left(\sqrt{p}\; p^{\frac{p-5}{2}}\right)^{p-1} & \text{für } p \equiv 1 \bmod 4 \\ \left(p^{\frac{p-3}{2}}\right)^{p-1} & \text{für } p \equiv 3 \bmod 4 \end{cases}.$$

Für Kongruenzgruppen vermuten wir ausgehend von Satz 1 einfache Formulierungen für die Anzahlen der entsprechenden Doppelnebenklassen, die aber allen bisherigen Beweisversuchen widerstanden haben und von denen wir einige im letzten Kapitel als Vermutungen angeben. Unter anderem vermuten wir für Kongruenzgruppen Δ mit zwei Spitzen unterschiedlicher Breite folgendes Gesetz für die Anzahl der Doppelnebenklassen, durch das die Streumatrix von Δ bereits vollständig beschrieben wird:

3. Vermutung: *Sei Δ eine Kongruenzuntergruppe mit genau zwei Spitzen, Spitzenvektor $S(\Delta) = [s_1 = \infty, s_2 = g_2\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, w_2]$. Dann gilt:*

$$b_{11}(c) = \begin{cases} w_1\varphi(c) & c \equiv 0 \bmod \frac{w_1}{w_2} \\ (w_1 - w_2)\varphi(c) & sonst \end{cases} .$$

Auch für gewisse Typen von Nichtkongruenzuntergruppen können wir die Streumatrix bestimmen, indem wir in Kapitel 3 einige Folgerungen aus Satz 1 herleiten. Erste Beobachtungen dieser Art gibt es von Petersson [Pet82] für Kongruenzuntergruppen mit einer Spitze und allgemeiner von Venkov [Ven81] für sogenannte zykloide Untergruppen, das sind Untergruppen mit genau einer Spitzenklasse, aber nicht notwendig Kongruenzuntergruppen. Wir erweitern dies in Kapitel 3 auf solche Untergruppen Δ von Λ, für die wir das gleiche Repräsentantensystem von Spitzenklassen wählen können:

4. Satz: *Seien $\Delta < \Lambda$ zwei Untergruppen von Γ mit $S(\Delta) = S(\Lambda) = [s_1, \ldots, s_r]$. Die Streumatrix von Δ ergibt sich aus der Streumatrix von Λ durch Multiplikation mit dem Index $[\Lambda : \Delta]$:*

$$\Phi(\Delta, s) = [\Lambda : \Delta]\Phi(\Lambda, s)$$

für $s \in \mathbb{C}$.

Darüberhinaus gibt es weitere Nichtkongruenzgruppen, für die wir mit Satz 1 zumindest Teile der Streumatrix konstruieren können: Sobald eine Spitzenklasse $[s_i]$ von Δ und Λ übereinstimmt, also keine Spitzen von Δ aus dieser Klasse unter Λ zueinander äquivalent werden, lassen sich die Anzahlen der Doppelnebenklassen der $i-$ten Spalte und $i-$ten Zeile der Streumatrix von Δ aus den Anzahlen von Λ bestimmen:

5. Satz: *Seien $\Delta < \Lambda$ Untergruppen von Γ mit zugehörigen Spitzenvektoren $S(\Lambda) := [s_1, \ldots, s_{r(\Lambda)}]$ und*

$$S(\Delta) = [s_1^1 = s_1, s_1^2, \ldots, s_1^{r_1}, s_2^1 = s_2, s_2^2, \ldots, s_2^{r_2}, \ldots, s_{r(\Lambda)}^1 = s_{r(\Lambda)}, s_{r(\Lambda)}^2, \ldots, s_{r(\Lambda)}^{r_{r(\Lambda)}}].$$

Darüberhinaus existiere ein $r_k \in \{r_1, \ldots, r_{r(\Lambda)}\}$ mit $r_k = 1$. Dann ergeben sich für $i \in \{1, \ldots, r(\Lambda)\}$:

$$v_i^j b_{ik}(c) = b_{ik}^{j1}(c).$$

Wenn für eine Nichtkongruenzuntergruppe Δ, die Untergruppe einer Kongruenzuntergruppe Λ ist, eine übereinstimmende Spitzenklasse $[s_i]$ beider Gruppen existiert, sind nach Satz 5 die Anzahlen von Δ in der $i-$ten Zeile und in der $i-$ten Spalte Vielfache der Euler'schen $\varphi-$Funktion. In Kapitel 3 finden sich einige Beispiele solcher Gruppen.

Die Bedeutung dieser Überlegungen können wir an der Determinante der Streumatrix zu einer Gruppe Δ verdeutlichen, die eine analytische Invariante zur Kontrolle der Spektraltheorie des Laplace-Operators von $\mathrm{L}^2(\Delta \setminus \mathbb{H}, \mathbb{C})$ liefert. Dieser Zusammenhang ist in Terras, Band 1 [Ter85] ausführlich dargestellt. Dazu sei für ein $T \in \mathbb{R}^{\geq 0}$:

$$N_\Delta(T) := |\{s \in \mathbb{C} : 0 \leq \mathrm{Im}(s) \leq T, \mathrm{Re}(s) \geq \frac{1}{2}, \det(\Phi(\Delta, s)) = 0\}|.$$

Selberg [Sel89, Sel91] hat gezeigt, daß das Weyl'sche asymptotische Gesetz für die Eigenwerte des Laplace-Operators gilt, falls es zu einem $\epsilon > 0$ eine Konstante $c_\epsilon \in \mathbb{R}^{\geq 0}$ gibt mit:

$$N_\Delta(T) \ll c_\epsilon T^{2-\epsilon}$$

Für Kongruenzgruppen Δ und ein $c \in \mathbb{R}^{\geq 0}$ gilt:

$$N_\Delta(T) \leq c\, T \log T,$$

so daß das Weyl'sche Gesetz immer erfüllt ist. Mit Satz 5 können wir diese Abschätzung jetzt auch für gewisse Nichtkongruenzgruppen beweisen.

Danksagung

Ich danke Herrn Prof. Dr. Fritz Grunewald für das interessante Thema und die Möglichkeit, die Arbeit in seiner Arbeitsgruppe mit aller Unterstützung, aber auch bei weitgehender Freiheit durchführen zu können. Ebenso möchte ich ihm für die anregenden Diskussionen, seine Förderung und sein Interesse am Fortgang dieser Arbeit danken.

Für die freundliche Bereitschaft, sich als Zweitgutachter zur Verfügung zu stellen, und für die vielen Diskussionen und Ratschläge möchte ich mich bei Herrn Prof. Dr. Rüdiger Braun bedanken.

Der Gesellschaft von Freunden und Förderern der Heinrich-Heine-Universität Düsseldorf danke ich für ihre finanzielle Unterstützung, durch die ich einige Wochen an der Universidad Nacional de Córdoba, Argentinien, verbringen konnte. Insbesondere möchte ich Prof. Dr. Roberto Miatello und Dr. Paulo Tirao für das herzliche Willkommen, die interessanten Gespräche und die Einblicke in ein wunderbares Land danken.

Meinen Kollegen Tobias Ebel, Dr. Benjamin Klopsch, Dr. Christian Liedtke, Sarah Maßberg und Evija Ribnere möchte ich für die angenehme Zusammenarbeit und für die Möglichkeiten zu anregenden Diskussionen danken.

Daniel Appel, Dr. Thorsten Oldag und Iris und Dr. Thorsten Warmt danke ich für ihre Korrekturen.

Besonderer Dank gilt meinem Mann Patrick sowie meiner Mutter Sabine und meinen Schwestern Juliane und Marlene für das Verständnis und die Unterstützung, die sie während meiner Promotionszeit immer wieder aufgebracht haben.

1 Die Modulgruppe und ihre Untergruppen

Die Modulgruppe ist eine aus der klassischen Theorie der automorphen Funktionen bestens bekannte Gruppe, die wir in diesem Kapitel zusammen mit ihrer Operation auf der oberen Halbebene kurz vorstellen, um für die spätere Theorie wichtige Begriffe wie Spitzen und deren Breiten einzuführen. Wir geben nur einen Überblick über die hier benötigten Begriffe und Sätze, weitere Informationen, Details und Beweise sind z.B. in den Büchern von Diamond und Shurman [DS05], Koblitz [Kob84] oder Schoeneberg [Sch74] zu finden.

1.1 Die Modulgruppe und die obere Halbebene

Als ein Modell für die *hyperbolische Ebene* verwenden wir die *obere Halbebene* der komplexen Zahlen:

$$\mathbb{H} := \{z = x + iy : x, y \in \mathbb{R}, y > 0\},$$

die eine Riemannsche Mannigfaltigkeit mit der vom Poincaré-Differential abgeleiteten Metrik ist [Iwa02]:

$$ds^2 = \frac{dx^2 + dy^2}{y^2}.$$

Die Gruppe $\mathrm{SL}(2, \mathbb{R})$ der reellen 2×2-Matrizen mit Determinante 1 operiert auf $\mathbb{H}$ mittels so genannter *Möbiustransformationen*: Für ein $g := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{R})$ und einen Punkt $z \in \mathbb{H}$ sei:

$$gz := \frac{az + b}{cz + d}.$$

Dies ist eine Operation auf der oberen Halbebene, da $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{R})$ und $z \in \mathbb{H}$ auch $\operatorname{Im} \gamma z > 0$ impliziert:

$$\operatorname{Im} \gamma z = \operatorname{Im} \frac{az + b}{cz + d} = \operatorname{Im} \frac{(az + b)(c\bar{z} + d)}{|cz + d|^2} = |cz + d|^{-2} \operatorname{Im}(adz + bc\bar{z}).$$

Wegen $\det \gamma = 1$ gilt $\operatorname{Im}(adz + bc\bar{z}) = (ad - bc) \operatorname{Im} z = \operatorname{Im} z$ und:

$$\operatorname{Im} \gamma z = |cz + d|^{-2} \operatorname{Im} z.$$

Die Möbiustransformationen lassen sich auf $x \in \mathbb{R} \cup \{\infty\}$ erweitern:

$$gx := \frac{ax+b}{cx+d} \quad \text{mit} \quad g\,\frac{-d}{c} := \infty \quad \text{und} \quad g\infty := \frac{a}{c}$$

und ergeben meromorphe Funktionen auf:

$$\mathbb{H}^\star := \mathbb{H} \cup \mathbb{R} \cup \{\infty\}\,.$$

Für $c = 0$ ist dies eine ganze Funktion und für $c \neq 0$ hat die Transformation genau einen Pol erster Ordnung bei $z = -d/c$ [Apo76, KK98]. Umgekehrt ist die Transformation $g := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ durch die zugehörige Funktion bis auf das Vorzeichen bestimmt, da die beiden Matrizen $1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und $-1 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ die identische Transformation ergeben. $\mathrm{PSL}(2,\mathbb{R}) := \mathrm{SL}(2,\mathbb{R})/\{\pm 1\}$ operiert also treu auf $\mathbb{H}^\star$. Wir beschäftigen uns hier mit diskreten Untergruppen von $\mathrm{SL}(2,\mathbb{R})$, und zwar mit Untergruppen der Modulgruppe:

$$\Gamma := \mathrm{PSL}(2,\mathbb{Z}),$$

die von zwei Transformationen erzeugt wird:

1.1 Satz: $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$ *wird von den beiden Transformationen*

$$B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : z \longmapsto -\frac{1}{z} \quad \textit{und} \quad S := \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} : z \longmapsto \frac{1}{-z+1}$$

erzeugt.

Damit läßt sich jedes $\gamma \in \Gamma$ darstellen als endliches Produkt in diesen Erzeugern:

$$\gamma = B^{k_1} S^{l_1} B^{k_2} S^{l_2} \cdot \ldots \cdot B^{k_n} S^{l_n}$$

mit $k_i, l_i \in \mathbb{Z}$ für $1 \leq i \leq n$. Die in Büchern über Modulformen, z.B. von Koblitz [Kob84] oder Apostol [Apo76], zu findende Darstellung mit $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und S läßt sich mit $T = S^{-1}B$ entsprechend übertragen [Kei02].
Es gibt eine ganze Reihe von Folgerungen für die möglichen Einträge einer Matrix in Γ, von denen wir hier nur zwei zitieren, deren Beweise in Shimura [Shi71] zu finden sind.

1.2 Satz:

1. *Sei* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. *Dann sind die Einträge spalten- und zeilenweise teilerfremd, es gilt also:*

$$\mathrm{ggt}\ (a,b) = \mathrm{ggt}\ (c,d) = \mathrm{ggt}\ (a,c) = \mathrm{ggt}\ (b,d) = 1.$$

2. *Zwei teilerfremde Zahlen $a, b \in \mathbb{Z}$ lassen sich spalten- oder zeilenweise zu einer Matrix in Γ ergänzen, es existieren also $c_1, c_2, d_1, d_2 \in \mathbb{Z}$ mit*

$$\gamma_1 = \left(\begin{smallmatrix} a & c_1 \\ b & d_1 \end{smallmatrix}\right), \gamma_2 = \left(\begin{smallmatrix} a & b \\ c_2 & d_2 \end{smallmatrix}\right) \in \Gamma.$$

Durch Nachrechnen sehen wir, daß sich aus Teil 2 dieses Satzes weitere Anforderungen an die Einträge der Matrizen formulieren lassen:

1.3 Korollar:

1. *Seien $a, c \in \mathbb{Z}$ mit* ggt $(a, c) = 1$. *Dann existieren zu einer Primzahl p mit $p|c$ ganze Zahlen $b_1, d_1 \in \mathbb{Z}$ mit $p|b_1$ und $\left(\begin{smallmatrix} a & b_1 \\ c & d_1 \end{smallmatrix}\right) \in \Gamma$ und zu einer Primzahl p mit $p|a$ existieren $b_2, d_2 \in \mathbb{Z}$ mit $p|d_2$ und $\left(\begin{smallmatrix} a & b_2 \\ c & d_2 \end{smallmatrix}\right) \in \Gamma$.*

   Insbesondere existieren zu $a, c \in \mathbb{Z}$ mit $a \equiv \pm 1(p)$ und $c \equiv 0(p)$ ganze Zahlen $b, d \in \mathbb{Z}$ mit $b \equiv \pm 1(p), d \equiv 0(p)$ und $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

2. *Seien $a, c \in \mathbb{Z}$ mit* ggt $(a, c) = 1$ *und p eine Primzahl mit $p \nmid a, c$. Dann existieren $b_1, d_1 \in \mathbb{Z}$ mit $p|b_1$ und $\left(\begin{smallmatrix} a & b_1 \\ c & d_1 \end{smallmatrix}\right) \in \Gamma$ und $b_2, d_2 \in \mathbb{Z}$ mit $p|d_2$ und $\left(\begin{smallmatrix} a & b_2 \\ c & d_2 \end{smallmatrix}\right) \in \Gamma$.*

Alle Matrizen in Γ lassen sich folgendermaßen klassifizieren:

1.4 Definition und Satz: *Die Elemente $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma, \gamma \neq 1$ sind entweder parabolisch oder elliptisch oder hyperbolisch. Genauer gilt:*

γ ist parabolisch
$:\Longleftrightarrow \quad |\operatorname{Spur}\gamma| = |a + d| = 2$
$\Longleftrightarrow$ *γ hat genau einen Fixpunkt in $\mathbb{H}^\star$ und dieser liegt auf $\mathbb{R} \cup \{\infty\}$*
$\Longleftrightarrow \quad \exists\ A \in \mathrm{SL}(2, \mathbb{R})$ *mit* $A\gamma A^{-1} = \pm \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ *für* $0 \neq \lambda \in \mathbb{R}$
(und $A^{-1}\gamma$ ist der eindeutig bestimmte Fixpunkt von γ in $\mathbb{H}^\star$).

γ ist elliptisch
$:\Longleftrightarrow \quad |\operatorname{Spur}\gamma| < 2$
$\Longleftrightarrow$ *γ hat genau einen Fixpunkt in $\mathbb{H}$*
$\Longleftrightarrow \quad \exists\ A \in \mathrm{SL}(2, \mathbb{R})$ *mit* $A\gamma A^{-1} = \left(\begin{smallmatrix} \cos(\varphi/2) & \sin(\varphi/2) \\ -\sin(\varphi/2) & \cos(\varphi/2) \end{smallmatrix}\right)$ = *hyperbolische Drehung um den Winkel $\varphi \neq 0$ für $-\pi < \frac{\varphi}{2} < \pi$ und Zentrum i (und A bildet den Fixpunkt von γ nach i ab).*

γ ist hyperbolisch
$:\Longleftrightarrow \quad |\operatorname{Spur}\gamma| > 2$
$\Longleftrightarrow$ *γ hat zwei verschiedene Fixpunkte in $\mathbb{R} \cup \{\infty\}$*
$\Longleftrightarrow \quad \exists\ A \in \mathrm{SL}(2, \mathbb{R})$ *mit* $A\gamma A^{-1} = \pm \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ *für* $\lambda \in \mathbb{R}$, $\lambda > 1$
(und A bildet die Fixpunkte von γ auf 0 und ∞ ab).

Die Fixpunkte von Γ in $\mathbb{H}^\star$ der parabolischen, elliptischen bzw. hyperbolischen Elemente von Γ bezeichnen wir als *parabolische, elliptische* bzw. *hyperbolische*

Fixpunkte von Γ, die parabolischen Fixpunkte werden auch *Spitzen* von Γ genannt. Um zu sehen, daß die Menge der Spitzen der Modulgruppe Γ aus der *projektiven Gerade über* $\mathbb{Q}$ besteht, führen wir mit der Operation von $\mathbb{Q}^\star = \mathbb{Q} \setminus \{0\}$ auf $\mathbb{Q}^2 \setminus \{(0,0)\}$, die für $\lambda \in \mathbb{Q}^\star$ durch $\lambda(a,b) = (\lambda a, \lambda b)$ gegeben ist, auf $\mathbb{Q} \times \mathbb{Q}$ eine Äquivalenzrelation $\sim$ ein:

$$(a,b) \sim (c,d) :\Longleftrightarrow \exists \lambda \in \mathbb{Q}^\star : \lambda(a,b) = (c,d),$$

Die projektive Gerade besteht dann aus den Äquivalenzklassen der gekürzten Brüche modulo ± 1 von $\mathbb{Q}^2 \setminus \{(0,0)\}$:

$$\mathbb{P}^1(\mathbb{Q}) := \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Q}^2 \setminus \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\} \right\} / \sim .$$

Damit liegen Geraden mit betragsmäßig gleicher Steigung in derselben Restklasse, für die wir einen Repräsentanten $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ mit $x, y \in \mathbb{N}_0, y \neq 0$ und ggt $(x,y) = 1$ wählen können und wir nehmen noch die Geraden mit unendlicher Steigung hinzu, für deren Restklasse wir als Repräsentanten $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ wählen.
Die Operation der Gruppe $\mathrm{SL}(2,\mathbb{R})$ auf $\mathbb{P}^1(\mathbb{Q})$ ist für ein $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{R})$ und eine Restklasse $s = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{Q})$ definiert als:

$$gs = g \begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}.$$

Wir sehen, daß diese Operation für Γ äquivalent zu den vorher definierten Möbiustransformationen ist, indem wir die Restklasse durch y kürzen und als Bruch schreiben. Die Operation ist unabhängig von der Wahl des Repräsentanten, da zu zwei Repräsentanten $s_1 = \left[\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right], s_2 = \left[\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}\right]$ derselben Restklasse in $\mathbb{P}^1(\mathbb{Q})$ ein $\lambda \in \mathbb{Q}^\star$ existiert mit $\lambda(x_2, y_2) = (x_1, y_1)$, so daß gs_1 und gs_1 in derselben Restklasse liegen:

$$gs_1 = \begin{bmatrix} ax_1 + by_1 \\ cx_1 + dy_1 \end{bmatrix} = \begin{bmatrix} a\lambda x_2 + b\lambda y_2 \\ c\lambda x_2 + d\lambda y_2 \end{bmatrix} = \lambda g s_2.$$

Mit diesen Vorüberlegungen können wir jetzt alle Spitzen von Γ bestimmen (vergleiche z.B. Shimura [Shi71]):

1.5 Satz: *Die Menge der Spitzen von* Γ *ist gleich* $\mathbb{P}^1(\mathbb{Q})$.

Beweis:
Es ist $\infty = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ ein Fixpunkt des parabolischen Elements $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$.
Ein beliebiges parabolisches Element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ mit $c \neq 0$ hat nach Satz 1.4 nur einen Fixpunkt $s \in \mathbb{R} \cup \{\infty\}$. Wenn s endlich ist, erfüllt es die Gleichung:

$$\frac{as + b}{cs + d} = s \Longleftrightarrow cs^2 + (d - a)s - b = 0.$$

Da die Diskriminante $c(-4bc-(d-a)^2) = c(-(a^2+2ad+d^2)+4(ad-bc))$ verschwindet, besitzt obige Gleichung eine doppelte Nullstelle s, die daher in $\mathbb{Q}$ liegen muß.
Umgekehrt existieren zu $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ mit $a, b \in \mathbb{N}_0$ und ggt $(a,b) = 1$ nach dem euklidischen Algorithmus $c, d \in \mathbb{Z}$ mit $ad - bc = 1$. Dann folgt $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ und $\gamma\infty = \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$. Da das Bild einer Spitze unter Γ wieder eine Spitze ist, sind alle Punkte aus $\mathbb{P}^1(\mathbb{Q})$ Spitzen von Γ. □

Darüber hinaus haben wir hiermit gezeigt, daß alle Spitzen Γ-äquivalent zu der Spitze ∞ sind: Für eine Untergruppe Δ von Γ heißen zwei Elemente $z_1, z_2 \in \mathbb{H}$ Δ-*äquivalent*, in Zeichen $z_1 \sim_\Delta z_2$, wenn ein $\delta \in \Delta$ existiert mit:

$$\delta s_1 = s_2.$$

In der ganzen Modulgruppe sind alle Spitzen zueinander äquivalent und damit folgt $\Gamma\backslash\mathbb{H}^\star = (\Gamma\backslash\mathbb{H}) \cup \{\infty\}$ (vergleiche z.B. [Shi71]). Bezüglich dieser Äquivalenzrelation läßt sich eine Untergruppe Δ der Modulgruppe visualisieren: Eine Teilmenge $F \subset \mathbb{H}$ ist ein *Fundamentalbereich für* Δ, falls F eine zusammenhängende Teilmenge von $\mathbb{H}$ ist mit den Eigenschaften, daß keine zwei Punkte von F zueinander Δ-äquivalent sind und daß jeder Punkt der oberen Halbebene Δ-äquivalent zu einem Punkt aus dem Abschluß von F ist (vergleiche z.B. [Apo76]). Ein typisches Beispiel ist der Fundamentalbereich der vollen Modulgruppe Γ:

$$\mathbb{F} := \left\{ z = x + iy \in \mathbb{H} : |z| > 1 \wedge -\frac{1}{2} < \operatorname{Re} z \leq \frac{1}{2} \text{ oder } |z| = 1 \wedge 0 \leq \operatorname{Re} z \leq \frac{1}{2} \right\}.$$

Allgemein heißt eine diskrete Untergruppe von $\mathrm{PSL}(2,\mathbb{C})$ *Fuchssche Gruppe* und kann mit Matrizen aus $\mathrm{PSL}(2,\mathbb{C})$ zu einer diskreten Untergruppe von $\mathrm{PSL}(2,\mathbb{R})$ konjugiert werden. Jede Fuchssche Gruppe Δ hat einen offensichtlich nicht eindeutig bestimmten Fundamentalbereich [Iwa02], jedoch haben alle Fundamentalbereiche $F(\Delta)$ von Δ das gleiche Volumen. Ein Punkt $z_1 \in \mathbb{H}^\star$ heißt *Grenzpunkt* einer Fuchsschen Gruppe Δ, wenn ein $z \in \mathbb{H}^\star$ und eine Folge $\delta_i \in \Delta$ existieren mit:

$$\lim_{i \longrightarrow \infty} \delta_i z = z_1.$$

Wenn die Menge $L(\Delta)$ dieser Grenzpunkte dem ganzen Rand der oberen Halbebene entspricht, also $L(\Delta) = \partial\mathbb{H}^\star = \overline{\mathbb{R}}$, spricht man von einer Fuchsschen Gruppe *erster Art*. Jede Fuchssche Gruppe erster Art hat eine endliche Anzahl von Erzeugern und einen Fundamentalbereich $F(\Delta)$ von endlichem Volumen $|F(\Delta)|$, der als ein konvexes Polygon gewählt werden kann. Genauer läßt sich zu einem $z_1 \in \mathbb{H}$, das nur Fixpunkt der Identität ist, folgendes *Normalpolygon* als Fundamentalbereich wählen (vergleiche Iwaniec [Iwa02]):

$$D(z_1) := \{ z \in \mathbb{H} : p(z, z_1) < p(z, \delta z_1) \text{ für alle } \delta \in \Delta, \delta \neq 1 \}.$$

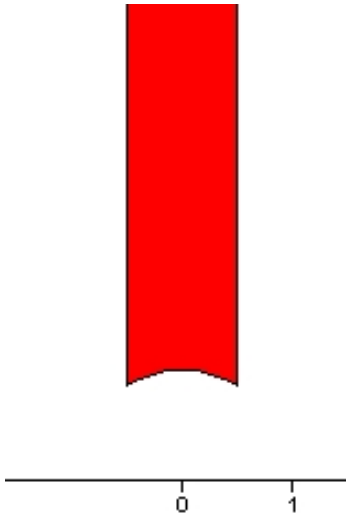

Abbildung 1.1: Fundamentalbereich für Γ

Ein Fundamentalbereich $F(\Delta)$ kann nach Abschluß in $\mathbb{C}^\star$ entweder kompakt sein oder nicht. Im ersten Fall wird Δ als *co-kompakt* bezeichnet. Dann muß $\overline{F(\Delta)}$ einen Punkt auf $\overline{\mathbb{R}}$ enthalten und die Seiten von $F(\Delta)$, die sich in diesem Punkt treffen, sind orthogonal zu $\overline{\mathbb{R}}$ und formen das Bild einer Spitze. Diese Spitzen sind genau die Fixpunkte parabolischer Elemente von Δ[Gun62]. Damit ist eine Fuchssche Gruppe erster Art genau dann nicht co-kompakt, wenn sie mindestens ein parabolisches Element enthält. Die hier betrachteten Untergruppen der Modulgruppe sind nicht co-kompakte Fuchssche Gruppen erster Art. Wir beschäftigen uns im Weiteren mit Untergruppen $\Delta < \Gamma$ von endlichem Index, die daher nur endlich viele Δ-Äquivalenzklassen von Spitzen besitzen [Shi71].

1.6 Definition: *Zu einer Untergruppe Δ von Γ mit endlichem Index sei $r := r(\Delta)$ die Anzahl der Δ-inäquivalenten Spitzen und:*

$$S_\Delta := \Delta \backslash \mathbb{P}^1(\mathbb{Q})$$

die Menge der Δ-Äquivalenzklassen der Spitzen mit dem Spitzenvektor:

$$S(\Delta) := [s_1, \ldots, s_r] \in (\mathbb{P}^1(\mathbb{Q}))^r$$

als ein vollständiges Repräsentantensystem.

Da eine dieser Äquivalenzklassen die Spitze ∞ enthalten muß, können wir $S(\Delta)$ gegebenenfalls so wählen, daß $s_1 = \infty$ der Repräsentant dieser Klasse ist.

1.7 Definition: *Für ein $s \in \mathbb{P}^1(\mathbb{Q})$ sei*

$$\mathrm{Stab}_\Delta(s) := \Delta(s) := \Delta_s := \{\delta \in \Delta \colon \delta s = s\}$$

der Stabilisator von s in Δ.

Das wichtigste Beispiel ist der Stabilisator Γ_∞ der vollen Modulgruppe:

$$\Gamma_\infty = \Gamma(\infty) = \{T^n \colon n \in \mathbb{Z}\} \text{ mit } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

der mit den Stabilisatoren der anderen Spitzen in folgendem Zusammenhang steht: Zu einer Spitze $s_i = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{Q})$ von Δ und zugehörigem Stabilisator $\Delta(s_i)$ existiert eine Matrix $g_i = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}(2,\mathbb{Z})$, so daß $g_i\infty = s_i$, da alle Elemente aus $\mathbb{P}^1(\mathbb{Q})$ Γ-äquivalent sind. Die erste Spalte von g_i ist eindeutig bestimmt:

$$g_i s_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \Longleftrightarrow a = x \wedge c = y.$$

Da ggt $(x, y) = 1$ ist, existieren nach dem euklidischen Algorithmus $b, d \in \mathbb{Z}$ mit

$$dx - by = 1 = \det g_i.$$

Die zweite Spalte von g_i ist nicht eindeutig bestimmt, da neben $b, d \in \mathbb{Z}$ auch $d + ny, b + nx$ für $n \in \mathbb{Z}$ die Gleichung erfüllen. Insgesamt ist g_i also bis auf Translation von rechts mit T^n eindeutig bestimmt und es folgt:

$$g_i^{-1}\Delta(s)g_i \subset \Gamma_\infty,$$

da sich der Stabilisator der vollen Modulgruppe zur Spitze s_i folgendermaßen umformen läßt:

$$\begin{array}{rcccccl} \Gamma(s_i) & = & \Gamma(g_i\infty) & = & \left\{\gamma \in \Gamma : g_i^{-1}\gamma g_i\infty = \infty\right\} & = & \left\{\gamma \in \Gamma : g_i^{-1}\gamma g_i \in \Gamma_\infty\right\} \\ & & & = & \left\{\gamma \in \Gamma : \gamma \in g_i\Gamma_\infty g_i^{-1}\right\} & = & g_i\Gamma_\infty g_i^{-1} \\ & & & = & \left\{g_i T^n g_i^{-1} : n \in \mathbb{Z}\right\}. & & \end{array}$$

Da $\Delta(s_i) = \Gamma(s_i) \cap \Delta \leq \Delta$ und $\Delta \leq_f \Gamma$, existiert

$$w_i := \min\left\{n \in \mathbb{N} : g_i T^n g_i^{-1} \in \Delta\right\}$$

und damit gilt:

$$\Delta(s_i) = g_i \left\{T^{w_i n} : n \in \mathbb{Z}\right\} g_i^{-1}.$$

Dieses Minimum bezeichnen wir als die *Spitzenbreite* der Spitze s_i. Spitzen derselben Äquivalenzklasse aus S_Δ haben die gleiche Spitzenbreite, so daß diese Definition unabhängig von der Wahl des Repräsentanten s_i ist:

1.8 Lemma:
Sei $s_1 \in \mathbb{P}^1(\mathbb{Q})$ Spitze von Δ der Breite w_1 und $s_2 \in \mathbb{P}^1(\mathbb{Q})$ mit $s_1 \sim_\Delta s_2$. Dann ist auch s_2 Spitze von Δ der Breite w_1.

Beweis:
Die Spitze s_2 habe die Breite w_2. Wir wählen für s_1, s_2 Matrizen $g_1, g_2 \in \Gamma$ mit $g_1\infty = s_1, g_2\infty = s_2$ und ein $\delta \in \Delta$ mit $s_1 = \delta s_2$. Dann gilt:

$$\Delta(s_1) = g_1 \left\{T^{w_1 n} : n \in \mathbb{Z}\right\} g_1^{-1}$$

und wegen $g_2 = \delta^{-1} g_1$ ergibt sich:

$$\Delta(s_2) = g_2 \left\{T^{w_2 n} : n \in \mathbb{Z}\right\} g_2^{-1} = \delta^{-1} g_1 \left\{T^{w_2 n} : n \in \mathbb{Z}\right\} g_1^{-1} \delta \subset \Delta.$$

Damit gilt auch $g_1 \left\{T^{w_2 n} : n \in \mathbb{Z}\right\} g_1^{-1} \subset \Delta$ und wir erhalten:

$$w_2 = w_1 = \min\left\{n \in \mathbb{N} : g_1 T^n g_1^{-1} \in \Delta\right\}.$$

□

Die Definition der Spitzenbreite ist offensichtlich unabhängig von der Wahl der g_i, da g_i bis auf Translation von rechts mit T^n eindeutig bestimmt ist und sich daher dieselben Stabilisatoren ergeben.

1.9 Definition: *Einer Untergruppe Δ von Γ mit endlichem Index und Spitzenvektor $S(\Delta) = [s_1, \ldots, s_r] \in (\mathbb{P}^1(\mathbb{Q}))^r$ ordnen wir den Vektor der Spitzenbreiten zu:*

$$W(\Delta) := [w_1, \ldots, w_r] \in \mathbb{N}^r.$$

Für die Breite w_i einer Spitze $s_i \in S_\Delta$ und zugehöriger Matrix $g_i = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}(2, \mathbb{Z})$ mit $g_i\infty = s_i$ gilt:

$$g_i^{-1} \Delta(s_i) g_i = \{T^{w_i n} : n \in \mathbb{Z}\} \subset \Gamma(\infty).$$

Im Allgemeinen gilt in der letzten Inklusion noch keine Gleichheit, wir können sie aber erreichen, wenn wir statt $g_i \in \Gamma$ eine Matrix aus $\mathrm{PSL}(2, \mathbb{R})$ wählen: Sei:

$$\hat{w}_i := \begin{pmatrix} \sqrt{w}_i & 0 \\ 0 & \frac{1}{\sqrt{w_i}} \end{pmatrix}$$

und $h_i := g_i \hat{w}_i \in \mathrm{PSL}(2, \mathbb{R})$. Indem wir die Gruppenoperation entsprechend auf reelle Zahlen erweitern, folgt:

$$h_i\infty = g_i \hat{w}_i \begin{bmatrix} 1 \\ 0 \end{bmatrix} = g_i \begin{bmatrix} \sqrt{w_i} \\ 0 \end{bmatrix} = g_i \begin{bmatrix} 1 \\ 0 \end{bmatrix} = s_i$$

und wir erhalten:

$$\begin{aligned} h_i^{-1}\Delta(s)h_i &= \begin{pmatrix} \frac{1}{\sqrt{w_i}} & 0 \\ 0 & \sqrt{w_i} \end{pmatrix} g_i^{-1}\Delta(s)g_i \begin{pmatrix} \sqrt{w_i} & 0 \\ 0 & \frac{1}{\sqrt{w_i}} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{\sqrt{w_i}} & 0 \\ 0 & \sqrt{w_i} \end{pmatrix} \left\{ \begin{pmatrix} 1 & w_i n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\} \begin{pmatrix} \sqrt{w_i} & 0 \\ 0 & \frac{1}{\sqrt{w_i}} \end{pmatrix} \\ &= \{T^n : n \in \mathbb{Z}\} = \Gamma_\infty. \end{aligned}$$

Damit haben wir folgenden Satz hergeleitet:

1.10 Satz: *Zu jeder Spitze $s_i \in S(\Delta)$ existiert ein $g_i \in \Gamma$ mit:*

1. $g_i\infty = s_i$
2. $g_i^{-1}\Delta(s_i)g_i = \{T^{w_i n} : n \in \mathbb{Z}\}$

Dabei ist g_i bis auf Multiplikation von rechts mit T^n für $n \in \mathbb{Z}$ eindeutig bestimmt und mit $h_i := g_i\hat{w}_i \in \mathrm{PSL}(2,\mathbb{R})$ gilt

$$h_i^{-1}\Delta(s_i)h_i = \Gamma(\infty).$$

Die Spitzenbreite ist invariant bezüglich Konjugation, so daß zueinander konjugierte Untergruppen insgesamt die gleichen Spitzenbreiten haben, diese Breiten aber bei jeder Untergruppe anderen Spitzenklassen zugeordnet sein können:

1.11 Lemma: *Sei $s_1 \in \mathbb{P}^1(\mathbb{Q})$ Spitze von Δ der Breite w_1 und $\gamma \in \Gamma$. Dann ist γs_1 Spitze von $\gamma\Delta\gamma^{-1}$ der Breite w_1.*

Beweis:
Da s_1 Spitze von Δ ist, existieren ein parabolisches $\delta \in \Delta$ mit $\delta s_1 = s_1$ und $|\operatorname{Spur}\delta| = 2$ und ein $g_1 \in \Gamma$ mit $g_1\infty = s_1$ nach Satz 1.10. Dann folgt $\gamma\delta\gamma^{-1} \in \gamma\Delta\gamma^{-1}$ mit $\gamma\delta\gamma^{-1}\gamma s_1 = \gamma s_1$ und $|\operatorname{Spur}\gamma\delta\gamma^{-1}| = 2$, da die Spur invariant bezüglich Konjugation ist. Wie im Beweis von Lemma 1.8 sehen wir, daß die Spitzenbreite w_2 von γs_1 gleich der Breite von s_1 ist, da $\Delta(\gamma s_1) = \gamma g_1 \{T^{w_2 n} : n \in \mathbb{Z}\} g_1^{-1}\gamma^{-1}$ und damit folgt:

$$g_1 \{T^{w_2 n} : n \in \mathbb{Z}\} g_1^{-1} \subset \Delta \text{ und } w_2 = w_1.$$

□

Die Breite einer Spitze entspricht offensichtlich dem Index des zugehörigen Stabilisators:

1.12 Lemma: *Sei Δ eine Untergruppe von Γ mit endlichem Index, Spitzenvektor $S(\Delta) = [s_1, \ldots, s_r]$ und Spitzenbreiten $W(\Delta) = [w_1, \ldots, w_r]$. Dann gilt für alle $i \in \{1, \ldots, r\}$:*

$$[\mathrm{Stab}_\Gamma(s_i) : \mathrm{Stab}_\Delta(s_i)] = w_i.$$

Beweis:
Nach Satz 1.10 existieren zu den Spitzen s_i Matrizen $g_i = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}(2,\mathbb{Z})$ mit $g_i\infty = s_i$ und mit diesen Matrizen erhalten wir hier:

$$\begin{array}{rclcl} \mathrm{Stab}_\Gamma(s_i) & = & \mathrm{Stab}_\Gamma(g_i\infty) & = & \{\gamma \in \Gamma : \gamma g_i\infty = g_i\infty\} \\ & = & \{\gamma \in \Gamma : g_i^{-1}\gamma g_i\infty = \infty\} & = & \{\gamma \in \Gamma : g_i^{-1}\gamma g_i \in \Gamma_\infty\} \\ & = & g_i \,\mathrm{Stab}_\Gamma(\infty) g_i^{-1} & = & \{g_i T^n g_i^{-1} : n \in \mathbb{Z}\} \end{array}$$

und

$$\mathrm{Stab}_\Delta(s_i) \;=\; \mathrm{Stab}_\Gamma(g_i\infty) \cap \Delta \;=\; \{g_i T^{w_i n} g_i - 1 : n \in \mathbb{Z}\}\,.$$

Insgesamt

$$\begin{array}{rcl} \mathrm{ord}(\mathrm{Stab}_\Gamma(s_i)/\,\mathrm{Stab}_\Delta(s_i)) & = & \mathrm{ord}(\{g_i T^n g_i^{-1} : n \in \mathbb{Z}\} \,/\, \{g_i T^{w_i n} g_i^{-1} : n \in \mathbb{Z}\}) \\ & = & \mathrm{ord}(\{[g_i T g_i^{-1}], [g_i T^2 g_i^{-1}], \ldots, [g_i T^{w_i} g_i^{-1}]\}) \\ & = & w_i \end{array}$$

□

Normalteiler haben einen speziellen Vektor der Spitzenbreiten, die Umkehr des folgenden Lemmas gilt aber nicht:

1.13 Lemma: *Eine Untergruppe $\Delta <_f \Gamma$ sei Normalteiler mit Spitzenklassen S_Δ. Dann haben alle Spitzen die gleiche Breite.*

Beweis:
Sei w_1 die Breite der Spitze $s_1 = \infty$ als Repräsentant der Spitzenklasse $[\infty]$. Um zu zeigen, daß jede andere Spitze $s_i \in S_\Delta$ ebenfalls die Breite w_1 hat, wählen wir $g_i \in \Gamma$ mit $s_i = g_i\infty$ nach Satz 1.10, so daß gilt:

$$\mathrm{Stab}_\Gamma(s_i) = g_i \,\mathrm{Stab}_\Gamma(\infty) g_i^{-1}.$$

Da Δ ein Normalteiler ist, definiert:

$$\begin{array}{rccc} f: & \Delta & \longrightarrow & \Delta \\ & \delta & \longmapsto & g_i \delta g_i^{-1} \end{array}$$

einen Δ-Automorphismus. δs_i liegt in derselben Nebenklasse wie s_i und es folgt:

$$g_i^{-1}\delta g_i\infty = \infty \quad \text{, also} \quad \mathrm{Stab}_\Delta(\infty) = g_i \,\mathrm{Stab}_\Delta(\infty) g_i^{-1}$$

und daher:

$$\begin{array}{rcl} [\mathrm{Stab}_\Gamma(s_i) : \mathrm{Stab}_\Delta(s_i)] & = & [g_i \,\mathrm{Stab}_\Gamma(\infty) g_i^{-1} : g_i \,\mathrm{Stab}_\Delta(\infty) g_i^{-1}] \\ & = & [\mathrm{Stab}_\Gamma(\infty) : \mathrm{Stab}_\Delta(\infty)] = w_1. \end{array}$$

□

Ein Ziel dieser Arbeit war es, ein Programm zu entwickeln, das zu einer gegebenen Untergruppe $\Delta <_f \Gamma$ den Spitzenvektor $S(\Delta)$ und den Vektor $W(\Delta)$ der Spitzenbreiten bestimmt. Die meisten Programme wurden in GAP (Groups, Algorithms, Programming) realisiert. Weitere Informationen sind auf der homepage **turnbull.mcs.st-and.ac.uk/∼gap/** [GAP] zu finden. Wenn nötig, wurden zusätzliche Programmteile in MAGMA oder Maple implementiert. Die wichtigsten im Rahmen dieser Arbeit entwickelten Programme sind im Anhang angefügt und können zusammen mit weiteren Programmen und Beispieldateien von meiner homepage heruntergeladen werden: **ckeil.de**.

1.2 Kongruenzuntergruppen

Eine Untergruppe Δ der vollen Modulgruppe mit endlichem Index wird als *Kongruenzuntergruppe* bezeichnet, wenn Δ die *Hauptkongruenzuntergruppe*:

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2,\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod n \right\}$$

für ein $n \in \mathbb{N}$ enthält, und andernfalls als *Nicht-Kongruenzuntergruppe*. Die Hauptkongruenzuntergruppe $\Gamma(n)$ ergibt sich als Kern des Gruppenhomomorphismuses:

$$\phi : \Gamma \longrightarrow \mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z}),$$

der die Einträge der Matrizen modulo n reduziert, und ist eine normale Untergruppe vom Index [Sch74]:

$$\mu = [\Gamma : \Gamma(n)] = \begin{cases} 6 & n = 2 \\ \frac{n^3}{2} \prod_{p|n} (1 - \frac{1}{p^2}) & n > 2. \end{cases}$$

Hauptkongruenzuntergruppen haben:

$$r = \frac{\mu}{n}$$

Klassen inäquivalenter Spitzen [Pet82] und da sie normale Untergruppen sind, folgt mit Lemma 1.13, daß jede der r Spitzen die Breite n hat.
Für eine Kongruenzuntergruppe Δ folgt aus $\Gamma(n) \subset \Delta$ auch $\Gamma(k) \subset \Delta$ für jedes Vielfache $k \in \mathbb{N}$ von n. Daher existiert eine kleinste solche Zahl, die Klein als den *Level* oder die *Stufe* der Kongruenzuntergruppe Δ bezeichnet [KF66]. Wichtige Beispiele für Kongruenzuntergruppen sind die volle Modulgruppe $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$ als Kongruenzgruppe vom Level 1, die *Heckeuntergruppen*:

$$\Gamma_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \colon c \equiv 0 \bmod n \right\}$$

vom Level n und die dazu konjugierten Untergruppen [Leh64]:

$$\Gamma^0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \colon b \equiv 0 \bmod n \right\} = B\Gamma_0(n)B^{-1}$$

mit $B := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
Ein Beispiel eines Fundamentalbereiches der Hauptkongruenzuntergruppe $\Gamma(5)$ ist in Abbildung 1.2 aufgeführt. Die Bilder wurden mit einem Programm von Verill[Ver] erzeugt, das für bestimmte Typen von Kongruenzuntergruppen ihren Fundamentalbereich zeichnet.

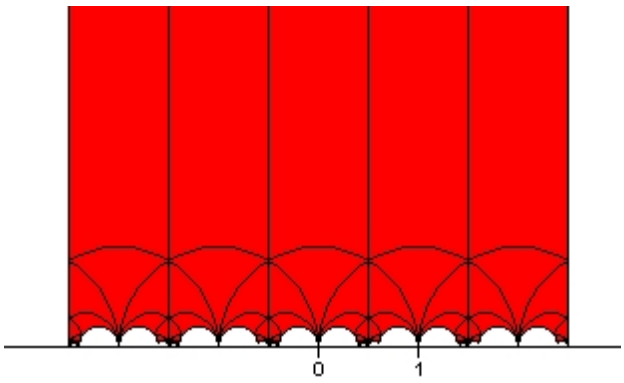

Abbildung 1.2: Fundamentalbereich für $\Gamma(5)$

Für eine Kongruenzuntergruppe Δ von Γ vom Level n gibt es bekannte Resultate über den Vektor $W(\Delta) = [w_1, \ldots, w_r]$ der Spitzenbreiten, die wir teilweise mit Überlegungen aus Kapitel 3 deutlich einfacher beweisen können.

1.14 Satz: *Es existiert ein $w_i \in W(\Delta)$ mit $w_i = \text{ggt } W(\Delta) = \text{ggt } \{w_1, \ldots, w_r\}$. Insbesondere ist diese Breite die kleinste, also gilt $w_i = \min W(\Delta)$.*

Larcher beweist diesen Satz zusammen mit weiteren interessanten Zusammenhängen in dem Artikel [Lar82], aus dem wir hier noch den folgenden Satz zitieren:

1.15 Satz: *Sei w_1 die Spitzenbreite der Spitze $s_1 = \infty$ und w_i die Spitzenbreite der Spitze $s_i = 0$, wobei nicht notwendig $i \neq 1$ gelten muß. Dann gilt $w_1 w_i \equiv 0 \bmod n$.*

Der Begriff *Level* wurde von Wohlfahrt [Woh89, Woh64] für eine beliebige Untergruppe Δ von Γ mit endlichem Index definiert als das kleinste gemeinsame Vielfache der Spitzenbreiten von Δ. Wir werden daher für eine beliebige Untergruppe $\Delta < \Gamma$ unter dem *erweiterten Level* das kleinste gemeinsame Vielfache $n = \text{kgV } W(\Delta)$ vestehen. Fricke und Wohlfahrt [Woh64, KF66] haben gezeigt, daß für Kongruenzuntergruppen diese Definition mit der früheren Definition des Levels als die größte natürliche Zahl n mit $\Gamma(n) \subset \Delta$ übereinstimmt. Nach Larcher [Lar82] existiert zu einer Kongruenzuntergruppe vom Level n auch eine Spitze der Breite n, so daß insgesamt auch das kleinste gemeinsame Vielfache angenommen wird:

1.16 Satz: *Es existiert ein* $w_i \in W(\Delta)$ *mit* $w_i = \text{kgV } W(\Delta) = \text{kgV } \{w_1, \ldots, w_r\}$. *Insbesondere ist diese Breite die größte, also gilt* $w_i = \max W(\Delta)$.

Damit ist für eine beliebige Untergruppe Δ von Γ sofort klar:

1.17 Lemma: *Wenn zu einer Untergruppe* $\Delta < \Gamma$ *keine Spitze* $s_i \in S(\Delta)$ *existiert mit* $w_i = \text{ggt } W(\Delta)$ *und keine Spitze* $s_j \in S(\Delta)$ *existiert mit* $w_j = \text{kgV } W(\Delta)$, *dann kann* Δ *keine Kongruenzuntergruppe sein.*

Der Index $[\Gamma : \Delta]$ einer Kongruenzuntergruppe muß damit größer oder gleich ihrem Level sein, da Δ eine Spitzenklasse dieser Breite besitzt und damit den zugehörigen Stabilisator enthält. Die Gleichheit gilt nur für sogenannte *zykloide* Kongruenzuntergruppen: Eine Untergruppe von Γ, deren Spitzen alle zueinander äquivalent sind, heißt *zykloid* und kann entweder eine Kongruenzuntergruppe sein oder nicht. Zykloide Kongruenzuntergruppen wurden von Petersson untersucht [Pet82], Untersuchungen für beliebige zykloide Untergruppen findet man bei Venkov [Ven81]. Nach Klein und Fricke [KF66] bilden die zykloiden Untergruppen nur einen verschwindend kleinen Bruchteil aller Untergruppen der Modulgruppe.

1.3 Ein Algorithmus zur Bestimmung der Kongruenzuntergruppen

Da für ein $n \in \mathbb{N}$ die Hauptkongruenzuntergruppe $\Gamma(n)$ den Kern des Gruppenhomomorphismuses ϕ bildet, ergibt sich die kurze exakte Folge:

$$1 \longrightarrow \Gamma(n) \xrightarrow{i} \text{PSL}(2,\mathbb{Z}) \xrightarrow{\phi} \text{PSL}(2,\mathbb{Z}/n\mathbb{Z}) \longrightarrow 1.$$

Sei nun $\Delta < \text{PSL}(2,\mathbb{Z})$ eine beliebige Untergruppe mit Index $\mu = [\Gamma : \Delta]$, Spitzenvektor $S(\Delta)$ und zugehörigen Spitzenbreiten $W(\Delta)$. Ferner existiere ein $s_i \in S(\Delta)$ mit $w_i = \text{kgV } (W(\Delta))$, da Δ nach Lemma 1.17 nur dann eine Kongruenzuntergruppe sein kann. Dann ist $n = w_i$ der erweiterte Level von Δ und

es ist zu überprüfen, ob $\Gamma(n) \subset \Delta$.
Um dies zu beantworten, verwenden wir die von Behr und Mennicke [BM68] angegebenen Relationen zu Beschreibung von $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ als Untergruppe einer freien Gruppe mit zwei Erzeugern modulo der von den Relationen erzeugten normalen Untergruppe. Diese sogenannten *Mennicke-Repräsentationen* lassen sich durch Identifizieren von ± 1 auf $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ übertragen. Eine einfache Darstellung dieser Relationen in Abhängigkeit von n findet sich bei Hsu, der sich ebenfalls damit beschäftigt, Kongruenzuntergruppen von $\mathrm{SL}(2, \mathbb{Z})$ zu identifizieren [Hsu96]. Er löst dieses Problem, indem er eine gegebene Untergruppe durch Permutationen beschreibt und einen Algorithmus angibt, um für diese Zykel mithilfe der Mennicke-Repräsentationen zu entscheiden, ob es sich um eine Kongruenzuntergruppe handelt oder nicht. Da wir Untergruppen der Modulgruppe über Erzeuger angeben, nutzen wir die folgenden Relationen für einen eigenen Algorithmus, dessen Implementierung im Anhang zu finden ist.

1.18 Satz: *Sei $n \in \mathbb{N}$ ungerade und sei $\frac{1}{2}$ das multiplikativ Inverse von $2 \bmod n$.* $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ *ist isomorph zu:*

$$\begin{aligned} G = \langle a, b \;\; | \;\; & a^n = 1 \\ & (ab^{-1}a)^4 = 1 \\ & (b^{-1}a)^3(ab^{-1}a)^{-2} = 1 \\ & (b^2a^{-\frac{1}{2}})^3(ab^{-1}a)^{-2} = 1 \rangle. \end{aligned}$$

Diese Relationen sind erfüllt für $a = T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $b = (BTB)^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

1.19 Satz: *Sei $n = 2^e$, sei $\frac{1}{5}$ das multiplikativ Inverse von $5 \bmod n$ und sei $s := l^{20}r^{-\frac{1}{5}}l^{-4}r^{-1}$.* $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ *ist isomorph zu:*

$$\begin{aligned} G = \langle l, r \;\; | \;\; & l^n = 1 \\ & (lr^{-1}l)^4 = 1 \\ & (r^{-1}l)^3(lr^{-1}l)^{-2} = 1 \\ & (lr^{-1}l)^{-1}s(lr^{-1}l)s = 1 \\ & s^{-1}rsr^{-25} = 1 \\ & (sr^5lr^{-1}l)^3(lr^{-1}l)^{-2} = 1 \rangle. \end{aligned}$$

Diese Relationen sind erfüllt für $l = T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $r = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

1.20 Satz: *Sei $n = 2^e m$ ungerade mit $e \neq 0$, sei $\frac{1}{2}$ das multiplikativ Inverse von $2 \bmod n$, $\frac{1}{5}$ das multiplikativ Inverse von $5 \bmod n$ und sei $s := l^{20}r^{-\frac{1}{5}}l^{-4}r^{-1}$. Sei $c \in \mathbb{N}$ mit $c \equiv 0 \bmod 2^e \;\wedge\; c \equiv 1 \bmod m$ und $d \in \mathbb{N}$ mit $d \equiv 1 \bmod 2^e \wedge$*

$d \equiv 0 \bmod m$. *Es sei* $a = L^c, b = R^c, l = L^d, r = R^d$.
$\mathrm{SL}(2,\mathbb{Z})$ *ist isomorph zu:*

$$\begin{aligned} G = \langle L, R \quad | \quad & L^n = 1 \\ & [a,r] = 1 \\ & [b,l] = 1 \\ & (ab^{-1}a)^4 = 1 \\ & (b^{-1}a)^3(ab^{-1}a)^{-2} = 1 \\ & (b^2a^{-\frac{1}{2}})^3(ab^{-1}a)^{-2} = 1 \\ & (lr^{-1}l)^4 = 1 \\ & (r^{-1}l)^3(lr^{-1}l)^{-2} = 1 \\ & s^{-1}(lr^{-1}l)^{-1}s^{-1}(lr^{-1}l) = 1 \\ & r^{25}s^{-1}r^{-1}s = 1 \\ & (sr^5lr^{-1}l)^3(lr^{-1}l)^{-2} = 1\rangle. \end{aligned}$$

Diese Relationen sind erfüllt für $L = T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *und* $R = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

Mit diesen Relationen können wir nun entscheiden, ob es sich bei einer gegebenen Gruppe Δ um eine Kongruenzuntergruppe handelt oder nicht. Um die Korrektheit des dafür entwickelten Algorithmus zu beweisen, betrachten wir die freie Gruppe in den Erzeugern A und B und erweitern die Relationen der Mennicke-Repräsentationen in A und B um die Relation $-1 = 1$, so daß wir eine Repräsentation von $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ erhalten. Nach den obigen Sätzen sind die Relationen unabhängig von n erfüllt für $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ und Γ wird auch von $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ erzeugt. Es seien $\tilde{R}_1, \ldots, \tilde{R}_\nu$ die Relationen der Mennicke-Repräsentation von $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ ausgewertet für $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Damit formulieren wir folgenden Satz:

1.21 Satz: *Sei* $\Delta < \Gamma$ *vom Index* $\mu = [\Gamma : \Delta]$ *mit erweitertem Level* n. *Ferner seien* $R_1, \ldots, R_\nu$ *die Relationen der Mennicke-Repräsentation von* $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ *und* $\tilde{R}_1, \ldots, \tilde{R}_\nu$ *die Relationen ausgewertet für* $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *und* $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. *Dann gilt* $\Gamma(n) \subset \Delta$ *genau dann, wenn* $\gamma R_i \gamma^{-1} \in \Delta$ *für alle* $\gamma \in \Gamma$ *und* $i = 1, \ldots, \nu$.

Beweis:
Sei $F_2 = \langle A, B\rangle$ die freie Gruppe auf zwei Erzeugern und:

$$f : F_2 \longrightarrow \mathrm{PSL}(2,\mathbb{Z}) \text{ mit } f(A) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, f(B) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Dabei ist f ein surjektiver Gruppenhomomorphismus und wir betrachten folgendes Diagramm:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \ker g & \longrightarrow & \langle A, B | -1 = 1\rangle & \xrightarrow{g} & \langle A, B | R_1, \ldots, R_\nu\rangle \\ & & & & \downarrow f & & \downarrow \cong \\ 1 & \longrightarrow & \ker(\Phi) = \Gamma(n) & \xrightarrow{i} & \mathrm{PSL}(2,\mathbb{Z}) & \xrightarrow{\Phi} & \mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z}) \end{array}$$

Dabei reduziert $\Phi : \mathrm{PSL}(2,\mathbb{Z}) \longrightarrow \mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ die Einträge in den Matrizen modulo n und $g : \langle A, B| - 1 = 1\rangle \longrightarrow \langle A, B|R_1, \ldots, R_\nu\rangle$ reduziert ein Wort in A und B mithilfe der Relationen $R_1, \ldots, R_\nu$. Beide Abbildungen sind surjektive Gruppenhomomorphismen und das Diagramm kommutiert. $\ker g$ ist der normale Abschluss der R_i in $\langle A, B| - 1 = 1\rangle$, $\ker(\Phi)$ ist der normale Abschluss der $\tilde{R}_i$ in $\mathrm{PSL}(2,\mathbb{Z})$ und insbesondere folgt:

$$f(\ker g) = \ker(\Phi) = \Gamma(n).$$

Wenn also $\gamma\tilde{R}_i\gamma^{-1} \in \Delta$ für alle $\gamma \in \Gamma$ gilt, folgt damit $\Gamma(n) \subset \Delta$. Umgekehrt sehen wir sofort, daß aus $\Gamma(n) \subset \Delta$ direkt $\gamma\tilde{R}_i\gamma^{-1} \in \Delta$ für alle $\gamma \in \Gamma$ folgt. □

Wir haben also gesehen, daß $\Gamma(n) \subset \Delta$ äquivalent dazu ist, daß:

$$\tilde{\Phi} : \Delta \longrightarrow \mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$$

surjektiv ist. Statt die Aussage des Satzes für alle $\gamma \in \Gamma$ zu überprüfen, reicht es aus, nur Repräsentanten der Nebenklassen von $\Gamma\backslash\Delta$ zu betrachten:

1.22 Korollar: *Unter den gleichen Voraussetzungen wie in Satz 1.21 gilt $\Gamma(n) \subset \Delta$ genau dann, wenn $\gamma_j R_i \gamma_j^{-1} \in \Delta$ für Repräsentanten $\gamma_1, \ldots, \gamma_\mu$ der Nebenklassen von $\Gamma\backslash\Delta$ und $i = 1, \ldots, \nu$.*

Beweis:

„⇐“ Sei $\gamma \in \Gamma$ und R_i eine der Relationen. Wir zeigen, daß aus $\gamma_j R_i \gamma_j^{-1} \in \Delta$ für alle $j = 1, \ldots, \mu$ folgt, daß $\gamma R_i \gamma^{-1} \in \Delta$. Zu $\gamma \in \Gamma$ existiert ein $j \in \{1, \ldots, \mu\}$ mit $\gamma \in \Delta\gamma_j$, also existiert ein $\delta \in \Delta$ mit $\gamma = \delta\gamma_j$. Damit folgt

$$\gamma R_i \gamma^{-1} = \delta\gamma_j R_i \gamma_j^{-1}\delta^{-1} \in \Delta,$$

da $\gamma_j R_i \gamma_j^{-1} \in \Delta$ nach Voraussetzung und $\delta \in \Delta$.

„⇒“ klar.

□

2 Eisensteinreihen und die Streumatrix

In der Theorie der Eisensteinreihen wird jeder Untergruppe der Modulguppe von endlichem Index eine Familie von Eisensteinreihen zugeordnet. Für die Darstellung der Fourierentwicklung solcher Reihen sind insbesondere die konstanten Terme von großem Interesse, die in der Streumatrix zusammengefasst werden. Im ersten Abschnitt stellen wir die Theorie der Eisensteinreihen basierend auf dem Buch von Kubota [Kub73] kurz vor und im zweiten Abschnitt beschäfigen wir uns genauer mit der Streumarix und ihrer Struktur. Die dort gewonnenen Erkenntnisse werden im letzten Abschnitt an einem einfachen Beispiel verdeutlicht.

2.1 Einführung in die Theorie der Eisensteinreihen

Im Weiteren sei Δ stets eine Untergruppe von Γ von endlichem Index, Spitzenvektor $S(\Delta) = [s_1 = \infty, s_2 = g_2\infty, \ldots, s_r = g_r\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, \ldots, w_r]$ mit den zugehörigen Matrizen $g_i \in \Gamma$ und entsprechenden $h_i = g_i\hat{w}_i \in \mathrm{PSL}(2,\mathbb{Z})$ mit $h_i\infty = s_i$ und $h_i^{-1}\Delta(s_i)h_i = \Gamma(\infty)$ nach Satz 1.10.

2.1 Definition: *Die Eisensteinreihe $E_i(z,s)$ zu einer Spitze s_i ist für $z \in \mathbb{H}$, $s \in \mathbb{C}$ definiert als:*

$$E_i(z,s) := \sum_{\delta \in \Delta(s_i)\backslash\Delta} \mathrm{Im}(h_i^{-1}\delta z)^s.$$

Diese Definition ist unabhängig von der Wahl des Repräsentanten für die Spitze s_i, von der Wahl der nach Satz 1.10 eindeutig bis auf Translation von rechts mit $T^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ bestimmten Matrix h_i und von der Wahl des Repräsentanten δ der Nebenklasse $\Delta(s_i)\backslash\Delta$ [Kub73]. Ein typisches Beispiel ist die Eisensteinreihe der vollen Modulgruppe [FB95]:

$$E(z,s) = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}\times\mathbb{Z}\backslash\{(0,0)\} \\ \mathrm{ggt}\ (c,d)=1}} \frac{\mathrm{Im}(z)^s}{|cz+d|^{2s}} = \sum_{\delta\in\Gamma_\infty\backslash\Gamma} \mathrm{Im}(\delta z)^s.$$

2.2 Satz: *Die Eisensteinreihe $E_i(z,s)$ zu einer Spitze $s_i \in S(\Delta)$ konvergiert absolut für* $\operatorname{Re} s > 1$.

Ein Beweis, der auch gleichmäßige Konvergenz auf kompakten Teilmengen von $\{s \in \mathbb{C} : \operatorname{Re} s > 1\}$ zeigt, findet sich bei Kubota [Kub73]. Wenn diese Reihe konvergiert, ist die Eisensteinreihe eine Δ-automorphe Funktion:

$$E_i(\delta z, s) = E_i(z, s)$$

für jedes $\delta \in \Delta$. Sei jetzt $s_j \in S(\Delta)$ eine weitere Spitze von Δ mit zugehöriger Matrix $h_j \in \mathrm{PSL}(2,\mathbb{Z})$ nach Satz 1.10, also mit $h_j\infty = s_j$. Dann ist $E_i(h_j z, s)$ eine in z periodische Funktion mit Periode 1:

$$E_i(h_j(z+1), s) = E_i(h_j z, s).$$

Daher bestimmen wir jetzt die Fourierentwicklung einer Eisensteinreihe $E_i(z,s)$ zu einer Spitze s_i in der Spitze s_j.

2.3 Definition: *Die Fourierentwicklung der Eisensteinreihe $E_i(z,s)$ in der Spitze s_j ist für* $\operatorname{Re} s > 1$ *definiert als:*

$$E_i(h_j z, s) = \sum_{m=-\infty}^{\infty} a_{ij,m}(y,s) e^{2\pi i m x}$$

mit:

$$a_{ij,m}(y,s) := \int_0^1 E_i(h_j z, s) e^{-2\pi i m x} dx.$$

Nun wollen wir für die $a_{ij,m}$ eine explizite Form finden. Dazu stellen wir die $a_{ij,m}$ zunächst als Integrale über Summen dar:

$$a_{ij,m} = \int_0^1 \sum_{\delta \in \Gamma(\infty)\backslash h_i^{-1}\Delta h_j} y(\delta z)^s e^{-mx} dx.$$

Jetzt realisieren wir eine Art *Bruhat-Zerlegung* der Doppelnebenklassen:

$$\Gamma(\infty) \setminus h_i^{-1}\Delta h_j / \Gamma(\infty) = \Gamma(\infty) \cup \left(\bigcup_{c,d} \Gamma(\infty)\gamma\Gamma(\infty) \right)$$

mit c, d so, daß $c > 0, d \in \mathbb{Z}/c\mathbb{Z}$ und daß sich c, d zu einer Matrix $\gamma \in \Gamma$ ergänzen lassen. Dies ermöglicht uns den Übergang von Integralen $\int_0^1$ zu Summen

über die Elemente der Doppelnebenklassen und führt uns zu einer endgültigen Darstellung der $a_{ij,m}$, für die wir die *modifizierte Bessel-Funktion* benötigen:

$$K_s(z) = \frac{\pi}{2}\frac{I_{-s}(z) - I_s(z)}{\sin(s\pi)},$$

wobei:

$$I_s(z) = \sum_{m=0}^{\infty} \frac{(\frac{z}{2})^{s+2m}}{m!\Gamma(s+m+1)}$$

mit der *Gamma-Funktion*:

$$\Gamma(s) = \int_0^\infty t^{z-1}e^{-t}dt,$$

die die Funktionalgleichungen:

$$\Gamma(z+1) = z\Gamma(z) \qquad \text{und} \qquad \Gamma(-z+1) = -z\Gamma(-z)$$

erfüllt. Für Details dieser Umformungen vergleiche z. B. Kubota [Kub73], wir geben hier jetzt nur das endgültige Ergebnis an:

$$a_{ij,m}(y,s) = 2\pi^s|m|^{s-\frac{1}{2}}\Gamma(s)^{-1}y^{\frac{1}{2}}K_{s-\frac{1}{2}}(2\pi|m|y)\varphi_{ij,m}(s)$$

für $m \neq 0$ und:

$$a_{ij,0}(y,s) = \delta_{ij}y^s + \varphi_{ij}(s)y^{1-s}$$

mit:

$$\varphi_{ij,m}(s) = \sum_{c>0}\frac{1}{c^{2s}}\left(\sum_d e^{2\pi i\frac{md}{c}}\right)$$

für $m \geq 0$, wobei die zweite Summation über solche $d \in \mathbb{R}$ mit d reduziert modulo c läuft, die sich zu einer Matrix $\gamma = \left(\begin{smallmatrix}\star & \star\\ c & d\end{smallmatrix}\right) \in h_i^{-1}\Delta h_j$ ergänzen lassen, und

$$\varphi_{ij}(s) = \pi^{\frac{1}{2}}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\varphi_{ij,0}(s).$$

Die Funktionen $\varphi_{ij,m}(s)$ sind also Dirichlet-Reihen, deren theoretische Grundlagen in [Apo76] oder [HR64] zu finden sind. Der Zusammenhang zu ganzen Modulformen wird z.B. in [Ran77] oder [Lan76] erläutert. Die zum konstanten Term der Fourierentwicklung von $E_i(z,s)$ in der Spitze s_j, also zu $m = 0$, gehörenden Funktionen φ_{ij} werden in der sogenannten *Streumatrix* zusammengefasst:

2.4 Definition: *Die Streumatrix hat für* $s \in \mathbb{H}$ *mit* $\operatorname{Re} s > 1$ *die Gestalt:*

$$\Phi(s) := (\varphi_{ij}(s))_{1\leq i,j\leq r}\,.$$

Die in den konstanten Termen $\varphi_{ij}(s)$ auftretenden Summen:

$$\sum_{c>0,\ d\ reduziert\ modulo\ c,\ \left(\begin{smallmatrix}\star & \star\\ c & d\end{smallmatrix}\right)\in h_i^{-1}\Delta h_j} 1$$

entsprechen der Anzahl der Doppelnebenklassen mit festem Eintrag $c \in \mathbb{R}^+$ links unten in:

$$\Gamma(\infty) \setminus h_i^{-1}\Delta h_j/\Gamma(\infty).$$

Nach Definition der h_i lassen sich diese Doppelnebenklassen umformulieren zu:

$$h_i^{-1}\Delta(s_i)h_i \setminus h_i^{-1}\Delta h_j/h_j^{-1}\Delta(s_j)h_j.$$

Dabei taucht die Restklasse zu $\Gamma(\infty)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\Gamma(\infty)$ nur dann in obiger Zerlegung auf, wenn $i = j$ gilt, da sonst die Spitzen s_i und s_j Δ-äquivalent wären.
Indem wir jeder Doppelnebenklasse ihr Inverses zuordnen:

$$\begin{array}{rccc} {}^{-1}: & \Gamma(\infty) \setminus h_i^{-1}\Delta h_j/\Gamma(\infty) & \longrightarrow & \Gamma(\infty) \setminus h_i^{-1}\Delta h_j/\Gamma(\infty) \\ & g & \longmapsto & g^{-1} \end{array}$$

sehen wir, daß:

$$(\Gamma(\infty) \setminus h_i^{-1}\Delta h_j/\Gamma(\infty))^{-1} = \Gamma(\infty) \setminus h_j^{-1}\Delta h_i/\Gamma(\infty).$$

Damit stimmt die Anzahl der Doppelnebenklassen für dasselbe feste c überein und wir erhalten folgenden Satz:

2.5 Satz: *Die Streumatrix ist symmetrisch.*

Es gibt eine ganze Reihe von Sätzen über analytische Fortsetzungen der Eisensteinreihen, die z.B. bei Kubota [Kub73] zu finden sind. Wir wollen hier ein Ergebnis, die Fortsetzbarkeit auf die ganze obere Halbebene angeben:

2.6 Satz: *Die Streumatrix $\Phi(s)$ ist meromorph für alle $s \in \mathbb{H}$ und erfüllt die Funktionalgleichung:*

$$\Phi(s)\Phi(1-s) = \mathrm{Id}_r.$$

Eisensteinreihen spielen eine große Rolle in der Spektraltheorie von $L^2(\Delta \setminus \mathbb{H})$, dem Hilbertraum der quadratisch integrierbaren Funktionen, die automorph bezüglich einer auf $\mathbb{H}$ operierenden diskontunuierlichen Gruppe Δ sind.

2.2 Die Einträge der Streumatrix

Um die Streumatrix genauer untersuchen zu können, benötigen wir einige Umformulierungen und Notationen. Zunächst wollen wir die Einträge der Streumatrix so umschreiben, daß in den Doppelnebenklassen über $\mathbb{N}$ und nicht mehr über $\mathbb{R}$ summiert wird: Die Einträge der Streumatrix haben nach Definition 2.4 für $1 \leq i, j \leq r$ die Gestalt:

$$\varphi_{ij}(s) = \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \varphi_{ij,0}(s)$$

mit:

$$\begin{aligned} \varphi_{ij,0}(s) &= \sum_{\tilde{c} \in \mathbb{R}^+} \frac{1}{\tilde{c}^{2s}} \sum_{d \bmod \tilde{c},\ \left(\begin{smallmatrix} \star & \star \\ \tilde{c} & d \end{smallmatrix}\right) \in h_i^{-1}\Delta h_j} 1 \\ &= \sum_{\tilde{c} \in \mathbb{R}^+} \frac{1}{\tilde{c}^{2s}} \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ \tilde{c} & \star \end{smallmatrix}\right)] \in \Gamma(\infty) \setminus h_i^{-1}\Delta h_j / \Gamma(\infty) \right\} \right|. \end{aligned}$$

Sei nun für $\tilde{c} \in \mathbb{R}^+$:

$$a_{ij}(\tilde{c}) := \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ \tilde{c} & \star \end{smallmatrix}\right)] \in \Gamma(\infty) \setminus h_i^{-1}\Delta h_j / \Gamma(\infty) \right\} \right|$$

die Anzahl der Doppelnebenklassen mit linkem unteren Eintrag $\tilde{c}$. Jetzt wollen wir diese Anzahl so umschreiben, daß wir über natürliche Zahlen summieren. Mit $h_i := g_i \hat{w}_i$ für $g_i \in \Gamma$ und $\hat{w}_i := \left(\begin{smallmatrix} \sqrt{w_i} & 0 \\ 0 & \frac{1}{\sqrt{w_i}} \end{smallmatrix}\right)$ nach Satz 1.10 gilt:

$$h_i^{-1}\Delta(s_i)h_i = \{T^n : n \in \mathbb{Z}\} = \Gamma(\infty)$$

und wir erhalten für die Doppelnebenklassen:

$$\begin{aligned} & \Gamma(\infty) \setminus h_i^{-1}\Delta h_j / \Gamma(\infty) \\ = \ & h_i^{-1}\Delta(s_i)h_i \setminus h_i^{-1}\Delta h_j / h_j^{-1}\Delta(s_j)h_j \\ = \ & \hat{w}_i^{-1}g_i^{-1}\Delta(s_i)g_i\hat{w}_i \setminus \hat{w}_i^{-1}g_i^{-1}\Delta g_j \hat{w}_j / \hat{w}_j^{-1}g_j^{-1}\Delta(s_j)g_j\hat{w}_j. \end{aligned}$$

Eine Matrix:

$$g = \begin{pmatrix} \star & \star \\ \tilde{c} & \star \end{pmatrix} \in \hat{w}_i^{-1}g_i^{-1}\Delta g_j \hat{w}_j$$

mit linkem unteren Eintrag $\tilde{c} \in \mathbb{R}^+$ läßt sich daher schreiben als:

$$\hat{w}_i^{-1}\gamma\hat{w}_j$$

für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in g_i^{-1}\Delta g_j$. Zu einem $c \in \mathbb{N}$ gibt es genau dann eine Matrix in $g_i^{-1}\Delta g_j$, wenn es zu einem $\tilde{c} = \sqrt{w_i}\sqrt{w_j}c \in \mathbb{R}^+$ eine Matrix $\left(\begin{smallmatrix} \star & \star \\ \tilde{c} & d \end{smallmatrix}\right) \in h_i^{-1}\Delta h_j$ gibt. Mit:

$$\begin{aligned} b_{ij}(c) &:= \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in g_i^{-1}\Delta(s_i)g_i \setminus g_i^{-1}\Delta g_j / g_j^{-1}\Delta(s_j)g_j \right\} \right| \\ &= \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \{T^{w_i n} : n \in \mathbb{Z}\} \setminus g_i^{-1}\Delta g_j / \{T^{w_j n} : n \in \mathbb{Z}\} \right\} \right| \end{aligned}$$

für $c \in \mathbb{N}$ ergibt sich für die Einträge der Streumatrix:

$$\begin{aligned}
\varphi_{ij}(s) &= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{\tilde{c}>0, \tilde{c}\in\mathbb{R}} \frac{a_{ij}(\tilde{c})}{\tilde{c}^{2s}} \\
&= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{c\in\mathbb{N}} \frac{b_{ij}(c)}{(\sqrt{w_i}\sqrt{w_j})^{2s} c^{2s}} \\
&= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{c\in\mathbb{N}} \frac{b_{ij}(c)}{(w_i w_j)^{s} c^{2s}} \\
&= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{1}{(w_i w_j)^{s}} \tilde{\varphi}_{ij}(s)
\end{aligned}$$

mit

$$\tilde{\varphi}_{ij}(s) := \sum_{c\in\mathbb{N}} \frac{b_{ij}(c)}{c^{2s}}$$

Die Streumatrix läßt sich damit aus der *Matrix der Bildungsgesetze* für die Anzahlen der Doppelnebenklassen mit $c \in \mathbb{N}$ konstruieren:

$$B := B(c) := (b_{ij}(c))_{1\le i,j\le r}\,.$$

Um weitere Eigenschaften der Streumatrix zu einer Gruppe $\Delta < \Gamma$ untersuchen zu können, benötigen wir eine spezielle Zerlegung von Γ bezüglich der Untergruppe Δ:

2.7 Satz: *Sei Δ eine Untergruppe von Γ mit endlichem Index, Spitzenvektor $S(\Delta) = [s_1 = \infty, \ldots, s_r = g_r\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, \ldots, w_r]$. Dann läßt sich Γ darstellen als:*

$$\Gamma = \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \Delta g_i T^l.$$

Beweis:

„$\subseteq$“ Sei $\gamma \in \Gamma$ und zeige $\gamma \in \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \Delta g_i T^l$. Wegen $\gamma \in \Gamma$ ist $\gamma\infty$ eine zu ∞ $\Gamma-$äquivalente Spitze von Γ, also muß ein $s_i \in S(\Delta)$ existieren, so daß $\gamma\infty$ eine zu s_i $\Delta-$äquivalente Spitze von Δ ist: $\exists\ \delta \in \Delta, \exists\ i \in \{1, \ldots, r\}$:

$$\gamma\infty = \delta s_i = \delta g_i \infty \Longleftrightarrow \gamma^{-1}\gamma\infty = \infty = \gamma^{-1}\delta g_i\infty.$$

Also liegt $\gamma^{-1}\delta g_i$ im Stabilisator $\mathrm{Stab}_\Gamma(\infty) = \Gamma_\infty = \{T^n | n \in \mathbb{Z}\}$ und damit existiert ein $m \in \mathbb{Z}$ mit $\gamma^{-1}\delta g_i = T^{-m} \Longleftrightarrow \gamma = \delta g_i T^m$.
Modulo w_i gerechnet ergibt sich: $\exists\ a \in \mathbb{Z}, b \in \{1, \ldots, w_i\}$ mit $m = aw_i + b$ und $\gamma = \delta g_i T^{aw_i+b} = \delta(g_i T^{w_i} g_i^{-1})^a g_i T^b$.
Wegen $\delta \in \Delta$ und $g_i T^{w_i} g_i^{-1} \in \mathrm{Stab}_\Delta(s_i) = \{g_i T^{w_i n} g_i^{-1} | n \in \mathbb{Z}\} \subset \Delta$ folgt $\gamma \in \Delta g_i T^b \subset \bigcup_{l=1}^{w_i} \Delta g_i T^l \subset \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \Delta g_i T^l$.

„$\supseteq$“ Sei $\gamma \in \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \Delta g_i T^l$ und zeige $\gamma \in \Gamma$. Das ist klar, da aus $\gamma \in \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \Delta g_i T^l$ folgt, daß $i \in \{1, \ldots, r\}$ und $l \in \{1, \ldots, w_i\}$ existieren mit $\gamma \in \Delta g_i T^l \subset \Gamma$ wegen $\Delta \subseteq \Gamma$, $g_i \in \Gamma$ und $T^l \in \Gamma$.

□

Da diese Darstellung von Γ sogar disjunkt ist, ergibt sich folgendes Korollar:

2.8 Korollar: *Unter den gleichen Voraussetzungen wie in Satz 2.7 gilt:*

$$[\Gamma : \Delta] = \sum_{i=1}^{r} w_i.$$

Beweis:
Nach Satz 2.7 gilt $\Gamma = \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \Delta g_i T^l$. Um zu zeigen, daß diese Darstellung disjunkt ist, nehmen wir an, daß $i, j \in \{1, \ldots, r\}$ und $l \in \{1, \ldots, w_i\}$, $m \in \{1, \ldots, w_j\}$ existieren mit $\Delta g_i T^l = \Delta g_j T^m$.
Aus $\Delta g_i T^l \infty = \Delta g_i \infty = \Delta s_i$ und $\Delta g_j T^m \infty = \Delta g_j \infty = \Delta s_j$ folgt $i = j$, so daß sich die Widerspruchsannahme schreiben läßt als $\Delta g_i T^l = \Delta g_i T^m$ und $l, m \in \{1, \ldots, w_i\}$. Damit gilt $g_i T^{l-m} g_i \in \Delta$, so daß T^{l-m} von der Gestalt $T^{w_i n}$ für ein $n \in \mathbb{Z}$ sein muß. Aus $w_i | l - m$ und $l, m \in \{1, \ldots, w_i\}$ folgt die Gleichheit $l = m$. □

In diese disjunkte Zerlegung läßt sich eine weitere Matrix aus Γ einbauen:

2.9 Korollar: *Unter den gleichen Voraussetzungen wie in Satz 2.7 gilt für ein beliebiges $\gamma \in \Gamma$:*

$$\Gamma = \gamma\Gamma = \bigcup_{i=1}^{r} \bigcup_{l=1}^{w_i} \gamma \Delta g_i T^l.$$

Mit dieser Zerlegung von Γ bezüglich Δ wollen wir jetzt zeigen, daß sich jede Zeile und damit aus Symmetriegründen auch jede Spalte der Streumatrix zu einem Quotienten aus *Riemannschen Zetafunktionen* aufsummieren läßt:
Die *Riemannsche Zetafunktion*:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

ist die einfachste unendliche Dirichlet-Reihe und konvergiert für $\operatorname{Re} s > 1$. Für alle positiven geraden ganzen Zahlen ist sie ein rationales Vielfaches von π^{2n} [HW58]:

$$\zeta(2n) = \frac{(2\pi)^{2n}}{2(2n)!} B_{2n},$$

wobei B_n die über folgende Reihen beschriebenen *Bernoulli-Zahlen* sind:

$$B_n := \frac{2(2n)!}{(2\pi)^{2n}} \sum_{k=1}^{\infty} \frac{1}{k^{2n}}.$$

Für die Primzahltheorie ist die Zetafunktion wegen der von Euler entdeckten Identität von großer Bedeutung:

2.10 Satz: *Für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$ gilt:*

$$\zeta(s) = \prod_{p \ prim} \frac{1}{1 - p^{-s}}.$$

Die Riemannsche Zeta-Funktion läßt sich mithilfe der *Eulerschen φ-Funktion*:

$$\begin{array}{rccl} \varphi: & \mathbb{N} \setminus \{0\} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & |\{m \in \mathbb{N} | 1 \leq m \leq n \text{ und } \operatorname{ggt}(n,m) = 1\}| \end{array}$$

ausdrücken:

2.11 Satz: *Für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$ gilt:*

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)}$$

Für Beweise und weitere Details vergleiche z.B. Hardy und Wright [HW58]. Die Werte der Eulerschen φ-Funktion lassen sich folgendermaßen berechnen:

2.12 Satz: *Für $n \in \mathbb{N} \setminus \{1\}$ mit Primfaktorzerlegung $n = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$ gilt $\varphi(n) = p_1^{l_1 - 1} \cdot \ldots \cdot p_r^{l_r - 1} \cdot (p_1 - 1) \cdot \ldots \cdot (p_r - 1)$.*

Ein Beweis dieses Satzes und weitere Informationen zur Eulerschen φ-Funktion finden sich z.B in [Lan74] oder [FS74].
Mit diesen Vorüberlegungen können wir jetzt zeigen, daß für jede Zeile der Streumatrix folgende Aufsummierung gilt:

2.13 Satz: *Sei Δ eine Untergruppe von Γ mit endlichem Index, Spitzenvektor $S(\Delta) = [s_1 = \infty, \ldots, s_r = g_r \infty]$ und Spitzenbreiten $W(\Delta) = [w_1, \ldots, w_r]$. Dann gilt für alle $k \in \{1, \ldots, r\}$ und $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$:*

$$\sum_{i=1}^{r} \tilde{\varphi}_{ki}(s) = w_k \frac{\zeta(2s-1)}{\zeta(2s)}.$$

Die Aussage dieses Satzes läßt sich mit Satz 2.11 umformen zu:

$$\sum_{i=1}^{r}\sum_{c=1}^{\infty}\frac{b_{ki}(c)}{c^{2s}} = w_k\sum_{c=1}^{\infty}\frac{\varphi(c)}{c^{2s}},$$

so daß sich Satz 2.13 sofort aus folgendem Satz ergibt:

2.14 Satz: *Unter den gleichen Voraussetzungen wie in Satz 2.13 gilt:*

$$w_k\varphi(c) = \sum_{i=1}^{r} b_{ki}(c).$$

Beweis:
Für $g_k^{-1} \in \Gamma$ ergibt sich nach Korollar 2.9:

$$\Gamma = g_k^{-1}\Gamma = \bigcup_{i=1}^{r}\bigcup_{l=1}^{w_i} g_k^{-1}\Delta g_i T^l$$

und es folgt mit dem unten aufgeführten Lemma 2.16:

$$\begin{aligned} w_k\varphi(c) &= |\,\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^{w_k n} : n\in\mathbb{Z}\}\backslash\Gamma/\{T^n : n\in\mathbb{Z}\}\}\,| \\ &= |\,\big\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^{w_k n} : n\in\mathbb{Z}\}\backslash\textstyle\bigcup_{i=1}^{r}\bigcup_{l=1}^{w_i} g_k^{-1}\Delta g_i T^l/\{T^n : n\in\mathbb{Z}\}\big\}\,| \\ &= \textstyle\sum_{i=1}^{r}\sum_{l=1}^{w_i} |\,\big\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^{w_k n} : n\in\mathbb{Z}\}\backslash g_k^{-1}\Delta g_i T^l/\{T^n : n\in\mathbb{Z}\}\big\}\,|. \end{aligned}$$

Nach der Definition der b_{ij} gilt:

$$\sum_{i=1}^{r} b_{ki}(c) = \sum_{i=1}^{r} |\,\big\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^{w_k n} : n\in\mathbb{Z}\}\backslash g_k^{-1}\Delta g_i/\{T^{w_i n} : n\in\mathbb{Z}\}\big\}\,|.$$

Die Behauptung folgt mit:

$$\begin{aligned} & \textstyle\sum_{l=1}^{w_i} |\,\big\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^{w_k n} : n\in\mathbb{Z}\}\backslash g_k^{-1}\Delta g_i T^l/\{T^n : n\in\mathbb{Z}\}\big\}\,| \\ = \;& |\,\big\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^{w_k n} : n\in\mathbb{Z}\}\backslash g_k^{-1}\Delta g_i/\{T^{w_i n} : n\in\mathbb{Z}\}\big\}\,| \\ = \;& b_{ki}(c). \end{aligned}$$

□

2.15 Lemma: *Für $c \in \mathbb{N}$ gilt:*

$$|\,\{[\left(\begin{smallmatrix}*&*\\c&*\end{smallmatrix}\right)] \in \{T^n : n\in\mathbb{Z}\}\backslash\Gamma/\{T^n : n\in\mathbb{Z}\}\}\,| = \varphi(c)$$

Beweis:
Wegen $\Gamma(\infty) = \{T^n | n \in \mathbb{Z}\}$ liegen zwei Elemente $\gamma_1, \gamma_2 \in \Gamma$ mit $\gamma_1 = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ genau dann in derselben Äquivalenzklasse, wenn sie sich durch Multiplikation

mit T^{n_1} von rechts und mit T^{n_2} von links für $n_1, n_2 \in \mathbb{Z}$ ineinander überführen lassen:

$$\gamma_2 = T^{n_1}\gamma_1 T^{n_2} = \begin{pmatrix} a + n_1 c & b + n_2 a + n_1 n_2 c + n_1 d \\ c & d + n_2 c \end{pmatrix}.$$

Diese Multiplikationen lassen den linken unteren Eintrag fest und für ein $c \in \mathbb{N}$ sind die Äquivalenzklassen durch einen zweiten Wert $a \in \{1, \ldots, c\}$ eindeutig bestimmt. Dabei kann nach Satz 1.2 nur dann eine Restklasse existieren, wenn ggt $(a, c) = 1$, also wenn a nicht c teilt. Im Fall der vollen Modulgruppe läßt sich aber umgekehrt nach Satz 1.2 jedes Paar (c, a) mit ggt $(c, a) = 1$ zu einer Matrix $\gamma = \left(\begin{smallmatrix} a & \star \\ c & \star \end{smallmatrix}\right) \in \Gamma$ ergänzen. □

Wenn wir jetzt statt $\Gamma(\infty)$ auf einer Seite $\{T^{kn} : n \in \mathbb{Z}\}$ für ein $k \in \mathbb{N}$ herausteilen, lassen sich Elemente $\gamma_1, \gamma_2 \in \Gamma$ einer Äquivalenzklasse mit $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ durch folgende Multiplikationen ineinander überführen:

$$\gamma_2 = T^{kn_1}\gamma_1 T^{n_2} = \begin{pmatrix} a + kn_1 c & b + n_2 a + kn_1 n_2 c + kn_1 d \\ c & d + n_2 c \end{pmatrix}.$$

Für ein $c \in \mathbb{N}$ gibt es zu jedem $a \in \{1, \ldots, c\}$ mit ggt $(a, c) = 1$ jetzt k verschiedene Äquivalenzklassen $a + n_1 c, a + 2n_1 c, \ldots, a + kn_1 c$, so daß wir folgendes Lemma gezeigt haben:

2.16 Lemma: *Für $c \in \mathbb{N}$ gilt:*

$$\left| \left\{ [\left(\begin{smallmatrix} * & * \\ c & * \end{smallmatrix}\right)] \in \{T^{kn} : n \in \mathbb{Z}\} \backslash \Gamma / \{T^n : n \in \mathbb{Z}\} \right\} \right| = k\varphi(c)$$

Nachdem wir in Satz 2.13 gezeigt haben, daß sich jede Zeile der Streumatrix zu einem Quotienten aus Riemannschen Zetafunktionen aufsummieren läßt, können wir als direkte Konsequenz die Anzahl der für eine vollständige Kenntnis der Streumatrix zu bestimmenden Einträge reduzieren: Da die Streumatrix nach Satz 2.5 symmetrisch ist, reichten bisher bereits die Einträge auf und oberhalb der Hauptdiagonalen aus. Jetzt können wir auch noch auf die Einträge auf der Hauptdiagonalen verzichten, so daß sich folgende Anzahl ergibt:

2.17 Korollar: *Um für eine Gruppe $\Delta < \Gamma$ mit $r > 1$ Spitzen die Streumatrix anzugeben, müssen genau $r\frac{r-1}{2}$ Einträge bestimmt werden.*

Beweis:
Da für die Streumatrix die Summe jeder Zeile nach Satz 2.13 bekannt ist, läßt sich der letzte Eintrag einer Zeile immer aus den übrigen dieser Zeile bestimmen. Damit müssen für die erste Zeile $r - 1$ Einträge berechnet werden. Nach Satz 2.5 ist die Streumatrix symmetrisch, so daß jetzt in der zweiten Zeile neben dem letzten noch ein weiterer Eintrag bekannt ist und $r - 2$ Einträge zu bestimmen sind. Allgemeiner müssen für die k-te Zeile mit $1 \leq k \leq r$ genau $r - k$ Einträge berechnet werden. Die letzte Zeile ergibt sich also komplett aus den bisher

bestimmten Einträgen, so daß nur $\sum_{k=1}^{r-1} k$ Einträge bestimmt werden müssen. Mit vollständiger Induktion nach r sehen wir, daß $\sum_{k=1}^{r-1} k = r\frac{r-1}{2}$. □

2.3 Ein Beispiel: $\Gamma_0(p)$

Nach diesen theoretischen Überlegungen wollen wir zunächst ein Beispiel betrachten und für einen speziellen Typ von Untergruppen die Streumatrix ganz elementar von Hand ausrechnen. Für eine Primzahl $p \in \mathbb{N}$ sei:

$$\Gamma_0(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod p \right\} = \left\{ \begin{pmatrix} a & b \\ cp & d \end{pmatrix} \in \Gamma \right\}.$$

Die Matrizen:

$$B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \text{ und } BT^{-j}B = \left(\begin{smallmatrix} 1 & 0 \\ j & 1 \end{smallmatrix}\right) \text{ für } j = 0, 1, \ldots, p-1$$

bilden ein Repräsentantensystem für die Nebenklassen $\Gamma/\Gamma_0(p)$, so daß für den Index $[\Gamma : \Gamma_0(p)] = p + 1$ gilt [Leh64]. Nach Apostol [Apo76] bildet die Menge:

$$\mathbb{F}_{\Gamma_0(p)} := \mathbb{F} \cup \bigcup_{j=0}^{p-1} BT^j\mathbb{F}$$

einen Fundamentalbereich für $\Gamma_0(p)$, wobei $\mathbb{F}$ der Fundamentalbereich von Γ aus Abschnitt 1.1 ist. In Abbildung 2.3 sind Fundamentalbereiche für die Gruppen $\Gamma_0(3)$ und $\Gamma_0(5)$ dargestellt.

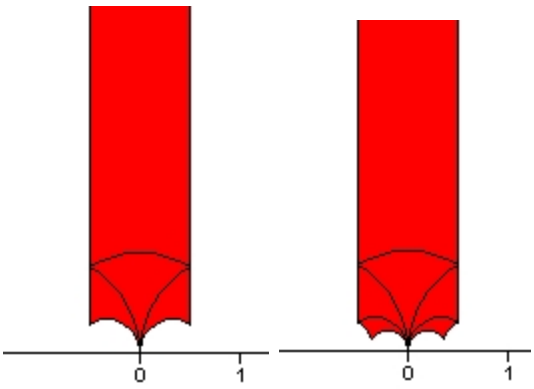

Abbildung 2.1: Fundamentalbereiche für $\Gamma_0(3)$ und $\Gamma_0(5)$

Im Folgenden sei $p \in \mathbb{N}$ eine fest gewählte Primzahl.

2.18 Satz: *$\Gamma_0(p)$ hat zwei Spitzen $s_1 := \infty$ und $s_2 := 0$.*

Beweis:
Da die $\Gamma_0(p)$-Äquivalenzklassen mit Repräsentanten aus $\mathbb{P}^1(\mathbb{Q})$ den Bahnen:

$$B_{\Gamma_0(p)}(s) := \{\gamma s : \gamma \in \Gamma_0(p)\} \qquad \text{für } s \in \mathbb{P}^1(\mathbb{Q})$$

von $\Gamma_0(p)$ in $\mathbb{P}^1(\mathbb{Q})$ entsprechen, ist folgende Behauptung äquivalent zur Aussage des Satzes:

$$B_{\Gamma_0(p)}\left(s_1 = \begin{bmatrix}1\\0\end{bmatrix}\right) \dot\cup\, B_{\Gamma_0(p)}\left(s_2 = \begin{bmatrix}0\\1\end{bmatrix}\right) = \mathbb{P}^1(\mathbb{Q}).$$

Da die Bahnen nach Definition zumindest eine Teilmenge von $\mathbb{P}^1(\mathbb{Q})$ bilden, bleibt zu zeigen, daß jede Restklasse $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{Q})$ mit ggt $(x, y) = 1$ in genau einer der beiden Bahnen liegt.
1. Fall: $p|y$
Dann existiert ein $c \in \mathbb{Z}$ mit $cp = y$ und nach dem euklidischen Algorithmus existieren $b, d \in \mathbb{Z}$ mit $dx + by = 1$. Wir setzen $\gamma := \left(\begin{smallmatrix}x & -b\\ cp & d\end{smallmatrix}\right) \in \Gamma_0(p)$.
2. Fall: $p \nmid y$
Dann gilt ggt $(p, y) = 1$ und damit auch ggt $(xp, y) = 1$. Nach dem euklidischen Algorithmus existieren $b, d \in \mathbb{Z}$ mit $dy + bxp = 1$.
Dann folgt $\gamma := \left(\begin{smallmatrix}y & -b\\ xp & d\end{smallmatrix}\right) \in \Gamma_0(p)$. □

Als nächstes bestimmen wir die Stabilisatoren der beiden Spitzen:

2.19 Lemma: $\mathrm{Stab}_\Delta(\infty) = \{T^n | n \in \mathbb{Z}\}$.

Beweis:
Aus der Definition des Stabilisators folgt für $\gamma = \left(\begin{smallmatrix}a & b\\ cp & d\end{smallmatrix}\right) \in \Gamma_0(p)$:

$$\begin{pmatrix}a & b\\ cp & d\end{pmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \Longleftrightarrow \begin{bmatrix}a\\c\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \Longleftrightarrow c = 0.$$

Die Matrizen in $\mathrm{Stab}_\Delta(\infty)$ sind also von der Gestalt $\gamma = \left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$ mit $a, b, d \in \mathbb{Z}$. Wegen $\det\gamma = 1$ folgt $a = d = 1$ und mit $T^n = \left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$ für $n \in \mathbb{Z}$ somit $\mathrm{Stab}_\Delta(\infty) = \{T^n | n \in \mathbb{Z}\} = \Gamma_\infty$. □

2.20 Lemma: $\mathrm{Stab}_\Delta(0) = \{BT^{np}B | n \in \mathbb{Z}\}$.

Beweis:
Für $\gamma = \left(\begin{smallmatrix}a & b\\ cp & d\end{smallmatrix}\right) \in \Gamma_0(p)$ gilt:

$$\begin{pmatrix}a & b\\ cp & d\end{pmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} \Longleftrightarrow \begin{bmatrix}b\\d\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} \Longleftrightarrow b = 0.$$

In $\mathrm{Stab}_\Delta(0)$ liegen also Matrizen der Gestalt $\gamma = \left(\begin{smallmatrix} a & 0 \\ cp & 1 \end{smallmatrix}\right)$ mit $a, c \in \mathbb{Z}$. Wegen $\det\gamma = 1$ folgt $a = 1$ und damit $\mathrm{Stab}_\Delta(0) = \{\left(\begin{smallmatrix} 1 & 0 \\ cp & 1 \end{smallmatrix}\right) | c \in \mathbb{Z}\}$. Mit $BT^nB = \left(\begin{smallmatrix} 1 & 0 \\ -n & 1 \end{smallmatrix}\right)$ ergibt sich insgesamt $\mathrm{Stab}_\Delta(0) = \{BT^{np}B | n \in \mathbb{Z}\}$. □

Wir haben jetzt für die Gruppe $\Gamma_0(p)$ den Spitzenvektor:

$$S(\Gamma_0(p)) = [s_1 = \infty, s_2 = 0]$$

und den Vektor der Spitzenbreiten:

$$W(\Gamma_0(p)) = [1, p]$$

bestimmt. Darüberhinaus benötigen wir noch die zugehörigen Matrizen $g_i \in \Gamma$ nach Satz 1.10 mit $g_i\infty = s_i$, nämlich:

$$g_1 = 1 \text{ und } g_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

sowie:

$$h_1 = 1 \text{ und } h_2 = \hat{w}_2 g_2 = \begin{pmatrix} 0 & -\sqrt{p} \\ \frac{1}{\sqrt{p}} & 0 \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{R}).$$

Um die Einträge φ_{ij} der Streumatrix zu berechnen, werden wir jetzt die Matrix der Bildungsgesetze:

$$B := \begin{pmatrix} b_{11}(c) & b_{12}(c) \\ b_{21}(c) & b_{22}(c) \end{pmatrix}$$

mit:

$$b_{ij}(c) = |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in g_i^{-1}\,\mathrm{Stab}_{\Gamma_0(p)}(s_i)g_i \setminus g_i^{-1}\Gamma_0(p)g_j / g_j^{-1}\,\mathrm{Stab}_{\Gamma_0(p)}(s_j)g_j\right\}|$$

für $c \in \mathbb{N}$ und $i, j \in \{1, 2\}$ bestimmen, aus der sich dann die Streumatrix konstruieren läßt.
Wir wollen zunächst für ein festes $c \in \mathbb{N}$ die Anzahl der Nebenklassen:

$$\begin{aligned} b_{11}(c) &= |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in g_1^{-1}\,\mathrm{Stab}_{\Gamma_0(p)}(s_1)g_1 \setminus g_1^{-1}\Gamma_0(p)g_1 / g_1^{-1}\,\mathrm{Stab}_{\Gamma_0(p)}(s_1)g_1\right\}| \\ &= |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T\rangle \setminus \Gamma_0(p) / \langle T\rangle\right\}| \end{aligned}$$

bestimmen und bemerken dabei, daß diese Zahl nur dann ungleich Null sein kann, wenn c ein Vielfaches von p ist. Damit folgt bereits:

$$b_{11}(c) = 0 \quad \text{für } c \not\equiv 0 \bmod p.$$

Sei also $c = c'p$ und wir betrachten die Multiplikation einer Matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c'p & d \end{smallmatrix}\right) \in \Gamma_0(p)$ mit T^{n_1} von links und mit T^{n_2} von rechts für $n_1, n_2 \in \mathbb{Z}$. Der linke untere Eintrag von γ bleibt dabei unverändert:

$$T^{n_1}\gamma T^{n_2} = \left(\begin{smallmatrix} a+n_1c & b+n_2a+n_1n_2c+n_1d \\ c'p & d+n_2c \end{smallmatrix}\right)$$

und für die Äquivalenzklassen lassen sich Repräsentanten mit Einträgen aus $\{1, \ldots, c'p\}$ wählen:

2.21 Satz: *Sei $a \in \{1, \ldots, c'p\}$ mit* ggt $(a, c'p) = 1$. *Dann existiert ein eindeutig bestimmtes $d \in \{1, \ldots, c'p\}$ mit $\left(\begin{smallmatrix} a & b \\ c'p & d \end{smallmatrix}\right) \in \langle T \rangle \setminus \Gamma_0(p) / \langle T \rangle$.*

Beweis:
Aus $a \in \{1, \ldots, c'p\}$ mit ggt $(a, c'p) = 1$ folgt mit dem euklidischen Algorithmus, daß $\lambda, \mu \in \mathbb{Z}$ existieren mit $\lambda a + \mu c'p = 1$, also $\lambda a = 1$ in $\mathbb{Z}/c'p\mathbb{Z}$. Damit ist $\bar{a}$ eine Einheit in $\mathbb{Z}/c'p\mathbb{Z}$, es existieren also ein eindeutig bestimmtes $\bar{d} \in \mathbb{Z}/c'p\mathbb{Z}$ mit $\overline{da} = 1$, bzw. $\overline{da} - 1 = 0$ in $\mathbb{Z}/c'p\mathbb{Z}$ und ein eindeutig bestimmter Repräsentant $d \in \{1, \ldots, c'p\}$ von $\bar{d}$. □

Der noch fehlende Eintrag b der entsprechenden Restklasse $\left(\begin{smallmatrix} a & b \\ c'p & d \end{smallmatrix}\right)$ ergibt sich aus folgender Gleichung:

$$\begin{aligned} & \det \left(\begin{smallmatrix} a+a_1c'p & \tilde{b} \\ c'p & d+d_1c'p \end{smallmatrix}\right) = ad + a_1dc'p + ad_1c'p + a_1d_1c'p^2 - \tilde{b}c'p = 1 \\ \iff\ & \tilde{b} = \tfrac{ad-1}{c'p} + d_1a + a_1d_1c'p + a_1d \\ \iff\ & b = \tfrac{ad-1}{c'p} \end{aligned}$$

Für den eindeutig bestimmten Repräsentanten $d \in \{1, \ldots, c'p\}$ von $\bar{d}$ ist $da - 1$ ein Vielfaches von $c'p$, also $b \in \mathbb{Z}$, und wegen $a, d \in \{1, \ldots, c'p\}$ folgt $b \in \mathbb{Z}/c'p\mathbb{Z}$. Damit entspricht die Anzahl der Äquivalenzklassen in $\langle T \rangle \setminus \Gamma_0(p) / \langle T \rangle$ der Anzahl der $a \in \{1, \ldots, c'p\}$ mit ggt $(a, c'p) = 1$, so daß sich insgesamt ergibt:

2.22 Lemma: *Für ein festes $c \in \mathbb{N}$ gilt:*

$$b_{11}(c) = \begin{cases} \varphi(c) & \text{für } c \equiv 0 \bmod p \\ 0 & \text{sonst} \end{cases}.$$

Da $\Gamma_0(p)$ nur zwei Spitzen hat, läßt sich aus diesem Bildungsgesetz die gesamte Matrix B der Bildungsgesetze konstruieren (für die Anzahl der benötigten Eingänge vergleiche Satz 2.17). Zuerst betrachten wir die Summe der ersten Zeile nach Satz 2.14:

$$b_{11}(c) + b_{12}(c) = w_1\varphi(c) = \varphi(c)$$

mit $w_1 = 1$, so daß sich für das zweite Bildungsgesetz ergibt:

$$b_{12}(c) = \begin{cases} 0 & \text{für } c \equiv 0 \bmod p \\ \varphi(c) & \text{sonst} \end{cases}.$$

Da die Streumatrix nach Satz 2.5 symmetrisch ist und damit auch die Matrix der Bildungsgesetze, gilt $b_{21}(c) = b_{12}(c)$, so daß sich für die Summe der zweiten Zeile ergibt:

$$b_{21}(c) + b_{22}(c) = w_2\varphi(c) = p\varphi(c)$$

mit $w_2 = p$ und daher:

$$b_{22}(c) = \begin{cases} p\varphi(c) & \text{für } c \equiv 0 \bmod p \\ (p-1)\varphi(c) & \text{sonst} \end{cases} .$$

Insgesamt erhalten wir damit als Matrix B der Bildungsgesetze:

$$\left(\begin{array}{ll} b_{11}(c) = \begin{cases} \varphi(c) \\ 0 \end{cases} & b_{12}(c) = \begin{cases} 0 \\ \varphi(c) \end{cases} \\ \\ b_{21}(c) = \begin{cases} 0 \\ \varphi(c) \end{cases} & b_{22}(c) = \begin{cases} p\varphi(c) \\ (p-1)\varphi(c) \end{cases} \end{array} \right) \begin{array}{ll} \text{für} & c \equiv 0 \bmod p \\ \text{für} & c \not\equiv 0 \bmod p \\ \\ \text{für} & c \equiv 0 \bmod p \\ \text{für} & c \not\equiv 0 \bmod p \end{array}$$

Wir haben hier die Bildungsgesetze ganz elementar mit kombinatorischen Überlegungen bestimmt. In Kapitel 3 werden wir eine elegantere Methode herleiten, indem wir ausnutzen, daß $\Gamma_0(p)$ eine Kongruenzuntergruppe mit zwei Spitzen ist.
Aus diesen Bildungsgesetzen lassen sich die Einträge:

$$\varphi_{ij}(s) = \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{c \in \mathbb{N}} \frac{b_{ij}(c)}{(w_i w_j)^s c^{2s}}$$

der Streumatrix konstruieren. Um für diese Dirichlet-Reihen eine geschlosssene Darstellung beweisen zu können, beschäftigen wir uns zunächst mit den Reihen:

$$\begin{aligned} Z_{11}(s) &:= \sum_{c=1}^{\infty} \frac{b_{11}(c)}{c^{2s}} = \sum_{n=1}^{\infty} \frac{\varphi(np)}{p^{2s} n^{2s}} \\ Z_{12}(s) &:= \sum_{c=1}^{\infty} \frac{b_{12}(c)}{c^{2s}} = \sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \frac{\varphi(n)}{n^{2s}} \\ Z_{22}(s) &:= \sum_{c=1}^{\infty} \frac{b_{22}(c)}{c^{s}} = pZ_{11}(s) + (p-1)Z_{12}(s). \end{aligned}$$

Darüberhinaus werden zwei Hilfsfunktionen benötigt:

$$\begin{aligned} \Lambda_p(s) &:= \sum_{k=0}^{\infty} \tfrac{\varphi(p^k)}{p^{2ks}} \\ \Theta_p(T) &:= \sum_{k=0}^{\infty} \varphi(p^k) T^k \end{aligned}$$

mit $s, T \in \mathbb{C}$, wobei die zweite Reihe folgenden Wert hat:

2.23 Lemma: $\Theta_p(T) = \frac{1-T}{1-pT}$ *für* $|T| < \frac{1}{p}$.

Beweis:
Mit $\varphi(p^k) = (p-1)p^{k-1} = \varphi(p)p^{k-1}$ für $k \geq 1$ ergibt sich:

$$\begin{aligned}
\Theta_p(T) &= 1 + \varphi(p)\sum_{k=1}^{\infty} p^{k-1}T^k \\
&= 1 + \varphi(p)T + \varphi(p)p^{-1}\sum_{k=2}^{\infty} p^kT^k \\
&= 1 + \varphi(p)T + \frac{\varphi(p)}{p}\left(\frac{1}{1-pT} - 1 - pT\right) \quad \text{für } |pT| < 1 \\
&= 1 + (p-1)T + \frac{p-1}{p}\left(\frac{1-1+pT-pT+p^2T^2}{1-pT}\right) \\
&= 1 + (p-1)T + \frac{p-1}{p}\left(\frac{p^2T^2}{1-pT}\right) \\
&= 1 + (p-1)T + \frac{p^3T^2 - p^2T^2}{p-p^2T} \\
&= \frac{p - p^2T + p^2T - p^3T^2 - pT + p^2T^2 + p^3T^2 - p^2T^2}{p-p^2T} \\
&= \frac{p-pT}{p(1-pT)} \\
&= \frac{1-T}{1-pT}
\end{aligned}$$

□

Damit lassen sich unsere Hilfsreihen umformulieren:

2.24 Satz:

$$Z_{12}(s) = \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} \frac{\varphi(n)}{n^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)}\frac{p^{2s}-p}{p^{2s}-1} \qquad \textit{für } s \in \mathbb{C} \textit{ mit } \operatorname{Re} s > 1.$$

Beweis:

$$Z_{12}(s) = \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} \frac{\varphi(n)}{n^{2s}} = \prod_{q \text{ prim, } q\neq p} \left(1 + \frac{\varphi(q)}{q^{2s}} + \frac{\varphi(q^2)}{q^{4s}} + \ldots\right)$$

Mit $\Lambda_q(s) := \sum_{k=0}^{\infty} \frac{\varphi(q^k)}{q^{2ks}}$ folgt nun:

$$\sum_{\substack{n=1 \\ p\nmid n}}^{\infty} \frac{\varphi(n)}{n^{2s}} = \prod_{q \text{ prim, } q\neq p} \Lambda_q(s).$$

Nach Lemma 2.23 gilt: $\Theta_q(T) := \sum_{k=0}^{\infty} \varphi(q^k)T^k = \frac{1-T}{1-qT}$ für $|qT| < 1$.
Für $T = q^{-2s}$ folgt $|\frac{q}{q^{2s}}| < 1$, da $\operatorname{Re} s > 1$, und wir können Lemma 2.23 anwenden:

$$\Lambda_q(s) = \Theta_q(q^{-2s}) = \frac{1 - q^{-2s}}{1 - q^{1-2s}}$$

und insgesamt:

$$\begin{aligned}
\sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \frac{\varphi(n)}{n^{2s}} &= \prod_{q \text{ prim, } q \neq p} \frac{1 - q^{-2s}}{1 - q^{1-2s}} \\
&= \prod_{q \text{ prim, } q \neq p} \frac{1}{1 - q^{1-2s}} \prod_{q \text{ prim, } q \neq p} (1 - q^{-2s}) \\
&= \prod_{q \text{ prim}} \frac{1}{1 - q^{1-2s}} (1 - p^{1-2s}) \Big(\prod_{q \text{ prim}} \frac{1}{1 - q^{-2s}} \Big)^{-1} \frac{1}{1 - p^{-2s}} \\
&= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{1 - p^{1-2s}}{1 - p^{-2s}} \\
&= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^{2s} - p}{p^{2s} - 1}.
\end{aligned}$$

□

Eine ähnliche geschlossene Form zeigen wir jetzt für den Eintrag links oben:

2.25 Satz:

$$Z_{11}(s) = \sum_{n=1}^{\infty} \frac{\varphi(np)}{p^{2s} n^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p-1}{p^{2s}-1} \quad \textit{für } s \in \mathbb{C} \textit{ mit } \operatorname{Re} s > 1.$$

Beweis:
Jedes $n \in \mathbb{N}$ läßt sich schreiben als $n = p^k m$ für $k \in \mathbb{N} \cup \{0\}$ und $m \in \mathbb{N}$ mit $p \nmid m$. Dann gilt:

$$\varphi(np) = \varphi(p^{k+1}m) = \varphi(p^{k+1})\varphi(m) = (p-1)p^k\varphi(m)$$

und es folgt:

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{\varphi(np)}{p^{2s}n^{2s}} &= \sum_{n=1}^{\infty}\frac{(p-1)p^k\varphi(m)}{p^{2s}p^{2ks}m^{2s}} \\
&= \sum_{\substack{m=1\\ p\nmid m}}^{\infty}\sum_{k=0}^{\infty}\frac{(p-1)p^k\varphi(m)}{p^{2s}p^{2ks}m^{2s}} \\
&= \frac{p-1}{p^{2s}}\sum_{\substack{m=1\\ p\nmid m}}^{\infty}\frac{\varphi(m)}{m^{2s}}\sum_{k=0}^{\infty}\frac{p^k}{p^{2ks}} \\
&= \frac{p-1}{p^{2s}}\sum_{\substack{m=1\\ p\nmid m}}^{\infty}\frac{\varphi(m)}{m^{2s}}\sum_{k=0}^{\infty}(p^{1-2s})^k \quad \text{mit } |p^{1-2s}|<1, \text{ da } \operatorname{Re}s>1 \\
&= \frac{p-1}{p^{2s}(1-p^{1-2s})}\sum_{\substack{m=1\\ p\nmid m}}^{\infty}\frac{\varphi(m)}{m^{2s}} \\
&= \frac{p-1}{p^{2s}(1-p^{1-2s})}\frac{\zeta(2s-1)}{\zeta(2s)}\frac{1-p^{1-2s}}{1-p^{-2s}} \quad \text{mit Satz 2.24} \\
&= \frac{\zeta(2s-1)}{\zeta(2s)}\frac{p-1}{p^{2s}-1}.
\end{aligned}$$

□

Damit ergibt sich für die noch fehlende Reihe:

$$\begin{aligned}
Z_{22}(s) &= pZ_{11}(s)+(p-1)Z_{12}(s) \\
&= \frac{\zeta(2s-1)}{\zeta(2s)}\frac{1}{p^{2s}-1}[p(p-1)+(p-1)(p^{2s}-p)] \\
&= \frac{\zeta(2s-1)}{\zeta(2s)}\frac{p^{2s+1}-p^{2s}}{p^{2s}-1}.
\end{aligned}$$

Um aus diesen Reihen der Bildungsgesetze die Streumatrix für $\Gamma_0(p)$ zu erhalten, müssen wir jetzt noch die entsprechenden Normierungen berücksichtigen: Zum Einen haben wir die Bildungsgesetze für $c\in\mathbb{N}$ statt für $\tilde{c}\in\mathbb{R}^+$ ermittelt und zum Anderen fehlen uns noch die Vorfaktoren aus Definition 2.4. Nach Satz 2.1 ergibt sich für die Einträge der Streumatrix:

$$\varphi_{ij}(s)=\pi^{\frac{1}{2}}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\sum_{c\in\mathbb{N}}\frac{b_{ij}(c)}{(w_iw_j)^sc^{2s}}.$$

Mit $w_1 = 1$ und $w_2 = p$ erhalten wir hier für $\operatorname{Re} s > 1$:

$$\begin{aligned}
\varphi_{11}(s) &= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} Z_{11}(s) \\
&= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p-1}{p^{2s}-1} \\
\varphi_{12}(s) &= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{1}{p^s} Z_{12}(s) \\
&= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^s - p^{1-s}}{p^{2s}-1} \\
\varphi_{22}(s) &= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{1}{p^{2s}} Z_{22}(s) \\
&= \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p}{p^{2s}} \frac{p-1}{1-p^{-2s}} + \frac{p-1}{p^{2s}} \frac{p-1}{p^{2s}-1}
\end{aligned}$$

Die Streumatrix für $\Gamma_0(p)$ hat also die Gestalt:

$$\Phi(\Gamma_0(p), s) = \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \frac{1}{p^{2s}-1} \begin{pmatrix} p-1 & p^s - p^{1-s} \\ p^s - p^{1-s} & p-1 \end{pmatrix}$$

und für die Determinante folgt:

$$\begin{aligned}
\det \Phi(\Gamma_0(p), s) &= \left(\pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \right)^2 \frac{(p-1)^2 - (p^s - p^{1-s})^2}{(p^{2s}-1)^2} \\
&= \left(\pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \right)^2 \frac{p^2 - p^{2s-2} - p^{2s} - 1}{(p^{2s}-1)^2} \\
&= \left(\pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} \right)^2 \frac{p^{2s-2} - 1}{p^{2s}-1}.
\end{aligned}$$

Dieses Ergebnis ist bereits bekannt: Hejhal hat in [Hej83] ebenfalls die Streumatrix für $\Gamma_0(p)$ konstruiert, jedoch ohne die Einträge so zu bestimmen. Er beschreibt die Doppelnebenklassen durch Kongruenzen und nutzt gruppentheoretische Sätze, um aus dieser Beschreibung die möglichen Einträge der Doppelnebenklassen in die Eisensteinreihen hineinzuziehen. Durch diese Überlegungen kommt er dann zu der gleichen Darstellung für die Streumatrix und ihrer Determinante, wobei er seine Ergebnisse direkt für $\Gamma_0(n)$ mit $n = p_1 \cdot \ldots \cdot p_k$ formuliert:

2.26 Satz: *Die Streumatrix für $\Gamma_0(n)$ hat die Gestalt:*

$$\Phi(\Gamma_0(n), s) = \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)} N_{p_1}(s) \otimes \ldots \otimes N_{p_k}(s)$$

als Tensorprodukt von Matrizen $N_{p_i}(s)$ mit:

$$N_{p_i}(s) = \frac{1}{p_i^{2s}-1} \begin{pmatrix} p_i - 1 & p^s - p_i^{1-s} \\ p_i^s - p_i^{1-s} & p_i - 1 \end{pmatrix}.$$

Dabei liefert das Tensorprodukt $A_1 \otimes \ldots \otimes A_k$ von Matrizen $A_1, \ldots, A_k$ eine Matrix, deren Eintrag in der $i_1 \cdot \ldots \cdot i_k-$ten Zeile und $j_1 \cdot \ldots \cdot j_k-$ten Spalte gleich dem Produkt $a_{i_1 j_1} a_{i_2 j_2} \cdot \ldots \cdot a_{i_k j_k}$ ist. Die Indexmenge $J \times J$ dieser Matrix ergibt sich als Produkt der Indexmengen $I_i \times I_i$ der Matrizen A_I, also $J = I_1 \times \ldots \times I_k$. Wir haben hier nur die Streumatrix für eine Primzahl p konstruiert, aber unser Konstruktionsprinzip läßt sich auf ein $n = p_1^{l_1} \cdot \ldots \cdot p_k^{l_k}$ übertragen: $\Gamma_0(n)$ ist eine Untergruppe vom Index:

$$[\Gamma : \Gamma_0(n)] = n \prod_{i=1}^{k} (1 + \frac{1}{p_i})$$

nach Schoeneberg [Sch74]. Ein Repräsentantensystem der Spitzen besteht nach Petersson [Pet82] aus ∞ und:

$$\bigcup_{t>1, t|n} R_t,$$

wobei R_t ein volles Restsystem modulo ggt (t^2, n) unter den $k \in \mathbb{Z}$ mit $0 \leq k \leq n-1$ und ggt $(k, n) = 1$ bezeichnet und $\varphi(\text{ggt } (t, \frac{n}{t}))$ Elemente hat. Alle Spitzen eines Restklassensystems haben dieselbe Breite:

$$N_t := \min\{m \in \mathbb{N} : t^2 m \equiv 0(n)\}.$$

Jetzt lassen sich die Bildungsgesetze analog konstruieren und in der Streumatrix zusammenfassen.

3 Die Streumatrix für Gruppen $\Delta < \Lambda < \Gamma$

Die bisher gezeigten Ergebnisse für die Streumatrix wollen wir nun verallgemeinern, indem wir eine Zwischengruppe:

$$\Delta \leq \Lambda \leq \Gamma$$

betrachten. Zunächst werden wir uns mit den Spitzenmengen dieser beiden Gruppen beschäftigen und die dabei gewonnenen Erkenntnisse nutzen, um die Streumatrix von Λ aus der Streumatrix von Δ zu konstruieren.

3.1 Konstruktion der Streumatrix von Λ aus der Streumatrix von Δ

Sei $r(\Delta)$ die Spitzenanzahl von Δ, $S(\Delta)$ ein zugehöriges Repräsentantensystem und $r(\Lambda)$ die Spitzenanzahl von Λ mit dem Repräsentantensystem:

$$S(\Lambda) := [s_1, \ldots, s_{r(\Lambda)}]$$

und den zugehörigen Spitzenbreiten:

$$W(\Lambda) := [w_1, \ldots, w_{r(\Lambda)}].$$

Wir stellen $S(\Delta)$ jetzt so dar, daß diejenigen Spitzen von Δ, die unter Λ zueinander äquivalent sind, beieinander stehen:

$$S(\Delta) = [\underbrace{\underbrace{s_1^1 = s_1, s_1^2, \ldots, s_1^{r_1}}_{\sim_\Lambda s_1}}_{:=S_1(\Delta)}, \underbrace{\underbrace{s_2^1 = s_2, s_2^2, \ldots, s_2^{r_2}}_{\sim_\Lambda s_2}}_{:=S_2(\Delta)}, \ldots, \underbrace{\underbrace{s_{r(\Lambda)}^1 = s_{r(\Lambda)}, s_{r(\Lambda)}^2, \ldots, s_{r(\Lambda)}^{r_{r(\Lambda)}}}_{\sim_\Lambda s_{r(\Lambda)}}}_{:=S_{r(\Lambda)}(\Delta)}].$$

Dann gilt $|S_i(\Delta)| = r_i$ und es gibt $\lambda_i^j \in \Lambda$ mit $\lambda_i^j s_i = s_i^j$ für $i \in \{1, \ldots, r(\Lambda)\}$. Die Breite der Spitze s_i^j von Δ in Γ sei w_i^j.
Darüberhinaus existieren zu den Spitzen $s_1, \ldots, s_{r(\Lambda)}$ von Λ nach Satz 1.10 Matrizen $g_i \in \Gamma$ mit $g_i\infty = s_i$ und $g_i^{-1}\,\mathrm{Stab}_\Lambda(s_i)g_i = \{T^{w_i n} : n \in \mathbb{Z}\}$ für

$i \in \{1, \ldots, r(\Lambda)\}$, wobei w_i die Breite der Spitze s_i ist. Es ergeben sich damit folgende Zusammenhänge nach Lemma 1.12:

$$[\mathrm{Stab}_\Gamma(s_i^j) : \mathrm{Stab}_\Delta(s_i^j)] = w_i^j$$

und:

$$[\mathrm{Stab}_\Gamma(s_i^j) : \mathrm{Stab}_\Lambda(s_i^j)] = w_i.$$

Wir wollen jetzt den neuen Begriff der *relativen Spitzenbreite* einer Spitze s_i^j von Δ in Λ einführen:

3.1 Definition: *Die relative Spitzenbreite einer Spitze von $\Delta < \Lambda$ in Λ sei:*

$$v_i^j := [\mathrm{Stab}_\Lambda(s_i^j) : \mathrm{Stab}_\Delta(s_i^j)].$$

3.2 Bemerkung: *Wegen*

$$[\mathrm{Stab}_\Gamma(s_i^j) : \mathrm{Stab}_\Delta(s_i^j)] = [\mathrm{Stab}_\Gamma(s_i^j) : \mathrm{Stab}_\Lambda(s_i^j)] \cdot [\mathrm{Stab}_\Lambda(s_i^j) : \mathrm{Stab}_\Delta(s_i^j)]$$

gilt offensichtlich $w_i | w_i^j$ und es existiert ein $v_i^j \in \mathbb{N}$ mit:

$$v_i^j = \frac{w_i^j}{w_i}.$$

Darüberhinaus gilt:

$$\mathrm{Stab}_\Delta(s_i^j) = \lambda_i^j \, \mathrm{Stab}_\Delta(s_i)(\lambda_i^j)^{-1}.$$

Der bisherige Begriff der Spitzenbreite gibt also die relative Spitzenbreite einer Spitze in Bezug auf die ganze Modulgruppe Γ an, in der alle Spitzen zueinander äquivalent sind. Dieses Konzept haben wir jetzt dergestalt verallgemeinert, daß jede Spitze $s_i^j \in S_i$ von Δ eine relative Spitzenbreite v_i^j bezüglich Λ zur Spitze s_i hat. Dann hat die Spitze $s_i^j \in S_i(\Delta)$ die relative Spitzenbreite w_i^j bezüglich Γ zur Spitze ∞ und jede Spitze s_i von Λ hat die relative Spitzenbreite w_i bezüglich Λ zur Spitze ∞.
Dies nutzen wir, um Satz 2.7 zu verallgemeinern: In diesem Satz hatten wir Γ ausgedrückt durch die Untergruppe Λ als:

$$\Gamma = \bigcup_{i=1}^{r(\Lambda)} \bigcup_{l=1}^{w_i} \Delta g_i T^l.$$

Dabei hat Γ nur eine Äquivalenzklasse von Spitzen und wir haben Γ bezüglich der Spitze ∞ zerlegt. Wenn wir jetzt Λ durch Δ ausdrücken wollen, hat die

Obergruppe Δ gegebenenfalls mehrere Spitzen in Γ. Daher läßt sich Λ bezüglich einer Spitze $s_k \in S(\Lambda)$ folgendermaßen zerlegen:

3.3 Satz: *Seien $\Delta \leq \Lambda$ Untergruppen von Γ mit endlichem Index, zugehörigen Spitzenvektoren:*

$$S(\Lambda) = [s_1 = \infty, s_2 = g_2\infty, \ldots, s_{r(\Lambda)} = g_{r(\Lambda)}\infty]$$

und:

$$\begin{aligned} S(\Delta) \;=\; & [s_1^1 = s_1, s_1^2 = \lambda_1^2 s_1, \ldots, s_1^{r_1} \lambda_1^{r_1} s_1, \\ & s_2^1 = s_2, s_2^2 = \lambda_2^2 s_2, \ldots, s_2^{r_2} = \lambda_2^{r_2} s_2, \quad \ldots \quad , \\ & s_{r(\Lambda)}^1 = s_{r(\Lambda)}, s_{r(\Lambda)}^2 = \lambda_{r(\Lambda)}^2 s_{r(\Lambda)}, \ldots, s_{r(\Lambda)}^{r_{r(\Lambda)}} = \lambda_{r(\Lambda)}^{r_{r(\Lambda)}} s_{r(\Lambda)}] \end{aligned}$$

mit den relativen Spitzenbreiten:

$$W(\Delta) = [v_1^1, v_1^2, \ldots, v_1^{r_1}, \quad \ldots \quad , v_{r(\Lambda)}^1, \ldots, v_{r(\Lambda)}^{r_{r(\Lambda)}}]$$

von Δ in Λ. Dann läßt sich Λ bezüglich einer Spitze $s_k \in S(\Lambda)$ durch Δ ausdrücken als:

$$\Lambda = \bigcup_{l=1}^{r_k} \bigcup_{n=1}^{v_k^l} \Delta \lambda_k^l g_k T^n g_k^{-1}.$$

Beweis:
Wir zeigen diesen Satz, indem wir den Beweis von Satz 2.7 verallgemeinern:

„$\subseteq$“ Sei $\lambda \in \Lambda$ und zeige $\lambda \in \bigcup_{l=1}^{r_k} \bigcup_{n=1}^{v_k^l} \Delta \lambda_k^l g_k T^n g_k^{-1}$. Zu λs_k existiert ein $l \in \{1, \ldots, r_k\}$ mit $\lambda s_k \sim_\Delta s_k^l$, also muß ein $\delta \in \Delta$ existieren mit:

$$\begin{aligned} & \lambda s_k = \delta s_k^l = \delta \lambda_k^l s_k \text{ wegen } \lambda_k^l s_k = s_k^l \\ \Leftrightarrow \quad & s_k = \lambda^{-1} \delta \lambda_k^l s_k, \end{aligned}$$

so daß $\lambda^{-1}\delta\lambda_k^l$ im Stabilisator $\mathrm{Stab}_\Lambda(s_k) = g_k \langle T^{w_k} \rangle g_k^{-1}$ liegt. Damit existiert ein $m \in \mathbb{Z}$ mit $\lambda^{-1}\delta\lambda_k^l = g_k T^{-mw_k} g_k^{-1}$, also folgt:

$$\lambda = \delta \lambda_k^l g_k T^{mw_k} g_k^{-1}.$$

Modulo v_k^l gerechnet existieren $a \in \mathbb{Z}, b \in \{1, \ldots, v_k^l\}$ mit $mw_k = av_k^l + b$ und:

$$\lambda = \delta \lambda_k^l g_k T^{av_k^l + b} g_k^{-1} = \delta (\lambda_k^l g_k T^{v_k^l} g_k^{-1} (\lambda_k^l)^{-1})^a \lambda_k^l g_k T^b g_k^{-1}.$$

Wegen $\delta \in \Delta$ und $\lambda_k^l g_k T^{v_k^l} g_k^{-1} (\lambda_k^l)^{-1} \in \mathrm{Stab}_\Delta(s_k^l) \subset \Delta$ folgt:

$$\lambda \in \bigcup_{n=1}^{v_k^l} \Delta \lambda_k^l g_k T^n g_k^{-1}.$$

„$\supseteq$“ Sei $\lambda \in \bigcup_{l=1}^{r_k} \bigcup_{n=1}^{v_k^l} \Delta\lambda_k^l g_k T^n g_k^{-1}$ und zeige $\lambda \in \Lambda$. Dies ist offensichtlich, da aus $\lambda \in \bigcup_{l=1}^{r_k} \bigcup_{n=1}^{v_k^l} \Delta\lambda_k^l g_k T^n g_k^{-1}$ folgt, daß $l \in \{1, \ldots, r_k\}$ und $n \in \{1, \ldots, v_k^l\}$ existieren mit $\lambda \in \Delta\lambda_k^l g_k T^n g_k^{-1} \subset \Lambda$.

□

Diese Zerlegung ist disjunkt, so daß sich folgendes Korollar ergibt:

3.4 Korollar: *Unter den gleichen Vorausetzungen wie in Satz 3.3 folgt:*

$$[\Lambda : \Delta] = \sum_{l=1}^{r_k} v_k^l.$$

Beweis:
In Korollar 2.8 zu Satz 2.7 haben wir gezeigt, daß die Zerlegung von Γ bezüglich einer Untergruppe Δ disjunkt ist. Der Beweis verläuft hier analog, indem wir zeigen, daß es zu einer Matrix $g \in \Lambda$ nur ein $i \in \{1, \ldots, v_k^l\}$ gibt mit $g \in \Delta\lambda_k^l g_k T^n g_k^{-1}$. □

Insgesamt erhalten wir:

$$\begin{array}{rcccl} [\Gamma : \Delta] & = & \sum_{i=1}^{r(\Lambda)} \sum_{j=1}^{r_i} w_i^j & = & \sum_{i=1}^{r(\Lambda)} \sum_{j=1}^{r_i} w_i v_i^j \\ & = & \sum_{i=1}^{r(\Lambda)} w_i \sum_{j=1}^{r_i} v_i^j & = & [\Gamma : \Lambda][\Lambda : \Delta]. \end{array}$$

Die bisher gewonnenen Erkenntnisse wollen wir nun benutzen, um die Streumatrix von Λ aus der Streumatrix von Δ zu bestimmen. Daher sei:

$$\Phi(\Delta, s) := \left(\varphi_{ik}^{jl}(\Delta, s)\right)$$

$$\text{für } i, k \in \{1, \ldots, r(\Lambda)\}, j \in \{1, \ldots, r_i\}, l \in \{1, \ldots, r_k\}$$

mit den konstanten Termen $\varphi_{ik}^{jl}(\Delta, s)$ der Eisensteinreihe zur Spitze s_i^j entwickelt in der Spitze s_k^l:

$$\varphi_{ik}^{jl}(\Delta, s) := \pi^{\frac{1}{2}} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \frac{1}{(w_i^j w_k^l)^s} \sum_{c=1}^{\infty} \frac{b_{ik}^{jl}(c)}{c^{2s}}$$

mit:

$$b_{ik}^{jl}(c) := \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \left\langle T^{w_i^j} \right\rangle \backslash g_i^{-1} (\lambda_i^j)^{-1} \Delta \lambda_k^l g_k / \left\langle T^{w_k^l} \right\rangle \right\} \right|,$$

da aus:

$$\lambda_i^j s_i = s_i^j \text{ und } g_i \infty = s_i$$

folgt, daß:

$$\lambda_i^j g_i \infty = s_i^j.$$

Die Streumatrix zur Obergruppe Λ sei wie bisher notiert als:

$$\Phi(\Lambda, s) := (\varphi_{ik}(\Lambda, s))_{i,k\in\{1,\ldots,r(\Lambda)\}}$$

für:

$$\varphi_{ik}(\Lambda, s) := \pi^{\frac{1}{2}} \frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)} \frac{1}{(w_i w_k)^s} \sum_{c=1}^{\infty} \frac{b_{ik}(c)}{c^{2s}}$$

mit:

$$b_{ik}(c) := |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i}\rangle \backslash g_i^{-1}\Lambda g_k / \langle T^{w_k}\rangle\right\}|.$$

Wir drücken die Anzahlen der Doppelnebenklassen b_{ik} durch die b_{ik}^{jl} all der Spitzen von Δ aus, die $\Lambda-$ äquivalent zu s_i bzw. s_k sind:

3.5 Satz: *Unter den gleichen Voraussetzungen wie in Satz 3.3 gilt*

$$v_i^j b_{ik}(c) = \sum_{l=1}^{r_k} b_{ik}^{jl}(c).$$

Beweis:
Mit der zu s_i^j gehörenden Matrix $\lambda_i^j \in \Lambda$ und Satz 3.3 läßt sich Λ bezüglich der Spitze s_k zerlegen:

$$\Lambda = (\lambda_i^j)^{-1}\Lambda = \bigcup_{l=1}^{r_k}\bigcup_{n=1}^{v_k^l} \Delta\lambda_k^l g_k T^n g_k^{-1}.$$

Jetzt benutzen wir die Zerlegung von Λ, um b_{ik} umzuformen:

$$\begin{aligned}
b_{ik}(c) &= |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i}\rangle \backslash g_i^{-1}\Lambda g_k / \langle T^{w_k}\rangle\right\}| \\
&= |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i}\rangle \backslash \textstyle\bigcup_{l=1}^{r_k}\bigcup_{n=1}^{v_k^l} g_i^{-1}(\lambda_i^j)^{-1}\Delta\lambda_k^l g_k T^n g_k^{-1} g_k / \langle T^{w_k}\rangle\right\}| \\
&= \textstyle\sum_{l=1}^{r_k}\sum_{n=1}^{v_k^l} |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i}\rangle \backslash g_i^{-1}(\lambda_i^j)^{-1}\Delta\lambda_k^l g_k T^n / \langle T^{w_k}\rangle\right\}| \\
&= \textstyle\sum_{l=1}^{r_k} |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i}\rangle \backslash g_i^{-1}(\lambda_i^j)^{-1}\Delta\lambda_k^l g_k T^n / \langle T^{w_k v_k^l}\rangle\right\}| \\
&= \textstyle\sum_{l=1}^{r_k} |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i}\rangle \backslash g_i^{-1}(\lambda_i^j)^{-1}\Delta\lambda_k^l g_k T^n / \langle T^{w_k^l}\rangle\right\}|
\end{aligned}$$

da aus $v_k^l = \frac{w_k^l}{w_k}$ folgt, daß $w_k v_k^l = w_k^l$ gilt. Mit $v_i^j = \frac{w_i^j}{w_i}$ erhalten wir:

$$\begin{aligned}
v_i^j b_{ik}(c) &= \textstyle\sum_{l=1}^{r_k} |\left\{[\left(\begin{smallmatrix}\star & \star\\ c & \star\end{smallmatrix}\right)] \in \langle T^{w_i^j}\rangle \backslash g_i^{-1}(\lambda_i^j)^{-1}\Delta\lambda_k^l g_k T^n / \langle T^{w_k^l}\rangle\right\}| \\
&= \textstyle\sum_{l=1}^{r_k} b_{ik}^{jl}.
\end{aligned}$$

□

Dabei ist zu beachten, daß in der rechten Seite kein $j \in \{1, \ldots, r_i\}$ auftaucht, diese Summation gilt also für jede fest gewählte Position j der einzelnen Bildungsgesetze. Anschaulich besitzt $B(\Delta, s) = (b_{ik}^{jl})$ mit $i, k \in \{1, \ldots, r(\Lambda)\}$ und $j \in \{1, \ldots, r_i\}$, $l \in \{1, \ldots, r_k\}$ folgende Struktur:

$$B(\Delta, s) = \left(\begin{array}{c|cccc} & s_1^1 \ldots s_1^{r_1} & s_2^1 \ldots s_2^{r_2} & \ldots & s_{r(\Lambda)}^1 \ldots s_{r(\Lambda)}^{r_{r(\Lambda)}} \\ \hline s_1^1 \\ \vdots \\ s_1^{r_1} & \begin{array}{c} b_{11}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_1\}} \\ {\scriptstyle l \in \{1,\ldots,r_1\}} \end{array} & \begin{array}{c} b_{12}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_1\}} \\ {\scriptstyle l \in \{1,\ldots,r_2\}} \end{array} & \ldots & \begin{array}{c} b_{1r(\Lambda)}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_1\}} \\ {\scriptstyle l \in \{1,\ldots,r_{r(\Lambda)}\}} \end{array} \\ s_2^1 \\ \vdots \\ s_2^{r_2} & \begin{array}{c} b_{21}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_2\}} \\ {\scriptstyle l \in \{1,\ldots,r_1\}} \end{array} & \begin{array}{c} b_{22}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_2\}} \\ {\scriptstyle l \in \{1,\ldots,r_2\}} \end{array} & \ldots & \begin{array}{c} b_{2r(\Lambda)}^{jl} \\ {\scriptstyle j \in \{2,\ldots,r_2\}} \\ {\scriptstyle l \in \{1,\ldots,r_{r(\Lambda)}\}} \end{array} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{r(\Lambda)}^1 \\ \vdots \\ s_{r(\Lambda)}^{r_{r(\Lambda)}} & \begin{array}{c} b_{r(\Lambda)1}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_{r(\Lambda)}\}} \\ {\scriptstyle l \in \{1,\ldots,r_1\}} \end{array} & \begin{array}{c} b_{r(\Lambda)2}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_{r(\Lambda)}\}} \\ {\scriptstyle l \in \{1,\ldots,r_2\}} \end{array} & \ldots & \begin{array}{c} b_{r(\Lambda)r(\Lambda)}^{jl} \\ {\scriptstyle j \in \{1,\ldots,r_{r(\Lambda)}\}} \\ {\scriptstyle l \in \{1,\ldots,r_{r(\Lambda)}\}} \end{array} \end{array}\right)$$

Dabei ergeben die Zeilen- oder Spaltensummen innerhalb eines Blockes die gesuchten Bildungsgesetze der Obergruppe:

$$v_i^j b_{ik} = \sum_{l=1}^{r_k} b_{ik}^{jl} \text{ für alle } j \in \{1, \ldots, r_i\} \text{ fest}$$

bzw.:

$$v_k^l b_{ik} = \sum_{j=1}^{r_i} b_{ik}^{jl} \text{ für alle } l \in \{1, \ldots, r_k\} \text{ fest.}$$

3.2 Die Streumatrix der Modulgruppe

Die im ersten Abschnitt gezeigten Ergebnisse über die Streumatrix einer Gruppe Δ lassen sich selbstverständlich hier wiederfinden: Dazu setzen wir die Obergruppe Λ gleich der ganzen Modulgruppe Γ, die nur eine Spitzenklasse hat. Als Repräsentant wählen wir ∞ mit dem zugehörigen Stabilisator:

$$\mathrm{Stab}_\Gamma(\infty) = \Gamma(\infty) = \{T^n : n \in \mathbb{Z}\}.$$

Daher hat die Spitze $s_1 = \infty$ die Breite 1 und die Streumatrix hat nur einen Eintrag $\varphi_{11}(s)$. Wir bestimmen jetzt $b_{11}(c)$ für ein $c \in \mathbb{N}$ als die Anzahl der Äquivalenzklassen in der Doppelnebenklasse $\Gamma(\infty)\backslash\Gamma/\Gamma(\infty)$. Zwei Elemente aus

Γ liegen genau dann in derselben Äquivalenzklasse, wenn sie sich durch Multiplikation mit T^{n_1} von rechts und mit T^{n_2} von links für $n_1, n_2 \in \mathbb{Z}$ ineinander überführen lassen. Wie bereits in Lemma 2.15 beschrieben, gibt es zu einen $c \in \mathbb{N}$ genau $\varphi(c)$ Doppelnebenklassen, so daß die Matrix der Bildungsgesetze folgende Gestalt hat:

$$B := (b_{11}(c)) = \varphi(c).$$

Damit erhalten wir für die eindimensionale Streumatrix:

$$\varphi_{11}(s) = \pi^{\frac{1}{2}} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \sum_{c=1}^{\infty} \frac{\varphi(c)}{c^{2s}}.$$

Gerade für diese Reihe können wir selbstverständlich eine geschlossene Form finden, indem wir:

$$Z(s) := \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^{2s}}$$

betrachten und folgenden Satz analog zu den entsprechenden Sätzen 2.24 und 2.25 zeigen:

3.6 Satz:

$$Z(s) = \frac{\zeta(2s-1)}{\zeta(2s)} \textit{ für } s \in \mathbb{C} \textit{ mit } \operatorname{Re} s > 1.$$

Beweis:
Da $\varphi(mn) = \varphi(m)\varphi(n)$ für $m, n \in \mathbb{N}$ mit ggt $(m, n) = 1$ gilt, ergibt sich:

$$Z(s) = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^{2s}} = \prod_{q \text{ prim}} (1 + \frac{\varphi(q)}{q^{2s}} + \frac{\varphi(q^2)}{q^{4s}} + \ldots).$$

Mit $\Lambda_q(s) := \sum_{k=0}^{\infty} \frac{\varphi(q^k)}{q^{2ks}}$ folgt nun:

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^{2s}} = \prod_{q \text{ prim}} \Lambda_q(s).$$

Nach Lemma 2.23 gilt $\Theta_q(T) := \sum_{k=0}^{\infty} \varphi(q^k) T^k = \frac{1-T}{1-qT}$ für $|qT| < 1$.
Für $T = q^{-2s}$ folgt $|\frac{q}{q^{2s}}| < 1$, da $\operatorname{Re} s > 1$. Wir erhalten:

$$\Lambda_q(s) = \Theta_q(q^{-2s}) = \frac{1 - q^{-2s}}{1 - q^{1-2s}}$$

und insgesamt gilt:

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^{2s}} &= \prod_{q \text{ prim}}\frac{1-q^{-2s}}{1-q^{1-2s}}\\ &= \prod_{q \text{ prim}}\frac{1}{1-q^{1-2s}}\prod_{q \text{ prim}}(1-q^{-2s})\\ &= \frac{\zeta(2s-1)}{\zeta(2s)},\end{aligned}$$

wie in Satz 2.11 bereits gezeigt. □

Wir erhalten damit für die Streumatrix der Modulgruppe:

3.7 Satz: *Für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$ gilt:*

$$\Phi(\Gamma, s) = \pi^{\frac{1}{2}}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\frac{\zeta(2s-1)}{\zeta(2s)}.$$

Eine alternative Herleitung der Streumatrix der Modulgruppe findet sich z.B. bei Kubota [Kub73].
Da es nur eine $\Gamma-$Äquivalenzklasse von Spitzen gibt, lassen sich die Spitzen der Untergruppe Δ mit $r_1 := r$ angeben als:

$$S(\Delta) = [s_1^1 = \infty, s_1^2 = g_1^2 s_1, \ldots, s_1^r = g_1^r s_1].$$

Mit $s_i := s_1^i$ und $g_i := g_1^i$ entspricht dies genau unserer bisherigen Notation:

$$S(\Delta) = [s_1 = \infty, s_2 = g_2 s_1, \ldots, s_r = g_r s_1].$$

Die relativen Spitzenbreiten von Δ in Γ sind genau die bisherigen Spitzenbreiten:

$$W(\Delta) := [w_1 := v_1^1, \ldots, w_r := v_1^r]$$

und für die Bildungsgesetze läßt sich die Notation ebenfalls vereinfachen zu:

$$b_{11}^{jl} =: b_{jl} \quad \text{für } j, l \in \{1, \ldots, r\}.$$

Bezüglich $\Gamma-$äquivalenter Spitzen gibt es nur einen Block in der Streumatrix von Δ und die Anwendung von Satz 3.5 liefert für $c \in \mathbb{N}$:

$$w_l b_{11}(c) = \sum_{j=1}^{r} b_{11}^{jl} = \sum_{j=1}^{r} b_{jl}.$$

Genau diese Aussage haben wir in Satz 2.14 bereits gezeigt.

3.3 Folgerungen

Mit Satz 3.5 lassen sich die Einträge der Streumatrix aus den Einträgen der Streumatrix einer Untergruppe konstruieren und wir können als erste Folgerung direkt die Streumatrix für zykloide Gruppen, also für Gruppen mit genau einer Spitzenklasse, angeben: Sei $\Delta < \Gamma$ eine zykloide Gruppe mit $S(\Delta) = \{s_1 = \infty\}$ und $W(\Delta) = [w_1]$, so daß nach Korollar 2.8 folgt: $[\Gamma : \Delta] = w_1$. Die Streumatrix hat nur einen Eintrag und für das zugehörige Bildungsgesetz $b_{11}^{11}(c)$ gilt nach Satz 3.5:

$$w_1 b_{11}(c) = b_{11}^{11}(c),$$

wobei $b_{11}(c) = \varphi(c)$ das eine Bildungsgesetz der Streumatrix von Γ ist, wir erhalten hier also:

$$b_{11}^{11}(c) = w_1 \varphi(c)$$

und haben damit folgenden Satz hergeleitet:

3.8 Satz: *Sei $\Delta < \Gamma$ eine zykloide Gruppe mit $S(\Delta) = \{s_1 = \infty\}$ und $W(\Delta) = [w_1]$. Dann folgt für die Streumatrix:*

$$\Phi(\Delta, s) = w_1 \Phi(\Gamma, s) = w_1 \pi^{\frac{1}{2}} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)}$$

für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$.

Diese Gestalt der Streumatrix wurde auch von Petersson [Pet82] für Kongruenzuntergruppen mit einer Spitze und allgemeiner für zykloide Untergruppen von Venkov [Ven81] bestimmt, der dieselbe Aussage über einen Vergleich von Eisensteinreihen zeigt. Wir werden jetzt diese Aussage verallgemeinern, indem wir zwei Gruppen Δ und Λ mit denselben Spitzenklassen betrachten, für die wir also die gleichen Repräsentanten wählen können. Dabei müssen Δ und Λ nicht notwendig Kongruenzuntergruppen sein.

3.9 Satz: *Seien $\Delta < \Lambda$ Untergruppen von Γ mit $S(\Delta) = S(\Lambda) = [s_1, \ldots, s_r]$. Die Streumatrix von Δ ergibt sich aus der Streumatrix von Λ durch Multiplikation mit dem Index $[\Lambda : \Delta]$:*

$$\Phi(\Delta, s) = [\Lambda : \Delta] \Phi(\Gamma, s) = \left([\Lambda : \Delta] \varphi_{ij}(s) \right)_{1 \le i,j \le r}$$

für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$.

Beweis:
Da beide Gruppen dieselben Spitzenklassen haben, folgt mit Satz 3.5 sofort:

$$v_i^1 b_{ij} = b_{ij}^{11} \text{ für alle } i, j \in \{1, \ldots, r\},$$

wobei b_{ij} die Bildungsgesetze von Λ, b_{ij}^{11} die Bildungsgesetze von Δ sind und v_i^1 die relative Breite der Spitze s_i von Δ in Λ ist. Da wir in Korollar 3.4 gesehen haben, daß sich der Index $[\Lambda : \Delta]$ als Summe der relativen Breiten der unter Λ zueinander äquivalent werdenden Spitzen ergibt, erhalten wir hier:

$$[\Lambda : \Delta] = \sum_{k=1}^{1} v_i^k \text{ für alle } i \in \{1, \ldots, r\},$$

also sind alle relativen Breiten identisch und gleich dem Index. □

3.10 Beispiele: Die folgenden Gruppen Δ_i mit $1 \leq i \leq 3$ sind alle Untergruppen der Kongruenzuntergruppe Λ vom Level 2, erzeugt von

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \right\}$$

mit dem Spitzenvektor $S(\Lambda) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right]$, Spitzenbreiten $W(\Lambda) = [2, 1]$ und $[\Gamma : \Lambda] = 3$. Für alle Untergruppen läßt ihre Streumatrix angeben als:

$$\Phi(\Delta_i, s) = [\Lambda : \Delta_i]\Phi(\Lambda, s).$$

1. Sei Δ_1 die Untergruppe erzeugt von:

   $$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 5 & -2 \end{pmatrix}, \begin{pmatrix} 2 & -5 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 8 & -5 \\ 13 & -8 \end{pmatrix}, \begin{pmatrix} 4 & -5 \\ 5 & -6 \end{pmatrix}, \begin{pmatrix} 8 & -13 \\ 5 & -8 \end{pmatrix} \right\}.$$

   Δ_1 ist eine Nichtkongruenzuntergruppe vom Index 15 mit dem Spitzenvektor $S(\Delta_1) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right]$, Spitzenbreiten $W(\Delta_1) = [10, 5]$, also mit dem erweiterten Level $n(\Delta_1) = 10$, und mit $[\Lambda : \Delta_1] = 5$.

2. Sei Δ_2 erzeugt von

   $$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 5 & -2 \end{pmatrix}, \begin{pmatrix} 4 & -7 \\ 7 & -12 \end{pmatrix}, \begin{pmatrix} 2 & -7 \\ 3 & -10 \end{pmatrix}, \begin{pmatrix} 4 & -11 \\ 3 & -8 \end{pmatrix} \right\}.$$

   Δ_2 ist eine Nichtkongruenzuntergruppe vom Index 18 mit dem Spitzenvektor $S(\Delta_2) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right]$, Spitzenbreiten $W(\Delta_2) = [12, 6]$, also mit dem erweiterten Level $n(\Delta_2) = 12$, und mit $[\Lambda : \Delta_2] = 6$.

3. Sei Δ_3 erzeugt von

   $$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 4 & -7 \end{pmatrix}, \begin{pmatrix} 2 & -5 \\ 5 & -12 \end{pmatrix}, \begin{pmatrix} 8 & -5 \\ 13 & -8 \end{pmatrix}, \begin{pmatrix} 2 & -7 \\ 3 & -10 \end{pmatrix} \right\}.$$

Δ_3 ist eine Nichtkongruenzuntergruppe vom Index 18 mit dem Spitzenvektor $S(\Delta_3) = \left[\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\right]$, Spitzenbreiten $W(\Delta_3) = [12, 6]$, also mit dem erweiterten Level $n(\Delta_3) = 12$, und mit $[\Lambda : \Delta_3] = 6$.

Falls nicht die kompletten Spitzenvektoren von Δ und Λ übereinstimmen, können wir Satz 3.5 immerhin auf solche Gruppen übertragen, bei denen mindestens eine Spitzenklasse übereinstimmt:

3.11 Satz: *Seien $\Delta < \Lambda$ Untergruppen von Γ mit zugehörigen Spitzenvektoren $S(\Lambda) := [s_1, \ldots, s_{r(\Lambda)}]$ und:*

$$S(\Delta) = [s_1^1 = s_1, s_1^2, \ldots, s_1^{r_1}, s_2^1 = s_2, s_2^2, \ldots, s_2^{r_2}, \ldots, s_{r(\Lambda)}^2, \ldots, s_{r(\Lambda)}^{r_{r(\Lambda)}}].$$

Darüberhinaus existiere ein $r_k \in \{r_1, \ldots, r_{r(\Lambda)}\}$ mit $r_k = 1$. Dann ergeben sich für $i \in \{1, \ldots, r(\Lambda)\}$ die zugehörigen Bildungsgesetze $b_{ik}(c)$ von Λ als:

$$v_i^j b_{ik}(c) = b_{ik}^{j1}(c).$$

Beweis:
Ein Repräsentant der $k-$ten Spitzenklasse von Λ ist die Spitze s_k und wir wählen in $S(\Delta)$ für die Klasse von s_k^1 denselben Repräsentanten, also $s_k = s_k^1$. Für $i \in \{1, \ldots, r(\Lambda)\}$ folgt mit Satz 3.5:

$$v_i^j b_{ik}(c) = \sum_{l=1}^{r_k} b_{ik}^{1l}(c) = b_{ik}^{j1}(c)$$

für ein beliebiges $j \in \{1, \ldots, r(\Lambda)\}$. □

Damit finden wir weitere Nichtkongruenzgruppen, für die wir mit Satz 3.5 zumindest Teile der Streumatrix konstruieren können: Seien $\Delta < \Lambda$ Untergruppen von Γ, Λ eine Kongruenzgruppe vom Level n und Δ keine Kongruenzgruppe. In den zugehörigen Spitzenvektoren $S(\Lambda) := [s_1, \ldots, s_{r(\Lambda)}]$ und:

$$S(\Delta) = [s_1^1 = s_1, s_1^2, \ldots, s_1^{r_1}, s_2^1 = s_2, s_2^2, \ldots, s_2^{r_2}, \ldots, s_{r(\Lambda)}^2, \ldots, s_{r(\Lambda)}^{r_{r(\Lambda)}}]$$

existiere ein $r_k \in \{r_1, \ldots, r_{r(\Lambda)}\}$ mit $r_k = 1$. Die Bildungsgesetze von Λ lassen sich aus den Bildungsgesetzen von $\Gamma(n)$ konstruieren und damit sind die $b_{ik}(c)$ Vielfache der Euler'schen $\varphi-$Funktion, so daß dies auch für die Bildungsgesetze $b_{ik}^{j1}(c)$ für $j \in \{1, \ldots, r(\Lambda)\}$ von Δ gilt, also für alle Einträge der $k-$ten Zeile und $k-$ten Spalte der Streumatrix. Die kleinste Spitzenzahl von Λ für diese Konstellation ist 3 und wir geben hier einige Beispielgruppen aus unserer Datenbank an:

3.12 Beispiele: Die folgenden Gruppen sind, ebenso wie die in Beispiel 3.10 betrachteten Gruppen mit zwei Spitzen, Untergruppen der Kongruenzuntergruppe Λ vom Level 2, erzeugt von:

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \right\}$$

mit dem Spitzenvektor $S(\Lambda) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right]$ und Spitzenbreiten $W(\Lambda) = [2, 1]$. Damit ist $r(\Lambda) = 2$ und die Streumatrix von Λ läßt sich aus der Matrix:

$$B(\Lambda) = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

der Bildungsgesetze konstruieren.

1. Sei Δ_1 die Untergruppe erzeugt von:

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & -3 \end{pmatrix}, \begin{pmatrix} 2 & 9 \\ -1 & -4 \end{pmatrix} \right\}.$$

Δ_1 ist eine Nichtkongruenzuntergruppe vom Index 9 mit dem Spitzenvektor $S(\Delta_1) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right]$ und Spitzenbreiten $W(\Delta_1) = [6, 2, 1]$, also mit dem erweiterten Level $n(\Delta_1) = 6$. Es gilt $r_1 = 1$, unter Λ werden also außer den bereits $\Delta-$äquivalenten Spitzen keine weiteren Spitzen zu ∞ äquivalent. Für die Matrix der Bildungsgesetze ergibt sich folgende Struktur:

$$B(\Delta) = \left(\begin{array}{c|ccc} & s_1^1 & s_2^1 & s_2^2 \\ \hline s_1^1 & b_{11}^{11} & b_{12}^{11} & b_{12}^{12} \\ s_2^1 & b_{21}^{11} & b_{22}^{11} & b_{22}^{12} \\ s_2^2 & b_{21}^{21} & b_{22}^{21} & b_{22}^{22} \end{array} \right)$$

Einen Teil dieser Bildungsgesetze bestimmen wir jetzt mit Satz 3.11 für $k = 1$:

$$v_i^j b_{i1}(c) = b_{i1}^{j1}$$

mit $v_i^j = \frac{w_i^j}{w_i}$. Wir erhalten zunächst die erste Spalte und wegen der Symmetrie auch die erste Zeile:

$$B(\Delta) = \left(\begin{array}{c|ccc} & s_1^1 & s_2^1 & s_2^2 \\ \hline s_1^1 & v_1^1 b_{11} & v_2^1 b_{21} & v_2^2 b_{21} \\ s_2^1 & v_2^1 b_{21} & b_{22}^{11} & b_{22}^{12} \\ s_2^2 & v_2^2 b_{21} & b_{22}^{21} & b_{22}^{22} \end{array} \right)$$

mit $v_1^1 = \frac{6}{2} = 3, v_2^1 = \frac{2}{1} = 2$ und $v_2^2 = \frac{1}{1} = 1$.

2. Sei Δ_2 erzeugt von:

$$\left\{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 4 \end{pmatrix}, \begin{pmatrix} 2 & -3 \\ 3 & -4 \end{pmatrix}\right\}.$$

Δ_2 ist eine Nichtkongruenzuntergruppe vom Index 9 mit dem Spitzenvektor $S(\Delta_2) = \left[\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\right]$ und Spitzenbreiten $W(\Delta_2) = [4, 2, 3]$, also mit dem erweiterten Level $n(\Delta_2) = 12$. Hier gilt $r_2 = 1$, unter Λ werden außer den bereits $\Delta-$äquivalenten Spitzen keine weiteren Spitzen zu $\begin{bmatrix}1\\1\end{bmatrix}$ äquivalent. Damit erhalten wir mit Satz 3.11 für $k = 2$ die zweite Spalte und die zweite Zeile der Streumatrix von Δ aus der Streumatrix von Λ:

$$v_i^j b_{i2}(c) = b_{i2}^{j1}$$

mit $v_i^j = \frac{w_i^j}{w_i}$, so daß folgt:

$$B(\Delta) = \left(\begin{array}{c|ccc} & s_1^1 & s_1^2 & s_2^1 \\ \hline s_1^1 & b_{11}^{11} & b_{11}^{12} & v_1^1 b_{12} \\ s_1^2 & b_{11}^{21} & b_{11}^{22} & v_2^1 b_{12} \\ s_2^1 & b_{21}^{11} & b_{21}^{12} & v_2^2 b_{22} \end{array}\right)$$

mit $v_1^1 = \frac{4}{2} = 2, v_2^1 = \frac{3}{1} = 3$ und $v_2^2 = \frac{2}{1} = 2$.

Das Konzept der relativen Spitzenbreiten können wir auch benutzen, um für Kongruenzuntergruppen einige Aussagen über den Vektor der Spitzenbreiten einfacher herzuleiten, als dies in der Literatur bisher möglich war. Durch die Teilbarkeiten, die sich aus den relativen Spitzenbreiten ergeben und die zugehörigen Aussagen über die Indexe der Stabilisatoren sehen wir, daß die Spitzenbreiten einer Kongruenzuntergruppe nur zwischen ggt $(W(\Delta))$ und kgV $(W(\Delta)) = n$ liegen können, und daß es zu jeder Grenze eine Spitze mit der entsprechenden Breite geben muß.

4 Die Streumatrix für Hauptkongruenzuntergruppen $\Gamma(p)$

Im ersten Kapitel haben wir *Kongruenzuntergruppen* eingeführt als solche Untergruppen $\Delta < \Gamma$ mit endlichem Index, die für ein $n \in \mathbb{N}$ die *Hauptkongruenzuntergruppe*:

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2,\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod n \right\}$$

enthalten. Im vorherigen Kapitel haben wir gesehen, wie sich die Streumatrix einer Gruppe Δ aus der Streumatrix einer ihrer Untergruppen konstruieren läßt. Um dieses Konzept auf Kongruenzuntergruppen anwenden zu können, wollen wir in diesem Kapitel die Streumatrix für die Hauptkongruenzuntergruppen bestimmen, so daß wir aus diesen Daten die Streumatrix einer Kongruenzuntergruppe aus der Streumatrix ihrer Hauptkongruenzuntergruppe herleiten können.
Dazu werden wir uns in diesem Kapitel mit der Streumatrix von $\Gamma(p)$ für eine Primzahl p beschäftigen. Im folgenden Kapitel verallgemeinern wir die dabei gewonnenen Erkenntnisse, um die Streumatrix von $\Gamma(n)$ zu konstruieren.
Dabei möchten wir die Struktur der Spitzenmenge einer Hauptkongruenzgruppe verstehen und die Anzahlen der Doppelnebenklassen $b_{ij}(c)$ für $c \in \mathbb{N}$ mit dieser Struktur in Verbindung bringen, um so einfache Kongruenzen für die Bildungsgesetze zu erhalten. Andere Ansätze, z.B. von Hejhal [Hej76, Hej83] führen zu allgemeinen Formeln, ohne auf die Struktur der Streumatrix näher einzugehen.
Zunächst stellen wir aber fest, daß sich für Hauptkongruenzgruppen die Anzahl der benötigten Bildungsgesetze weiter reduzieren läßt, da sie Normalteiler sind und damit alle Spitzen dieselbe Breite haben (vergleiche 1.13). Normale Untergruppen der Modulgruppe wurden unter anderem von Newmann untersucht und klassifiziert [New64, New63, New67].

4.1 Satz: *Sei Δ ein Normalteiler von Γ mit r Spitzen der Breite w und Bildungsgesetzen $b_{11}, \ldots, b_{1r}$. Dann sind die Bildungsgesetze $b_{i1}, \ldots, b_{ir}$ der $i-$ten Zeile für $2 \leq i \leq r$ eine Permutation der Gesetze der ersten Zeile.*

Beweis:
Seien $i, j \in \{1, \ldots, r\}$ und $s_i = \begin{bmatrix} x_i \\ y_i \end{bmatrix}, s_j = \begin{bmatrix} x_j \\ y_j \end{bmatrix} \in S := \Delta \setminus \mathbb{P}^1(\mathbb{Q})$ Spitzen von Δ mit den zugehörigen Matrizen $g_i = \begin{pmatrix} x_i & u_i \\ y_i & v_i \end{pmatrix}, g_j = \begin{pmatrix} x_j & u_j \\ y_j & v_j \end{pmatrix} \in \Gamma$ nach Satz 1.10. Für $c \in \mathbb{N}$ ist $b_{ij}(c)$ definiert als:

$$b_{ij}(c) = |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus g_i^{-1}\Delta g_j / \langle T^w \rangle\right\}|.$$

Um $b_{ij}(c)$ durch ein schon bekanntes Bildungsgesetz der ersten Zeile zu beschreiben, drücken wir jetzt g_j durch g_i aus: Da in Γ alle Spitzen zueinander äquivalent sind, existiert ein $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ mit $\gamma s_j = s_i$ und es folgt:

$$g_i s_i = g_i \gamma s_j = \infty.$$

Damit bilden sowohl g_j als auch $g_i\gamma$ die Spitze s_j auf unendlich ab, und da Matrizen mit dieser Eigenschaft eindeutig bis auf Multiplikation mit T^n von rechts bestimmt sind, existiert ein $m \in \mathbb{Z}$ mit $g_j = g_i \gamma T^m$. Dann existiert eine Spitze $s \in \mathbb{P}^1(\mathbb{Q})$ mit $\gamma T^m s = \infty$ und da s in einer der Spitzenklassen von Δ liegt, ist s $\Delta-$äquivalent zu einem Repräsentanten aus $S(\Delta)$. Es existieren also ein $\delta \in \Delta$ und ein $k \in \{1, \ldots, r\}$ mit $\delta s_k = s$. Daher folgt:

$$\gamma T^m \delta s_k = \gamma T^m s = \infty,$$

bis auf Translation mit T^n für ein $n \in \mathbb{Z}$ entspricht γT^m der zur Spitze s_k gehörenden Matrix g_k. Da die Anzahl der Doppelnebenklassen unabhängig von der Wahl der Matrix g_k ist, bedeutet dies für b_{ij}:

$$\begin{aligned} b_{ij}(c) &= |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus g_i^{-1}\Delta g_j / \langle T^w \rangle\right\}| \\ &= |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus g_i^{-1}\Delta g_i \gamma T^k / \langle T^w \rangle\right\}| \\ &= |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus \Delta \gamma T^k / \langle T^w \rangle\right\}| \\ &= |\left\{[\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus \Delta g_k / \langle T^w \rangle\right\}| \\ &= b_{1k}(c) \end{aligned}$$

für ein $k \in \{1, \ldots, r\}$. □

Wir wissen mit Satz 4.1 nur, daß zu einem beliebigen Bildungsgesetz b_{ij} ein $k \in \{1, \ldots, r\}$ existiert mit $b_{ij} = b_{1k}$. Wie diese Permutationen der Bildungsgesetze genau aussehen, werden wir in diesem und im nächsten Kapitel für spezielle Normalteiler, nämlich für Hauptkongruenzgruppen, untersuchen. Unabhänging von den vorherigen Überlegungen sehen wir sofort, daß bei den Hauptkongruenzuntergruppen auf der Hauptdiagonalen der Streumatrix immer derselbe Eintrag steht:

4.2 Lemma: *Sei Δ ein Normalteiler von Γ mit r Spitzen der Breite w und Bildungsgesetzen $b_{11}, \ldots, b_{1r}$. Dann gilt:*

$$b_{jj} = b_{11}$$

für alle $1 \leq j \leq r$.

Beweis:
Mit der zur Spitze $s_j \in S(\Delta)$ gehörenden Matrix $g_j \in \Gamma$ nach Satz 1.10 ist b_{jj} definiert als:

$$\begin{aligned} b_{jj}(c) &= \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus g_j^{-1} \Delta g_j / \langle T^w \rangle \right\} \right| \\ &= \left| \left\{ [\left(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix}\right)] \in \langle T^w \rangle \setminus \Delta / \langle T^w \rangle \right\} \right| \\ &= b_{11}(c). \end{aligned}$$

□

Nach diesen allgemeinen Vorbemerkungen sei jetzt p eine ungerade Primzahl und wir betrachten die Hauptkongruenzuntergruppe $\Gamma(p)$ mit dem Index:

$$\mu := [\Gamma : \Gamma(p)] = \frac{p(p^2-1)}{2}$$

und:

$$r := \frac{\mu}{p} = (p+1)\frac{p-1}{2}$$

inäquivalenten Spitzen. Die Spitzenmenge $S := S(\Gamma(p)) = [s_1, \ldots, s_r]$ enthalte Repräsentanten der r Klassen von Spitzen aus:

$$S_p := \Gamma(p) \setminus \mathbb{P}^1(\mathbb{Q}),$$

die alle die gleiche Spitzenbreite p haben. Um die Spitzenklassen S_p so anzuordnen, daß sich für die zugehörigen Bildungsgesetze eine gewisse Struktur ergibt, sind zwei Schritte notwendig: Zunächst werden wir S_p in Blöcke sortieren und dann innerhalb jeden Blockes die Restklassen gemäß der zugehörigen Bildungsgesetze anordnen.

4.1 Eine Blockstruktur der Spitzenmenge

Um eine spezielle Anordnung der Spitzenklassen zu erreichen, parametrisieren wir als erstes $S_p := \Gamma(p) \setminus \mathbb{P}^1(\mathbb{Q})$:

$$\begin{array}{rccc} \lambda_p : & \mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_p) \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & \begin{bmatrix} x \\ y \end{bmatrix}_p := \begin{bmatrix} x \bmod p \\ y \bmod p \end{bmatrix} \end{array}$$

mit $\mathbb{P}^1(\mathbb{F}_p) = \{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \ldots, \left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right]\}$. Die Fasern der $p+1$ Elemente aus $\mathbb{P}^1(\mathbb{F}_p)$ haben die Gestalt:

$$\begin{array}{rcl} \lambda_p^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]) & = & \{\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{F}) : y \equiv 0(p)\} \\ \lambda_p^{-1}(\left[\begin{smallmatrix}t\\1\end{smallmatrix}\right]) & = & \{\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{F}) : x \equiv yt(p), y \not\equiv 0(p)\}, \quad t \in \{0, 1, \ldots, p-1\}. \end{array}$$

Urbilder aus verschiedenen Fasern lassen sich nicht durch Elemente von $\Gamma(p)$ ineinander überführen, denn für $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma(p)$ und $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{F})$ folgt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} \equiv \begin{bmatrix} x \\ y \end{bmatrix} (p).$$

Damit erhalten wir auf den Spitzenklassen folgende Abbildung:

$$\begin{array}{rccc} \lambda: & \Gamma(p) \backslash \mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_p) \\ & \overline{\begin{bmatrix} x \\ y \end{bmatrix}} & \longmapsto & \begin{bmatrix} x \\ y \end{bmatrix}_p := \begin{bmatrix} x \bmod p \\ y \bmod p \end{bmatrix}. \end{array}$$

λ ist wohldefiniert, denn zu zwei Repräsentanten $s_1 = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, s_2 = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ der gleichen Nebenklasse modulo p existiert ein $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma(p)$ mit:

$$\gamma s_1 = \begin{bmatrix} ax_1 + by_1 \\ cx_1 + dy_1 \end{bmatrix} = s_2 = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$$

und wegen $a \equiv 1(p), b \equiv 0(p), c \equiv 0(p), d \equiv 1(p)$ folgt:

$$\begin{array}{rcccl} ax_1 + by_1 \bmod p & = & x_1 \bmod p & = & x_2 \bmod p \\ cx_1 + dy_1 \bmod p & = & y_1 \bmod p & = & y_2 \bmod p. \end{array}$$

Die Abbildung λ ist offensichtlich surjektiv, da jedes Element aus $\mathbb{P}^1(\mathbb{F}_p)$ seine Entsprechung in $\mathbb{P}^1(\mathbb{Q})$ besitzt.
Für den nächsten Schritt benötigen wir zwei Untergruppen von $\Gamma_p := \mathrm{PSL}(2, \mathbb{F}_p)$, die *Borel-Gruppe*:

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{F}_p) \right\}$$

und die normale Untergruppe:

$$B_1 := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{F}_p) \right\} \lhd B,$$

deren Quotient B/B_1 wir mit der zyklischen Gruppe der Ordnung $\frac{p-1}{2}$ identifizieren:

$$\begin{array}{rccc} \eta: & B/B_1 & \longrightarrow & \mathbb{F}_p^\star/\{\pm 1\} \\ & \left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right] & \longmapsto & a. \end{array}$$

Dabei ist η wohldefiniert, da zu zwei Repräsentanten $\beta_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \beta_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ einer Klasse $\left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right]$ ein $\beta = \begin{pmatrix} 1 & \tilde{b} \\ 0 & 1 \end{pmatrix} \in \mathrm{B}$ existiert mit:

$$\beta\beta_1 = \begin{pmatrix} a_1 & b_1 + a_1\tilde{b} \\ 0 & d_1 \end{pmatrix} = \beta_2,$$

so daß $a_1 = a_2$.

4.3 Lemma: *Die Abbildung η ist eine Bijektion.*

Beweis:
Um die Injektivität zu zeigen, seien $\beta_1, \beta_2 \in B$ mit $\eta(\beta_1) = \eta(\beta_2) = a$, also $\beta_1 = \begin{pmatrix} a & b_1 \\ 0 & d_1 \end{pmatrix}, \beta_2 = \begin{pmatrix} a & b_2 \\ 0 & d_2 \end{pmatrix}$ für $b_1, b_2, d_1, d_2 \in \mathbb{F}_p$. Da die Determinante den Wert 1 hat und das multiplikativ Inverse in $\mathbb{F}_p$ eindeutig ist, folgt $d_1 = a^{-1} = d_2$, so daß ein $\beta \in B$ existiert mit $\beta_1\beta = \beta_2$, die beiden Matrizen liegen also in B/B_1 in der gleichen Restklasse.
Da sich jedes $a \in \mathbb{F}_p^\star/\{\pm 1\}$ zu einer Matrix $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in B$ ergänzen läßt, ist η auch surjektiv und damit eine Bijektion. □

Wir haben gesehen, daß B/B_1 genau $\frac{p-1}{2}$ Nebenklassen besitzt. Indem wir jede Faser von λ mit dieser Gruppe identifizieren, zeigen wir, daß jede Faser genau $\frac{p-1}{2}$ Restklassen enthält.
Zunächst betrachten wir die Faser von ∞:

$$\lambda^{-1}([\tfrac{1}{0}]) = \{[\tfrac{x}{y}] \in \mathbb{P}^1(\mathbb{F}_p) : y \equiv 0(p)\}$$

und bilden sie in den Quotienten B/B_1 ab:

$$\begin{aligned} \psi: \quad \lambda^{-1}([\tfrac{1}{0}]) \subset S_p \quad &\longrightarrow \qquad B/B_1 \\ \overline{\begin{bmatrix} x \\ y \end{bmatrix}} \qquad &\longmapsto \quad \left[\begin{pmatrix} x & b \\ 0 & d \end{pmatrix}\right], \end{aligned}$$

indem $[\tfrac{x}{y}]$ mit Korollar 1.3 zu einer Matrix $\beta = \left(\begin{smallmatrix} x & b \\ y & d \end{smallmatrix}\right) \in \Gamma$ mit $\beta[\tfrac{1}{0}] = [\tfrac{x}{y}]$ und $p|y$ ergänzt wird, wobei diese Ergänzung nach Satz 1.10 eindeutig bis auf Multiplikation mit T^n von rechts ist. Dann ergibt die Reduktion der Einträge modulo p von β eine Matrix $\rho(\beta) \in B$, die bis auf Multiplikation mit Elementen aus B_1 eindeutig bestimmt ist.
Um zu sehen, daß diese Zuordnung wohldefiniert ist, betrachten wir zwei Repräsentanten $s_1 = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, s_2 = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ der gleichen Nebenklasse, d.h. es existiert

ein $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(p)$ mit $\gamma s_1 = s_2$. Wir ergänzen s_1 zu einer Matrix $\beta_1 = \begin{pmatrix} x & b_1 \\ y & d_1 \end{pmatrix}$ mit $p|y$ und $\beta_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = s_1$, also $\gamma\beta_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = s_2$. Für die entsprechende Matrix $\beta_2 \in B$, zu der sich s_2 ergänzen läßt, gilt für ein $n \in \mathbb{N}$:

$$\beta_2 = \gamma\beta_1 T^n = \begin{pmatrix} ax_1 + by_1 & ab_1 + bd_1 \\ cx_1 + dy_1 & cb_1 + dd_1 \end{pmatrix} T^n.$$

Reduktion modulo p ergibt wegen $a \equiv 1(p), b \equiv 0(p), c \equiv 0(p), d \equiv 1(p)$:

$$\begin{pmatrix} ax_1 + by_1 & ab_1 + bd_1 \\ cx_1 + dy_1 & cb_1 + dd_1 \end{pmatrix} T^n \bmod p = \begin{pmatrix} x & b_1 \\ y & d_1 \end{pmatrix} T^{n \bmod p}$$

mit $T^{n \bmod p} \in B_1$.

4.4 Lemma: *Die Abbildung ψ ist eine Bijektion.*

Beweis:
Seien $s_1, s_2 \in \lambda^{-1}([\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}])$ mit $\psi(s_1) = \psi(s_2) = [(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix})]$. Dann existiert ein $\beta \in B$ mit $\rho(\beta_1) = \rho(\beta_2)\beta$, die Reduktion modulo p der Ergänzungen von s_1, s_2 zu Matrizen unterscheidet sich also nur durch Multiplikation mit einer Matrix aus B_1. Somit existiert ein $\gamma \in \Gamma(p)$ mit $\beta_1 = \gamma\beta_2 T^n$ und es folgt $s_1 = \gamma s_2$. Also liegen s_1, s_2 in derselben Restklasse von $S_p = \Gamma(p) \setminus \mathbb{P}^1(\mathbb{Q})$ und ψ ist injektiv.
Da sich jedes $a \in \mathbb{F}_p^\star$ zu einer Matrix $\beta \in B$ ergänzen läßt und $s := [\begin{smallmatrix} a \\ 0 \end{smallmatrix}] \mathbb{P}^1(\mathbb{F}_p)$ seine Entsprechung in $\mathbb{P}^1(\mathbb{Q})$ besitzt, ist ψ surjektiv. □

Die Hintereinanderausführung der beiden Abbildungen liefert eine Bijektion:

$$f: \quad \lambda^{-1}([\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}]) \quad \longrightarrow \quad \mathbb{F}_p^\star / \{\pm 1\}.$$

Damit hat $\lambda^{-1}([\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}])$ genau $\frac{p-1}{2}$ Elemente, oder anders ausgedrück hat $\Gamma(p)$ genau $\frac{p-1}{2}$ Bahnen in der Faser von ∞.
Γ operiert transitiv auf $\mathbb{P}^1(\mathbb{Q})$, so daß sich die bisherigen Überlegungen für die Faser von unendlich auf die anderen Fasern übertragen lassen. Wir definieren:

$$\begin{array}{rccc} g: & \lambda^{-1}([\begin{smallmatrix} x \\ y \end{smallmatrix}]) & \longrightarrow & \lambda^{-1}([\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}]) \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & \left[g_{x,y}^{-1} \begin{bmatrix} x \\ y \end{bmatrix} \right]_p, \end{array}$$

indem $[\begin{smallmatrix} x \\ y \end{smallmatrix}] \in \mathbb{P}^1(\mathbb{F}_p)$ eindeutig bis auf Multiplikation mit T^n von rechts zu einer Matrix $g_{x,y} = (\begin{smallmatrix} x & b \\ y & d \end{smallmatrix}) \in \Gamma$ ergänzt wird mit $g_{x,y}[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}] = [\begin{smallmatrix} x \\ y \end{smallmatrix}]$ und anschließend $g_{x,y}$ modulo p reduziert wird. Da Γ transitiv auf $\mathbb{P}^1(\mathbb{Q})$ operiert, ist g bijektiv und liefert:

$$\tilde{f} := f \circ g: \quad \lambda^{-1}([\begin{smallmatrix} x \\ y \end{smallmatrix}]) \xrightarrow{g} \quad \lambda^{-1}([\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}]) \quad \xrightarrow{f} \quad \mathbb{F}_p^\star / \{\pm 1\}.$$

Damit haben wir gezeigt, daß in jeder der $p+1$ Fasern von λ genau $\frac{p-1}{2}$ Bahnen von $\Gamma(p)$ liegen und wir können jetzt die $(p+1)\frac{p-1}{2}$ Spitzenklassen von $\Gamma(p)$ nach den Fasern sortieren:

$$\tilde{S}_p =: \{\underbrace{[s_1],\ldots,[s_{\frac{p-1}{2}}]}_{\in\lambda^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right])},\underbrace{[s_{\frac{p-1}{2}+1}],\ldots,[s_{2\frac{p-1}{2}}]}_{\in\lambda^{-1}(\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right])},\ldots,\underbrace{[s_{p\frac{p-1}{2}+1}],\ldots,[s_{(p+1)\frac{p-1}{2}}]}_{\in\lambda^{-1}(\left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right])}\}$$

mit dem geordneten Vektor von Repräsentanten:

$$\tilde{S} =: [\underbrace{s_1,\ldots,s_{\frac{p-1}{2}}}_{\in\lambda^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right])},\underbrace{s_{\frac{p-1}{2}+1},\ldots,s_{2\frac{p-1}{2}}}_{\in\lambda^{-1}(\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right])},\ldots,\underbrace{s_{p\frac{p-1}{2}+1},\ldots,s_{(p+1)\frac{p-1}{2}}}_{\in\lambda^{-1}(\left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right])}].$$

4.2 Bildungsgesetze zu den einzelnen Blöcken

Nachdem wir im vorherigen Abschnitt die Spitzenmenge S nach den Fasern $\lambda^{-1}(\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right])$ sortiert haben, bestimmen wir in diesem Abschnitt für die Spitzen aus jedem Block die zugehörigen Bildungsgesetze. Nach Satz 4.1 benötigen wir nur die Bildungsgesetze der ersten Zeile:

$$b_{1j}(c) = |\,\{[\left(\begin{smallmatrix}\star&\star\\c&\star\end{smallmatrix}\right)] \in \langle T^p\rangle \setminus \Gamma(p)g_j/\langle T^p\rangle\}\,|$$

für $j \in \{1,\ldots,r\}$ und $c \in \mathbb{N}$. Zunächst werden wir b_{1j} für solche Spitzen s_j bestimmen, die in der Faser von ∞ liegen, und danach für $s_j \in \lambda^{-1}(\left[\begin{smallmatrix}t\\1\end{smallmatrix}\right])$ mit $t \in \{0,1,\ldots,p-1\}$.

4.2.1 Ein Bildungsgesetz für Spitzen aus der Faser von unendlich

Sei $s_j = \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \lambda^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right])$, also mit $p|y$. Wir untersuchen für ein $c' \in \mathbb{N}$ die Anzahl der Doppelnebenklassen:

$$b_{1j}(c') = |\,\{[\left(\begin{smallmatrix}\star&\star\\c'&\star\end{smallmatrix}\right)] \in \langle T^p\rangle \setminus \Gamma(p)g_j/\langle T^p\rangle\}\,|.$$

Dabei ist $g_j = \begin{pmatrix}x & z_1\\ y & z_2\end{pmatrix}$ nach Satz 1.10 eindeutig bis auf Multiplikation mit T^n von rechts bestimmt, so daß wir hier g_j so wählen können, daß $z_1 \equiv 0(p)$. Für $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in \Gamma$ folgt:

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} g_j = \begin{pmatrix}ax+by & az_i+bz_2\\ cx+dy & cz_1+dz_2\end{pmatrix}$$

und wegen $c \equiv 0(p)$ und $y \equiv 0(p)$ gilt immer $cx+dy \equiv 0(p)$. Es kann also nur dann Repräsentanten einer Doppelnebenklasse geben, wenn die linke untere Ecke kongruent 0 modulo p ist. Wir erhalten als erstes Ergebnis:

4.5 Lemma:

$$b_1 j(c') = 0 \quad \text{für } c' \not\equiv 0(p).$$

Sei im Weiteren $c' \in \mathbb{N}$ mit $c' \equiv 0(p)$ fest.
Um die zugehörige Anzahl der Doppelnebenklassen zu bestimmen, wollen wir eine Bijektion zwischen den Doppelnebenklassen und einer uns besser bekannten Menge herstellen. Dazu identifizieren wir jede Klasse zunächst mit ihrem oberen linken Eintrag, den wir modulo $c'p$ reduzieren:

$$\begin{array}{rccc} \Theta_{j,c'}: & \langle T^p\rangle \setminus \Gamma(p) g_j / \langle T^p\rangle & \longrightarrow & (\mathbb{Z}/c'p\mathbb{Z})^\star \\ & \left[\begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix}\right] & \longmapsto & \alpha \bmod c'p. \end{array}$$

Diese Abbildung ist wohldefiniert, denn zu $\gamma_1, \gamma_2 \in \Gamma$ mit:

$$\gamma_1 g_j = \begin{pmatrix} \alpha_1 & \beta_1 \\ c' & \delta_1 \end{pmatrix}, \gamma_2 g_j = \begin{pmatrix} \alpha_2 & \beta_2 \\ c' & \delta_2 \end{pmatrix}$$

aus derselben Doppelnebenklasse, also mit $[\gamma_1 g_j] = [\gamma_2 g_j] = \left[\left(\begin{smallmatrix} \alpha & \beta \\ c' & \delta \end{smallmatrix}\right)\right]$, existieren $n_1, n_2 \in \mathbb{N}$ mit:

$$T^{n_1 p} \gamma_1 g_j T^{n_2 p} = \gamma_2 g_j.$$

Ausmultiplizieren ergibt:

$$\begin{pmatrix} \alpha_1 + c' n_1 p & \beta_1 + \delta_1 n_1 p + \alpha_1 n_2 p + c' n_1 n_2 p^2 \\ c' & \delta_1 + c' n_2 p \end{pmatrix} = \begin{pmatrix} \alpha_2 & \beta_2 \\ c' & \delta_2 \end{pmatrix},$$

also $\alpha_1 + c' n_1 p = \alpha_2$ oder $\alpha_1 \equiv \alpha_2(c'p)$.

4.6 Lemma: *Die Abbildung $\Theta_{j,c'}$ ist injektiv.*

Beweis:
Wir wählen $\gamma_1, \gamma_2 \in \Gamma(p)$ mit $\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \gamma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ mit gleichem Bild unter $\Theta_{j,c'}$, also mit $a_1 x + b_1 y \equiv a_2 x + b_2 y (c'p)$, und zeigen $[\gamma_1 g_1] = [\gamma_2 g_2]$, also die Existenz von $n_1, n_2 \in \mathbb{Z}$ mit $T^{pn_1} \gamma_1 g_1 T^{pn_2} = \gamma_2 g_2$.
Wegen $a_1 x + b_1 y \equiv a_2 x + b_2 y (c'p)$ existiert ein $n_1 \in \mathbb{Z}$ mit:

$$a_1 x + b_1 y + c' p n_1 = a_2 x + b_2 y,$$

also stimmen die ersten Spalten von $T^{pn_1} \gamma_1 g_1$ und $\gamma_2 g_2$ überein. Aus $c_1, c_2 \equiv 0(p)$ und $d_1, d_2 \equiv \pm 1(p)$ erhalten wir $c_1 z_1 + d_1 z_2 \equiv \pm z_2(p)$ und $c_2 z_1 + d_2 z_1 \equiv \pm z_2(p)$, so daß ein $n_2 \in \mathbb{Z}$ existiert mit $c_1 z_1 + d_1 z_2 + p n_2 = c_2 z_1 + d_2 z_1$. Dann stimmen die unteren linken Einträge von $\gamma_1 g_1 T^{pn_2}$ und von $\gamma_2 g_2$ überein, so daß wir insgesamt $T^{pn_1} \gamma_1 g_1 T^{pn_2} = \gamma_2 g_2$ erhalten. □

Da $\Theta_{j,c'}$ schon injektiv ist, suchen wir jetzt eine Teilmenge von $(\mathbb{Z}/c'p\mathbb{Z})^\star$ so, daß wir eine Bijektion erhalten. Dazu sei:

$$U_{j,c'} := \{\alpha \in (\mathbb{Z}/c'p\mathbb{Z})^\star : \alpha \equiv \pm\bar{x}(p)\}$$

mit $x \equiv \bar{x}(p)$ und $\bar{x} \in \{-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}\}$. Dabei kann $\bar{x}$ nicht Null sein, da $y \equiv 0(p)$ und ggt $(x, y) = 1$. Wir betrachten:

$$\tilde{\Theta}_{j,c'} : \ \langle T^p\rangle \setminus \Gamma(p)g_j/\langle T^p\rangle \ \longrightarrow \ U_{j,c'}$$

und zeigen, daß dies ein Isomorphismus ist, indem wir die noch fehlende Surjektivität beweisen:

4.7 Lemma: *Die Abbildung $\tilde{\Theta}_{j,c'}$ ist surjektiv.*

Beweis:
Sei $\alpha \in (\mathbb{Z}/c'p\mathbb{Z})^\star$ mit $\alpha \equiv \pm\bar{x}(p)$. Wir zeigen, daß ein Repräsentant θ der Klasse:

$$\left[\begin{pmatrix}\alpha & \beta\\ c' & \delta\end{pmatrix}\right] \in \langle T^p\rangle \setminus \Gamma(p)g_j/\langle T^p\rangle$$

existiert mit:

$$\theta = \begin{pmatrix}\alpha & \beta\\ c' & \delta\end{pmatrix} = \begin{pmatrix}a & b\\ c' & d\end{pmatrix}\begin{pmatrix}x & z_1\\ y & z_2\end{pmatrix} \in \Gamma(p)g_j \Leftrightarrow \begin{pmatrix}\alpha & \beta\\ c' & \delta\end{pmatrix}\Gamma(p)g_j^{-1} \in \Gamma(p).$$

Wir zeigen also, daß $\beta, \gamma \in \mathbb{Z}$ existieren mit:

$$\begin{pmatrix}\alpha & \beta\\ c' & \delta\end{pmatrix}\begin{pmatrix}z_2 & -z_1\\ -y & x\end{pmatrix} = \begin{pmatrix}\alpha z_2 - \beta y & -\alpha z_1 + \beta x\\ c'z_2 - \delta y & -c'z_1 + \delta x\end{pmatrix} \in \Gamma(p).$$

Wir wählen $\delta \equiv \alpha^{-1}(p)$ und $\beta \equiv 0(p)$, also z.B. $\delta = \alpha^{-1}$ und $\beta = 0$ und zeigen, daß mit $\theta = \begin{pmatrix}\alpha & 0\\ c' & \alpha^{-1}\end{pmatrix}$ die Behauptung folgt. Dazu müssen folgende Äquivalenzen gelten:

1.	$\alpha z_2 - \beta y \equiv \pm 1(p)$	$\Leftrightarrow$	$\alpha z_2 \equiv \pm 1(p)$ da $y \equiv 0(p)$	$\Leftrightarrow$	$z_2 \equiv \pm\alpha^{-1}(p)$
2.	$-\alpha z_1 + \beta x \equiv 0(p)$		erfüllt, da $\beta = 0$ und $p \mid z_1$		
3.	$c'z_2 - \delta y \equiv 0(p)$		erfüllt, da $p \mid c', p \mid z_1$		
4.	$-c'z_1 + \delta x \equiv \pm 1(p)$	$\Leftrightarrow$	$\delta x \equiv 0(p)$, da $c' \equiv 0(p)$		
		$\Leftrightarrow$	$\alpha^{-1}x \equiv \pm 1(p)$, da $\delta \equiv \alpha^{-1}(p)$	$\Leftrightarrow$	$x \equiv \pm\alpha(p)$

Da g_j die Determinante 1 hat, folgt mit $xz_2 - yz_1 = 1$:

$$xz_2 - yz_1 \equiv 1(p) \Leftrightarrow xz_2 \equiv 1(p), \text{ da } y \equiv 0(p) \Leftrightarrow z_2 \equiv x^{-1}.$$

Mit $\alpha \equiv \pm\bar{x}(p)$ erhalten wir $x \equiv \bar{x}(p)$, so daß $x \equiv \pm\alpha(p)$ (die 4. Äquivalenz) erfüllt ist und mit $z_2 \equiv x^{-1}(p)$ auch $z_2 \equiv x^{-1} \equiv \pm\alpha^{-1}(p)$ (die 1. Äquivalenz). □

Jetzt haben wir unsere gesuchte Anzahl $b_{1j}(c')$ mit der Anzahl der Elemente in $U_{j,c'}$ identifiziert. Für $c' = c_0 p^l$ mit $c_0, l \in \mathbb{Z}$ und $p \nmid c_0$ folgt:

$$|\,(\mathbb{Z}/c'p\mathbb{Z})^\star\,| = \varphi(c'p) = \varphi(c_0 p^{l+1}) = p^l(p-1)\varphi(c_0) = p\varphi(c_0 p^l).$$

Für die Anzahl derjenigen Elemente in $(\mathbb{Z}/c'p\mathbb{Z})^\star$, die kongruent $\pm\bar{x} \bmod p$ sind, ergeben sich genau $\frac{p-1}{2}$ dieser Möglichkeiten, da:

$$x \equiv 0, \pm 1, \ldots, \pm\frac{p-1}{2}$$

alle Möglichkeiten sind, kongruent $\bmod p$ zu sein. Damit erhalten wir:

$$|U_{j,c'}| = \frac{1}{\frac{p-1}{2}} p\varphi(c') = \frac{2p}{p-1}\varphi(c')$$

und wir haben insgesamt folgenden Satz hergeleitet:

4.8 Satz: *Sei s_j eine Spitze aus der Faser von unendlich. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \frac{2p}{p-1}\varphi(c) & \text{für } c \equiv 0(p) \\ 0 & \text{für } c \not\equiv 0(p) \end{cases}$$

für $c \in \mathbb{N}$.

4.2.2 Ein Bildungsgesetz für Spitzen aus den übrigen Fasern

Mit ähnlichen Überlegungen wollen wir jetzt für eine Spitze $s_j = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \lambda^{-1}(\left[\begin{smallmatrix} t \\ 1 \end{smallmatrix}\right])$ mit $t \in \{0, \ldots, p-1\}$ die Anzahl der Doppelnebenklassen für $c' \in \mathbb{N}$ untersuchen:

$$b_{1j}(c') = |\,\{[\left(\begin{smallmatrix} \star & \star \\ c' & \star \end{smallmatrix}\right)] \in \langle T^p\rangle \setminus \Gamma(p) g_j / \langle T^p\rangle\}\,|.$$

Da s_j in der Faser $\lambda^{-1}(\left[\begin{smallmatrix} t \\ 1 \end{smallmatrix}\right])$ liegt, gilt $x \equiv yt(p)$ und $y \not\equiv 0(p)$, also $y \equiv \bar{y}$ für ein $\bar{y} \in \{1, \ldots, p-1\}$. Dabei läßt sich $g_j = \begin{pmatrix} x & z_1 \\ y & z_2 \end{pmatrix}$ nach Korollar 1.3 so wählen, daß $z_1 \equiv \bar{y}(p)$ und $z_2 \equiv 0(p)$. Für $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ folgt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} g_j = \begin{pmatrix} ax+by & az_1+bz_2 \\ cx+dy & cz_1+dz_2 \end{pmatrix}$$

und wegen $c \equiv 0(p)$ und $d \equiv \pm 1(p)$ gilt immer $cx + dy \equiv \pm y(p)$. Es kann also nur dann Repräsentanten einer Doppelnebenklasse geben, wenn die linke untere Ecke kongruent 0 modulo p ist:

4.9 Lemma:

$$b_{1j}(c') = 0 \quad \textit{für } c' \not\equiv \pm y(p).$$

Sei im Weiteren $c' \in \mathbb{N}$ mit $c' \equiv \pm y(p)$ fest. Wie im vorherigen Abschnitt für eine Spitze aus der Faser von ∞ konstruieren wir jetzt eine Bijektion zwischen den Doppelnebenklassen und einer uns besser bekannten Menge. Dazu verwenden wir die im vorherigen Abschnitt eingeführte Abbildung $\Theta_{j,c'}$:

$$\begin{array}{rccc} \Theta_{j,c'}: & \langle T^p\rangle \setminus \Gamma(p) g_j / \langle T^p\rangle & \longrightarrow & (\mathbb{Z}/c'p\mathbb{Z})^\star \\ & \left[\begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix}\right] & \longmapsto & \alpha \bmod c'p \end{array}$$

Diese Abbildung ist, wie im vorherigen Abschnitt gezeigt, wohldefiniert und injektiv, da diese Eigenschaften unabhängig von g_j sind. Wir können unsere vorherigen Überlegungen einfach übernehmen und suchen jetzt eine entsprechende Teilmenge, in die $\Theta_{j,c'}$ surjektiv abbildet:

$$U_{j,c'} := \{\alpha \in (\mathbb{Z}/c'p\mathbb{Z})^\star : \alpha \equiv t(p)\}$$

und:

$$\tilde{\Theta}_{j,c'}: \quad \langle T^p\rangle \setminus \Gamma(p) g_j / \langle T^p\rangle \quad \longrightarrow \quad U_{j,c'}.$$

4.10 Lemma: *Die Abbildung $\tilde{\Theta}_{j,c'}$ ist surjektiv.*

Beweis:
Sei $\alpha \in U_{j,c'}$. Wir zeigen, daß ein Repräsentant θ der Klasse:

$$\left[\begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix}\right] \in \langle T^p\rangle \setminus \Gamma(p) g_j / \langle T^p\rangle$$

existiert mit:

$$\theta = \begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix} = \begin{pmatrix} a & b \\ c' & d \end{pmatrix} \begin{pmatrix} x & z_1 \\ y & z_2 \end{pmatrix} \in \Gamma(p) g_j \Leftrightarrow \begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix} \Gamma(p) g_j^{-1} \in \Gamma(p).$$

Wir zeigen also, daß $\beta, \gamma \in \mathbb{Z}$ existieren mit:

$$\begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix} \begin{pmatrix} z_2 & -z_1 \\ -y & x \end{pmatrix} = \begin{pmatrix} \alpha z_2 - \beta y & -\alpha z_1 + \beta x \\ c' z_2 - \delta y & -c' z_1 + \delta x \end{pmatrix} \in \Gamma(p).$$

Da $y \equiv \bar{y}$ mit $\bar{y} \in \{1, \ldots, p-1\}$, existiert $\bar{y}^{-1} \in \{1, \ldots, p-1\}$ mit $y\bar{y}^{-1} \equiv \bar{y}\bar{y}^{-1} \equiv 1(p)$. Wir wählen $\beta \equiv -\bar{y}^{-1}(p)$ und $\delta \equiv 0(p)$ und zeigen, daß mit $\theta = \begin{pmatrix} \alpha & -\bar{y}^{-1} \\ c' & 0 \end{pmatrix}$ die Behauptung folgt. Dazu müssen folgende Äquivalenzen gelten:

1. $\alpha z_2 - \beta y \equiv \pm 1(p) \quad \Leftrightarrow \quad -\beta\bar{y} \equiv \pm 1(p)$
   da $z_2 \equiv 0(p), y \equiv \bar{y}(p) \beta \equiv -\bar{y}^{-1}(p)$
   $\Leftrightarrow \quad \beta \equiv \mp\bar{y}^{-1}(p)$
2. $-\alpha z_1 + \beta x \equiv 0(p) \quad \Leftrightarrow \quad \alpha\bar{y}^{-1} - \bar{y}^{-1} yt \equiv 0(p)$
   da $x \equiv yt(p), z_1 \equiv -\bar{y}^{-1}(p), \beta \equiv -\bar{y}^{-1}(p)$
   $\Leftrightarrow \quad \alpha \equiv yt(p)$ da $\bar{y}^{-1} \not\equiv 0(p)$
3. $c' z_2 - \delta y \equiv 0(p)$ erfüllt, da $p | z_2, p | \delta$
4. $-c' z_1 + \delta x \equiv \pm 1(p) \quad \Leftrightarrow \quad \pm y\bar{y}^{-1} \equiv \pm 1(p)$
   da $c' \equiv \pm y(p), y \equiv \bar{y}(p), z_1 \equiv -\bar{y}^{-1}, \delta \equiv 0(p)$

Mit den Voraussetzungen an α und der Wahl von β und δ sind alle Äquivalenzen erfüllt. □

Jetzt haben wir unsere gesuchte Anzahl $b_{1j}(c')$ wieder mit der Anzahl der Elemente in $U_{j,c'}$ identifiziert:

$$|U_{j,c'}| = |\{\alpha \in (\mathbb{Z}/c'p\mathbb{Z})^\star : \alpha \equiv t(p)\}| = \frac{1}{p} |\, (\mathbb{Z}/c'p\mathbb{Z})^\star \,| = \frac{1}{p} p\varphi(c') = \varphi(c'),$$

da die Kongruenz $\alpha \equiv t(p)$ wegen $t \in \{0, \ldots, p-1\}$ genau eine der p möglichen Kongruenzen in $(\mathbb{Z}/c'p\mathbb{Z})^\star$ ist. Wir haben insgesamt gezeigt:

4.11 Satz: *Sei $s_j = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ eine Spitze aus der Faser $\lambda^{-1}(\left[\begin{smallmatrix} t \\ 1 \end{smallmatrix}\right])$ mit $t \in \{0, \ldots, p-1\}$. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \varphi(c) & \text{für } c \equiv \pm y(p) \\ 0 & \text{für } c \not\equiv \pm y(p) \end{cases}$$

für $c \in \mathbb{N}$.

Innerhalb einer Faser gibt es für den unteren Eintrag y der Spitzen $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ modulo ± 1 genau:

$$\frac{\varphi(p)}{2} = \frac{p-1}{2}$$

Möglichkeiten, so daß die $\frac{p-1}{2}$ Bildungsgesetze einer Faser folgende Gestalt haben:

$$b_1(c) = \begin{cases} \varphi(c) & c \equiv \pm 1(p) \\ 0 & c \not\equiv \pm 1(p) \end{cases}, \ldots, b_{\frac{p-1}{2}}(c) = \begin{cases} \varphi(c) & c \equiv \pm\frac{p-1}{2}(p) \\ 0 & c \not\equiv \pm\frac{p-1}{2}(p) \end{cases}.$$

4.3 Anordnung der Bildungsgesetze in der Streumatrix

Für $\Gamma(p)$ haben wir in den vorherigen Abschnitten insgesamt $\frac{p-1}{2}+1$ verschiedene Bildungsgesetze $b_0, b_1, \ldots, b_{\frac{p-1}{2}}$ bestimmt, die wir jetzt mit ihrer Nummer aus $\mathbb{F}_p/\{\pm 1\}$ identifizieren. Damit reicht es, statt der Matrix B der Bildungsgesetze eine Matrix B' mit den Nummern der entsprechenden Bildungsgesetze anzugeben. Um die Struktur der Streumatrix untersuchen zu können, ordnen wir unsere bereits nach Fasern von λ sortierte Spitzenmenge:

$$\tilde{S}_p =: \{\underbrace{[s_1], \ldots, [s_{\frac{p-1}{2}}]}_{\in\lambda^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right])}, \underbrace{[s_{\frac{p-1}{2}+1}], \ldots, [s_{2\frac{p-1}{2}}]}_{\in\lambda^{-1}(\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right])}, \ldots, \underbrace{[s_{p\frac{p-1}{2}+1}], \ldots, [s_{(p+1)\frac{p-1}{2}}]}_{\in\lambda^{-1}(\left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right])}\}$$

mit dem Vektor von Repräsentanten:

$$\tilde{S} =: [\underbrace{s_1, \ldots, s_{\frac{p-1}{2}}}_{\in\lambda^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right])}, \underbrace{s_{\frac{p-1}{2}+1}, \ldots, s_{2\frac{p-1}{2}}}_{\in\lambda^{-1}(\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right])}, \ldots, \underbrace{s_{p\frac{p-1}{2}+1}, \ldots, s_{(p+1)\frac{p-1}{2}}}_{\in\lambda^{-1}(\left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right])}]$$

so an, daß die zugehörigen Nummern der Bildungsgesetze in der ersten Zeile der Streumatrix aufsteigen. In der ersten Zeile hat die Matrix der Bildungsgesetze dann die Gestalt:

$$B' = \begin{pmatrix} \overbrace{0\ 0\ \ldots\ 0}^{s_i\in\lambda^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right])} & \overbrace{1\ 2\ \ldots\ \frac{p-1}{2}}^{s_i\in\lambda^{-1}(\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right])} & \overbrace{1\ 2\ \ldots\ \frac{p-1}{2}}^{s_i\in\lambda^{-1}(\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right])} & \ldots & \overbrace{1\ 2\ \ldots\ \frac{p-1}{2}}^{s_i\in\lambda^{-1}(\left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right])} \\ & & & & \end{pmatrix}$$

Nachdem wir bereits die Anzahlen der Doppelnebenklassen für die Einträge der ersten Zeile der Streumatrix bestimmt haben, beschäftigen wir uns in diesem Abschnitt mit den anderen Zeilen der Streumatrix. In Satz 4.1 haben wir gesehen, daß alle anderen Zeilen der Streumatrix Permutationen der ersten Zeile sind, so daß es keine noch nicht bestimmten Bildungsgesetze gibt. Uns interessieren diese Permutationen. Wir wollen also wissen, welches Bildungsgesetz zu beliebigen Spitzen $s_i, s_j \in S_p = \Gamma(p) \setminus \mathbb{P}^1(\mathbb{Q})$ gehört und dafür folgende Abbildung konstruieren:

$$F: \quad S_p \times S_p \quad \longrightarrow \quad \mathbb{F}_p/\{\pm 1\}.$$

Um uns dieser Abbildung zu nähern, benötigen wir einige Vorüberlegungen. In Abschnitt 4.1 haben wir bereits spezielle Untergruppen von $\Gamma_p := \mathrm{PSL}(2, \mathbb{F}_p)$

eingeführt, nämlich die *Borel-Gruppe*:

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{F}_p) \right\}$$

und die normale Untergruppe:

$$B_1 := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{F}_p) \right\} \lhd B,$$

deren Quotienten B/B_1 wir mit $\mathbb{F}_p^\star/\{\pm 1\}$ identifiziert haben. Für diesen Quotienten definieren wir auf:

$$\Sigma_p := \mathrm{PSL}(2, \mathbb{F}_p)/B_1$$

eine Operation:

$$\begin{array}{rccc} \star: & B/B_1 \times \Sigma_p & \longrightarrow & \Sigma_p \\ & ([b], [\sigma]) & \longmapsto & [b] \star [\sigma] := [\sigma b^{-1}] \end{array}$$

Diese Operation ist wohldfiniert: Seien b_1, b_2 Repräsentanten von $[b]$ in B/B_1, d.h. es existiert ein $\beta = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in B_1$ mit $b_1 = b_2\beta$, also $b_2^{-1} = \beta b_1^{-1}$, und seien σ_1, σ_2 Repräsentanten von $[\sigma] \in \Sigma_p$, d.h. es existiert ein $\tilde{\beta} = \left(\begin{smallmatrix} 1 & \tilde{b} \\ 0 & 1 \end{smallmatrix}\right) \in B_1$ mit $\sigma_1 = \sigma_2\tilde{\beta}$. Dann folgt $\sigma_2 = \sigma_1\tilde{\beta}^{-1}$ und wir erhalten:

$$[b] \star [\sigma] = \sigma b_1^{-1} = \sigma\tilde{\beta}^{-1}\tilde{\beta}b_1^{-1} = \sigma_2 b_2^{-1}.$$

Mit $\star$ haben wir eine Gruppenoperation von B/B_1 auf Σ_p eingeführt:

1. $([b][c]) \star [\sigma] = \sigma(bc)^{-1} = \sigma c^{-1}b^{-1} = [b] \star ([\sigma c^{-1}]) = [b] \star ([c][\sigma])$
   für b, c Repräsentanten von $[b], [c] \in B/B_1$ und σ Repräsentant von $[\sigma] \in \Sigma_p$.

2. $[1] \star [\sigma] = \sigma b^{-1} = \sigma = [\sigma]$
   für $b = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ Repräsentant von $[1] \in \Sigma_p$ und σ Repräsentant von $[\sigma] \in \Sigma_p$.

4.12 Satz: *Jede Bahn von B/B_1 auf Σ_p hat genau $\frac{p-1}{2}$ Elemente.*

Beweis:
Für ein $[\sigma] \in \Sigma_p$ ist die Bahn definiert als:

$$B_{B/B_1}([\sigma]) := \{[b] \star [\sigma] : [b] \in B/B_1\}.$$

$B/B_1 \cong \mathbb{F}_p^\star/\{\pm 1\}$ hat genau $\frac{p-1}{2}$ Elemente und wenn wir zeigen, daß es kein $[\sigma] \in \Sigma_p$ gibt mit $[b_1]\star[\sigma] = [b_2]\star[\sigma]$ für zwei verschiedene Restklassen $[b_1] \neq [b_2]$ aus Σ_p, folgt die Behauptung.

Als Widerspruchsannahme seien b_1, b_2 Repräsentanten von $[b_1] \neq [b_2]$, σ Repräsentant einer beliebigen Klasse $[\sigma] \in \Sigma_p$ und es gelte $\sigma b_1^{-1} = \sigma b_2^{-1}$. Es folgt $\sigma = \sigma b_2^{-1} b_1$ und damit $b_2^{-1} b_1 \in [1]$, also $[b_1] = [b_2]$. □

4.13 Satz: *B/B_1 operiert transitiv auf jeder Faser von:*

$$\begin{array}{rccc} s: & \Sigma_p & \longrightarrow & \mathrm{PSL}(2,\mathbb{F}_p)/B \\ & [\sigma] = \sigma B_1 & \longmapsto & [\sigma]_B := \sigma B. \end{array}$$

Beweis:
s ist wohldefiniert, da für Repräsentanten σ_1, σ_2 von $[\sigma]$ ein $\beta \in B_1$ existiert mit $\sigma_1 = \sigma_2 \beta$ und es folgt:

$$s([\sigma]) = \sigma_1 B = \sigma_2 \beta B = \sigma_2 B.$$

Um zu sehen, daß B/B_1 transistiv auf $s^{-1}([\sigma]_B)$ operiert, zeigen wir, daß zu $\sigma_1, \sigma_2 \in s^{-1}([\sigma]_B)$ ein $[b] \in B/B_1$ existiert mit $[b] \star [\sigma_1] = [\sigma_2]$. Wegen $\sigma_1, \sigma_2 \in s^{-1}([\sigma]_B)$ gilt $\sigma_1 \beta = \sigma_2$ für ein $\beta = \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ 0 & \tilde{d} \end{smallmatrix}\right) \in \Gamma_p$. Mit $b := \beta^{-1}$ existiert also ein Repräsentant einer Klasse $[b] \in B/B_1$ mit:

$$[b] \star [\sigma_1] = \sigma_1 b^{-1} = \sigma_1 \beta = \sigma_2 = [\sigma_2].$$

□

Jetzt können wir eine Abbildung definieren, die jeder Spitzenklasse ein Element aus Σ_p zuordnet:

$$\begin{array}{rccc} h: & S_p\Gamma(p)\backslash\mathbb{P}^1(\mathbb{Q}) = & \longrightarrow & \Sigma_p/B_1 \\ & \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] & \longmapsto & \tilde{g}_{x,y}. \end{array}$$

Dabei wählen wir zu $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ eine Matrix $g_{x,y} \in \Gamma$ mit $g_{x,y}\infty = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$, die nach Satz 1.10 eindeutig bis auf Multiplikation mit T^n von rechts ist. Anschliessend reduzieren wir diese Matrix modulo p zu $\tilde{g}_{x,y}$. Dabei ist die Restklasse in Σ_p/B_1 unabhängig von der Wahl der Matrix $g_{x,y} \in \Gamma$, da diese eindeutig bis auf Multiplikation mit T^n von rechts bestimmt ist.
Diese Abbildung ist wohldefiniert: Zu zwei Repräsentanten $s_1 = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, s_2 = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ derselben Spitzenklasse existiert ein $\gamma \in \Gamma(p)$ mit $\gamma s_1 = s_2$. Wenn wir eine Matrix $g_{x_1,y_1} \in \Gamma$ mit $g_{x_1,y_1}\infty = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$ wählen, folgt $\gamma g_{x_1,y_1}\infty = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ und $\gamma g_{x_1,y_1}\infty = g_{x_2,y_2} T^n$ für ein geeignetes $n \in \mathbb{N}$, da die Matrix g_{x_2,y_2} eindeutig bis auf Multiplikation mit T^n ist. Bei der Reduktion modulo p erhalten wir dieselbe Klasse in Σ_p/B_1, da $\gamma \equiv [\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)] \bmod p$ und $T^n \bmod p \in B_1$.

Jetzt betrachten wir das direkte Produkt $\Sigma_p \times \Sigma_p$, auf das sich die eben eingeführten Operationen erweitern lassen:
Γ_p operiert auf $\Sigma_p \times \Sigma_p$ durch:

$$\gamma([s],[t]) := (\gamma s, \gamma t)$$

für $\gamma \in \Gamma_p$ und s,t Repräsentanten der Nebenklassen $[s],[t] \in \Sigma_p = \mathrm{PSL}(2,\mathbb{F}_p)/B_1$.
$B/B_1 \times B/B_1$ operiert auf $\Sigma_p \times \Sigma_p$ durch:

$$([b_1],[b_2]) \star ([s],[t]) := ([b_1]\star[s],[b_2]\star[t]) = (sb_1^{-1}, tb_2^{-1})$$

für $[b_1],[b_2] \in B/B_1$.
Jetzt können wir die erste unserer gewünschten Abbildungen definieren:

$$\begin{array}{rccc} f: & \Sigma_p \times \Sigma_p & \longrightarrow & \mathbb{F}_p/\{\pm 1\} \\ & ([\sigma],[\tau]) & \longmapsto & \sigma_1\tau_3 - \sigma_3\tau_1 \bmod p \end{array}$$

für $\sigma = \left(\begin{smallmatrix}\sigma_1 & \sigma_2 \\ \sigma_3 & \sigma_4\end{smallmatrix}\right), \tau = \left(\begin{smallmatrix}\tau_1 & \tau_2 \\ \tau_3 & \tau_4\end{smallmatrix}\right) \in \Sigma_p$.
Diese Abbildung ist wohldefiniert: Seien $\sigma, \tilde{\sigma}$ Repräsentanten von $[\sigma] \in \Sigma_p$ und $\tau, \tilde{\tau}$ von $[\tau] \in \Sigma_p$. Dann existieren $\beta_1, \beta_2 \in B_1$ mit $\sigma = \tilde{\sigma}\beta_1$ und $\tau = \tau\beta_2$, die ersten Spalten der Matrizen bleiben also unverändert.
Wir erkennen folgende Eigenschaften von f für $[\sigma],[\tau] \in \Sigma_p$ und $b_1 = \left(\begin{smallmatrix}\alpha_1 & \beta_1 \\ 0 & \delta_1\end{smallmatrix}\right), b_2 = \left(\begin{smallmatrix}\alpha_2 & \beta_2 \\ 0 & \delta_2\end{smallmatrix}\right) \in B/B_1$:

1. $f([\sigma],[\sigma]) = \sigma_1\sigma_3 - \sigma_3\sigma_1 \bmod p = 0$
2. $f(b_1 \star [\sigma],[\sigma]) = f([\sigma b_1^{-1}],[\sigma]) = \sigma_1\sigma_3 d - \sigma_3 d\sigma_1 \bmod p = 0$
   wegen $\sigma b_1^{-1} = \left(\begin{smallmatrix}\sigma_1\delta_1 & -\sigma_1\beta_1+\sigma_2\alpha_1 \\ \sigma_3\delta_1 & -\sigma_3\beta_1+\sigma_4\alpha_1\end{smallmatrix}\right)$
3. $f([\sigma],[\tau]) = \sigma_1\tau_3 - \sigma_3\tau_1 \bmod p = -\sigma_1\tau_3 + \sigma_3\tau_1 \bmod p = \tau_1\sigma_3 - \tau_3\sigma_1 \bmod p$
   $= f([\tau],[\sigma])$
4. $f(b_1 \star [\sigma], b_1 \star [\tau]) = f\left(\begin{pmatrix}\delta_1\sigma_1 & \sigma_2\alpha_1 - \sigma_1\beta_1 \\ \sigma_3\delta_1 & \sigma_4\alpha_1 - \sigma_3\beta_1\end{pmatrix}, \begin{pmatrix}\delta_1\tau_1 & \tau_2\alpha_1 - \tau_1\beta_1 \\ \tau_3\delta_1 & \tau_4\alpha_1 - \tau_3\beta_1\end{pmatrix}\right)$
   $= \delta_1\delta_2(\sigma_1\tau_3 - \sigma_3\tau_1) = \delta_1\delta_2 f([\sigma],[\tau])$

Jetzt bilden wir die Hintereinanderausführung der beiden bisher untersuchten Abbildungen, um den Repräsentanten zweier Spitzenklassen s_i, s_j die Nummer des zugehörigen Bildunsgesetzes b_{ij} in $\mathbb{F}_p/\{\pm 1\}$ zuzuordnen:

$$\begin{array}{rccccc} F: & \overline{S_p} \times \overline{S_p} & \overset{(h,h)}{\longrightarrow} & \Sigma_p \times \Sigma_p & \overset{f}{\longrightarrow} & \mathbb{F}_p/\{\pm 1\} \\ & (\overline{\begin{bmatrix}x\\y\end{bmatrix}}, \overline{\begin{bmatrix}u\\v\end{bmatrix}}) & & \longmapsto & & xv - uy \bmod p. \end{array}$$

Als Komposition wohldefinierter Abbildungen ist F offensichtlich wohldefiniert und wir erkennen folgende Eigenschaften von F für $s = \overline{\begin{bmatrix} x \\ y \end{bmatrix}}, t = \overline{\begin{bmatrix} u \\ v \end{bmatrix}} \in S_p$ und $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}(2, \mathbb{F}_p)$:

1. $F(s,t) = F(t,s)$,

   da mit $f(s,t) = f(t,s)$ gilt: $F(s,t) = uy - xv \equiv xv - uy$ in $\mathbb{F}_p/\{\pm 1\}$.

2. $F(\sigma(s,t)) = F(s,t)$,

   $$\text{da } F(\sigma(s,t)) = F\left(\overline{\begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}}, \overline{\begin{bmatrix} au+bv \\ cu+dv \end{bmatrix}}\right) = (ad-bc)(xv-uy) = xv-uy$$

3. $F((\sigma s,t)) = F(s, \sigma^{-1}t)$,

   $$\text{da } F((\sigma s,t)) = F\left(\overline{\begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}}, \overline{\begin{bmatrix} u \\ v \end{bmatrix}}\right) = axu + byv - cxu - dyu$$

   $$= x(-cu+av) - y(du-bv) = F\left(\overline{\begin{bmatrix} x \\ y \end{bmatrix}}, \overline{\begin{bmatrix} du-bv \\ -cu+av \end{bmatrix}}\right) = F(s, \sigma^{-1}t)$$

Die Streumatrix wird jetzt durch F vollständig beschrieben, da sich ihre Einträge aus den entsprechenden Reihen der Bildungsgesetze ergeben. Wegen der ersten Eigenschaft von F sehen wir nochmals, daß die Streumatrix symmetrisch ist, und wegen der ersten Eigenschaft von f, nämlich $f([\sigma],[\sigma]) = 0$, enthält die Hauptdiagonale der Streumatrix nur das Bildungsgesetz b_0, wie wir in Lemma 4.2 bereits gezeigt haben. Darüberhinaus bestehen alle Blöcke von Bildungsgesetzen auf der Hauptdiagonalen nur aus b_0, da wegen Eigenschaft 2 von f für $[\sigma] \in \Sigma_p$ und $b_1 \in B/B_1$ gilt:

$$f(b_1 \star [\sigma],[\sigma]))f([\sigma], b_1 \star [\sigma]) = 0.$$

Aus Eigenschaft 4 von F erhalten wir, daß innerhalb eines Blockes auf der Gegendiagonale immer dasselbe Bildungsgesetz steht.

Damit ergibt sich für die Streumatrix folgende Struktur:

$$\left(\begin{array}{c|cccc|cccc|c|cccc}
 & s_i \in \lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}]) & & & & s_i \in \lambda^{-1}([\begin{smallmatrix}1\\1\end{smallmatrix}]) & & & & \dots & s_i \in \lambda^{-1}([\begin{smallmatrix}p\\1\end{smallmatrix}]) & & & \\
\hline
 & 0 & 0 & \dots & 0 & 1 & 2 & \dots & \frac{p-1}{2} & & 1 & 2 & \dots & \frac{p-1}{2} \\
s_i & 0 & 0 & \dots & 0 & 2 & 3 & \dots & 1 & & 2 & 3 & \dots & 1 \\
\in & \vdots & & & \vdots & \vdots & & & \vdots & \dots & \vdots & & & \vdots \\
\lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}]) & 0 & 0 & \dots & 0 & \frac{p-1}{2} & 1 & \dots & \frac{p-1}{2}-1 & & \frac{p-1}{2} & 1 & \dots & \frac{p-1}{2}-1 \\
 & 1 & 2 & \dots & \frac{p-1}{2} & 0 & 0 & \dots & 0 & & 1 & 2 & \dots & \frac{p-1}{2} \\
s_i & 2 & 3 & \dots & 1 & 0 & 0 & \dots & 0 & & 2 & 3 & \dots & 1 \\
\in & \vdots & & & \vdots & \vdots & & & \vdots & \dots & \vdots & & & \vdots \\
\lambda^{-1}([\begin{smallmatrix}1\\1\end{smallmatrix}]) & \frac{p-1}{2} & 1 & \dots & \frac{p-1}{2}-1 & 0 & 0 & \dots & 0 & & \frac{p-1}{2} & 1 & \dots & \frac{p-1}{2}-1 \\
 & & & & & & & & & & & & & \\
\vdots & & \vdots & & & & \vdots & & & \vdots & & \vdots & & \\
 & & & & & & & & & & & & & \\
s_i & & & & & & & & & & & & & \\
\in & & & & & & & & & & & & & \\
\lambda^{-1}([\begin{smallmatrix}p\\1\end{smallmatrix}]) & & & & & & & & & & & & &
\end{array}\right)$$

Um zu zeigen, wie sich die Streumatrix mit diesem Konzept darstellen läßt, betrachten wir $\Gamma(7)$ als kleinstes sinnvolles Beispiel. Bei $\Gamma(3)$ enthält jede Faser nur ein Element, so daß wir nur die Bildungsgesetze b_0, b_1 haben, und bei $\Gamma(5)$ hat jede Faser zwei Elemente, so daß die Art der Permutationen nicht zu erkennen ist.

4.14 Beispiel:
$\Gamma(7)$ hat 24 Spitzen und die Abbildung λ hat 8 Fasern mit jeweils 3 Elementen. Ein nach Fasern sortiertes Repräsentantensystem der Spitzen ist der folgende Spitzenvektor, wobei die Spitzen innerhalb einer Faser so angeordnet sind, daß die Nummern der Bildungsggesetze in der ersten Zeile der Streumatrix in jeder Faser aufsteigen.

$$S(\Gamma(7)) = \left\{ \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}2\\7\end{bmatrix}, \begin{bmatrix}4\\7\end{bmatrix}, \quad \begin{bmatrix}0\\-1\end{bmatrix}, \begin{bmatrix}-7\\2\end{bmatrix}, \begin{bmatrix}7\\-4\end{bmatrix}, \quad \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}5\\-2\end{bmatrix}, \begin{bmatrix}3\\-4\end{bmatrix}, \right.$$
$$\begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}3\\-2\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \quad \begin{bmatrix}1\\-2\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}, \begin{bmatrix}3\\1\end{bmatrix}, \quad \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\-1\end{bmatrix}, \begin{bmatrix}2\\-3\end{bmatrix}, $$
$$\left. \begin{bmatrix}2\\-1\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}3\\2\end{bmatrix}, \quad \begin{bmatrix}1\\-1\end{bmatrix}, \begin{bmatrix}2\\5\end{bmatrix}, \begin{bmatrix}4\\3\end{bmatrix} \right\}$$

Zur Veranschaulichung werten wir jetzt unsere Abbildung F an einigen Spitzen aus, wobei wir in $\mathbb{F}_p/\{\pm 1\}$ rechnen:

1. $F([\begin{smallmatrix}2\\3\end{smallmatrix}], [\begin{smallmatrix}2\\3\end{smallmatrix}]) = 2 \cdot 3 - 3 \cdot 2 = 0$
2. $F([\begin{smallmatrix}2\\1\end{smallmatrix}], [\begin{smallmatrix}3\\2\end{smallmatrix}]) = 2 \cdot 2 - 3 \cdot 1 = 1$

3. $F(\left[\begin{smallmatrix}2\\3\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\2\end{smallmatrix}\right]) = 2 \cdot 2 - 3 \cdot 3 = -5 \equiv 2(7)$
4. $F(\left[\begin{smallmatrix}4\\7\end{smallmatrix}\right], \left[\begin{smallmatrix}2\\5\end{smallmatrix}\right]) = 4 \cdot 5 - 2 \cdot 7 = 6 \equiv 1 \text{ in } \mathbb{F}_p/\{\pm 1\}$
5. $F(\left[\begin{smallmatrix}1\\4\end{smallmatrix}\right], \left[\begin{smallmatrix}2\\5\end{smallmatrix}\right]) = 1 \cdot 5 - 2 \cdot 4 = -3 \equiv 4(7) \equiv 3 \text{ in } \mathbb{F}_p/\{\pm 1\}$

In Kapitel 6 werden wir die Determinante der Streumatrix für die Hauptkongruenzgruppen $\Gamma(p)$ bestimmen und unser Vorgehen unter anderem an dieser Matrix verdeutlichen. Wir werden dabei die Matrix der Bildungsgesetze so codieren, daß sich ihre Dimension reduziert. Die reduzierte Matrix werden wir so weit wie möglich diagonalisieren. Bei den entsprechenden Rücksubstituitionen bleibt die beinahe vollständige Diagonalisierung erhalten. Ausgehend von den Bildungsgesetzen entwickeln wir für die Diagonaleinträge die zugehörigen Eisensteinreihen und stellen sie in geschlossener Form dar. Mit weiteren Untersuchungen werden wir dann die Determinante des nicht diagonalisierten Teils bestimmen und erhalten die Determinante der Streumatrix von $\Gamma(p)$ durch Multiplikation der Teilergebnisse.
Insgesamt ergibt sich folgende Matrix der Bildungsgesetze von $\Gamma(7)$:

$$B = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc|ccc}
0&0&0&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3\\
0&0&0&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1\\
0&0&0&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2&3&1&2\\
\hline
1&2&3&0&0&0&1&2&3&2&3&1&3&1&2&3&1&2&2&3&1&1&2&3\\
2&3&1&0&0&0&2&3&1&3&1&2&1&2&3&1&2&3&3&1&2&2&3&1\\
3&1&2&0&0&0&3&1&2&1&2&3&2&3&1&2&3&1&1&2&3&3&1&2\\
\hline
1&2&3&1&2&3&0&0&0&1&2&3&2&3&1&3&1&2&3&1&2&2&3&1\\
2&3&1&2&3&1&0&0&0&2&3&1&3&1&2&1&2&3&1&2&3&3&1&2\\
3&1&2&3&1&2&0&0&0&3&1&2&1&2&3&2&3&1&2&3&1&1&2&3\\
\hline
1&2&3&2&3&1&1&2&3&0&0&0&1&2&3&2&3&1&3&1&2&3&1&2\\
2&3&1&3&1&2&2&3&1&0&0&0&2&3&1&3&1&2&1&2&3&1&2&3\\
3&1&2&1&2&3&3&1&2&0&0&0&3&1&2&1&2&3&2&3&1&2&3&1\\
\hline
1&2&3&3&1&2&2&3&1&1&2&3&0&0&0&1&2&3&2&3&1&3&1&2\\
2&3&1&1&2&3&3&1&2&2&3&1&0&0&0&2&3&1&3&1&2&1&2&3\\
3&1&2&2&3&1&1&2&3&3&1&2&0&0&0&3&1&2&1&2&3&2&3&1\\
\hline
1&2&3&3&1&2&3&1&2&2&3&1&1&2&3&0&0&0&1&2&3&2&3&1\\
2&3&1&1&2&3&1&2&3&3&1&2&2&3&1&0&0&0&2&3&1&3&1&2\\
3&1&2&2&3&1&2&3&1&1&2&3&3&1&2&0&0&0&3&1&2&1&2&3\\
\hline
1&2&3&2&3&1&3&1&2&3&1&2&2&3&1&1&2&3&0&0&0&1&2&3\\
2&3&1&3&1&2&1&2&3&1&2&3&3&1&2&2&3&1&0&0&0&2&3&1\\
3&1&2&1&2&3&2&3&1&2&3&1&1&2&3&3&1&2&0&0&0&3&1&2\\
\hline
1&2&3&1&2&3&2&3&1&3&1&2&3&1&2&2&3&1&1&2&3&0&0&0\\
2&3&1&2&3&1&3&1&2&1&2&3&1&2&3&3&1&2&2&3&1&0&0&0\\
3&1&2&3&1&2&1&2&3&2&3&1&2&3&1&1&2&3&3&1&2&0&0&0
\end{array}\right)$$

5 Die Streumatrix für Hauptkongruenzuntergruppen $\Gamma(n)$

Die in dem vorherigen Kapitel gewonnenen Erkenntisse für $\Gamma(p)$ wollen wir jetzt so weit wie möglich für Hauptkongruenzuntergruppen $\Gamma(n)$ verallgemeinern mit der Primfaktorzerlegung $n = p_1^{l_1} \cdot \ldots \cdot p_m^{l_m}$ mit Primzahlen $p_1, \ldots, p_m$ und $l_1, \ldots, l_m \in \mathbb{N}$. Da $\mathbb{Z}/n\mathbb{Z}$ nur dann ein Körper ist, wenn n eine Primzahl ist, definieren wir als erstes $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$. Dazu betrachten wir die Menge aller Paare von Elementen aus $\mathbb{Z}/n\mathbb{Z}$ mit der Eigenschaft, daß das von ihnen erzeugte Ideal der ganze Ring ist:

$$P := \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : \langle x, y \rangle = \mathbb{Z}/n\mathbb{Z} \right\}$$

mit $\langle x, y \rangle = \{ax+by : a, b \in \mathbb{Z}/n\mathbb{Z}\}$. Auf P läßt sich folgende Äquivalenzrelation definieren:

$$\begin{bmatrix} x \\ y \end{bmatrix} \sim \begin{bmatrix} u \\ v \end{bmatrix} :\Leftrightarrow \exists \lambda \in (\mathbb{Z}/n\mathbb{Z})^\star \text{ mit } x = \lambda u \wedge y = \lambda v.$$

Diese Relation ist:

1. reflexiv, da $\lambda = 1 \in (\mathbb{Z}/n\mathbb{Z})^\star$,
2. symmetrisch, da λ invertierbar und
3. transitiv, da $(\mathbb{Z}/n\mathbb{Z})^\star$ eine multiplikative Gruppe ist,

so daß wir wirklich eine Äquivalenzrelation definiert haben. Modulo dieser Äquivalenzrelation können wir jetzt $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ erklären als:

5.1 Definition: $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z}) := P \,/\sim = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in \mathbb{Z} \text{ mit } \langle x, y \rangle = \mathbb{Z}/n\mathbb{Z} \right\} / \sim$

Wir wählen also solche Paare $x, y \in \mathbb{Z}/n\mathbb{Z}$, für die das von ihnen erzeuge Ideal der ganze Ring $\mathbb{Z}/n\mathbb{Z}$ ist, und identifizieren diejenigen Erzeugerpaare miteinander, die sich durch Einheiten ineinander überführen lassen. Für $n = p$ entspricht dies unserer bisherigen Definition: Wir haben für $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ Repräsentanten der

Form $\{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\1\end{smallmatrix}\right], \ldots, \left[\begin{smallmatrix}p-1\\1\end{smallmatrix}\right]\}$ gewählt, die alle offensichlich ganz $\mathbb{Z}/p\mathbb{Z}$ erzeugen, da die Eins in dem von ihnen erzeugten Ideal liegt. Wegen ihrer Struktur liegen alle Repräsentanten in verschiedenen Nebenklassen bezüglich der von uns eingeführten Äquivalenzrelation und alle anderen Repräsentanten $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]$ sind zu den bisherigen äquivalent.
Um das im vorherigen Kapitel entwickelte Konzept zur Bestimmung der Bildungsgsetze auf $\Gamma(n)$ übertragen zu können, betrachten wir zunächst nur eine Primzahlpotenz, untersuchen also die Gruppen $\Gamma(p^k)$ für eine Primzahl p.

5.1 Die Gruppen $\Gamma(p^k)$

Es sei $p^k \neq 2$, denn diesen Fall haben wir bereits im vorherigen Kapitel betrachtet. Dann gilt:

$$\mu := [\Gamma : \Gamma(p^k)] = p^{3k-2}\frac{p^2-1}{2}$$

und $\Gamma(p^k)$ hat:

$$r := \frac{\mu}{p^k} = p^{2k-2}\frac{p^2-1}{2}$$

Nebenklassen in $S_{p^k} := \Gamma(p^k) \setminus \mathbb{P}^1(\mathbb{Q})$. Wir definieren $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ wie oben eingeführt und suchen nun ein vollständiges Repräsentantensystem für die Äquivalenzklassen von $\mathbb{P}^1(\mathbb{Z}/p^kZ)$. Dazu sei:

$$R := \left\{ \begin{bmatrix}1\\t\end{bmatrix}, \begin{bmatrix}t\\1\end{bmatrix} : t \in \mathbb{Z}/p^k\mathbb{Z}, t \equiv 0(p) \right\} \bigcup \left\{ \begin{bmatrix}y\\1\end{bmatrix} : y \in (\mathbb{Z}/p^k\mathbb{Z})^\star \right\}.$$

Offensichtlich erzeugen alle Paare $< x, y >$ aus R ganz $\mathbb{Z}/p^k\mathbb{Z}$ und sind bezüglich der Äquivalenzrelation $\sim$ nicht zueinander äquivalent, da sie sich nicht durch ein $\lambda \in (\mathbb{Z}/p^k\mathbb{Z})^\star$ ineinander überführen lassen. Es bleibt noch zu zeigen, daß alle anderen Elemente $\begin{bmatrix}x\\y\end{bmatrix} \in \mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ zu einem Repräsentanten aus R äquivalent sind.

1. $y \equiv 0(p)$: Dann läßt sich $x \not\equiv 0(p)$ invertieren: $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] = \left[\begin{smallmatrix}1\\yx^{-1}\end{smallmatrix}\right]$ mit $yx^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$ und $y \equiv 0(p)$, also ist $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]$ zu einem Element aus R äquivalent.

2. $x \equiv 0(p)$: Analog läßt sich x in $\mathbb{Z}/n\mathbb{Z}$ invertieren und $\left[\begin{smallmatrix}yx^{-1}\\1\end{smallmatrix}\right]$ liegt in R.

3. $x, y \not\equiv 0(p)$: Dann ist y in in $\mathbb{Z}/n\mathbb{Z}$ invertierbar und $\left[\begin{smallmatrix}yx^{-1}\\1\end{smallmatrix}\right]$ liegt in R.

Wir können also $\mathbb{P}^1(\mathbb{Z}/p^kZ)$ durch R repräsentieren, wobei für die Anzahl an Elementen in R gilt:

$$|R| = 2(p^k - \varphi(p^k)) + \varphi(p^k)) = 2p^k - p^{k-1}(p-1) = p^{k-1}(p+1).$$

Damit haben wir den folgenden Satz gezeigt:

5.2 Satz: *$\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ hat genau $p^{k-1}(p+1)$ Elemente.*

5.3 Beispiel: Für $\mathbb{P}^1(\mathbb{Z}/8\mathbb{Z})$ können wir folgende Repräsentanten wählen:

$$\mathbb{P}^1(\mathbb{Z}/8\mathbb{Z}) = \left\{ \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}1\\6\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}3\\1\end{bmatrix}, \begin{bmatrix}5\\1\end{bmatrix}, \begin{bmatrix}7\\1\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}4\\1\end{bmatrix}, \begin{bmatrix}6\\1\end{bmatrix} \right\}$$

Analog zu unserem Vorgehen in Kapitel 3 führen wir jetzt eine Abbildung der Spitzenklassen von $\Gamma(p^k)$ nach $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z})$ ein:

$$\begin{array}{rccc} \lambda: & \Gamma(p^k)\setminus\mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z}) \\ & \overline{\begin{bmatrix}x\\y\end{bmatrix}} & \longmapsto & \begin{bmatrix}x\\y\end{bmatrix}_{p^k}. \end{array}$$

Wir sehen wie in Abschnitt 4.1, daß diese Abbildung wohldefiniert und surjektiv ist.

5.4 Satz: *Jede Faser von λ hat genau $p^{k-1}\frac{p-1}{2}$ Elemente.*

Beweis:
Hier verallgemeinern wir unsere Überlegungen für $\Gamma(p)$, indem wir zunächst die *verallgemeinerte Borel-Gruppe* definieren als:

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{PSL}(2, (\mathbb{Z}/p^k\mathbb{Z})) \right\}$$

mit der normalen Untergruppe:

$$B_1 := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}(2, (\mathbb{Z}/p^k\mathbb{Z})) \right\} \lhd B,$$

deren Quotienten B/B_1 wir mit der zyklischen Gruppe der Ordnung $p^{k-1}\frac{p-1}{2}$ identifizieren:

$$\begin{array}{rccc} \eta: & B/B_1 & \longrightarrow & (\mathbb{Z}/p^k\mathbb{Z})^\star/\{\pm 1\} \\ & \left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right] & \longmapsto & a \end{array}$$

mit $|(\mathbb{Z}/p^k\mathbb{Z})^\star| = \varphi(p^k) = p^{k-1}(p-1)$ und $|(\mathbb{Z}/p^k\mathbb{Z})^\star/\{\pm 1\}| = p^{k-1}\frac{p-1}{2}$. Die Überlegungen, daß η wohldefiniert und bijektiv ist, lassen sich analog aus Abschnitt 4.1 und dem dort bewiesenen Lemma 4.3 übernehmen. Jetzt identifizieren wir jede Faser von λ mit dieser Gruppe und zeigen dadurch, daß jede Faser genau $p^{k-1}\frac{p-1}{2}$ Restklassen enthält: Dafür betrachten wir zunächst die Faser von ∞:

$$\lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}]) = \{[\begin{smallmatrix}x\\y\end{smallmatrix}] \in \mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z}) : y \equiv 0(p)\}$$

und bilden sie in den Quotienten B/B_1 ab:

$$\begin{array}{rccc} \psi: & \lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}]) \subset S_{p^k} & \longrightarrow & B/B_1 \\ & \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] & \longmapsto & \left[\begin{pmatrix}x & b\\0 & d\end{pmatrix}\right], \end{array}$$

indem $[\begin{smallmatrix}x\\y\end{smallmatrix}]$ nach Korollar 1.3 zu einer Matrix $\beta = \left(\begin{smallmatrix}x & b\\y & d\end{smallmatrix}\right) \in \Gamma$ mit $\beta[\begin{smallmatrix}1\\0\end{smallmatrix}] = [\begin{smallmatrix}x\\y\end{smallmatrix}]$ und $p^k|y$ ergänzt wird, wobei diese Ergänzung nach Satz 1.10 eindeutig bis auf Multiplikation mit T^n von rechts ist. Dann ergibt die Reduktion der Einträge modulo p^k von β eine Matrix $\rho(\beta) \in B$, die bis auf Multiplikation mit Elementen aus B_1 eindeutig bestimmt ist. Diese Zuordnung ist, wie schon die in Abschnitt 4.1 definierte, wohldefiniert, da sich die Bilder von Elementen der gleichen Nebenklasse von $\Gamma(p^k)$ durch Matrizen aus B_1 ineinander überführen lassen. Analog zu Lemma 4.4, in dem wir die gleiche Behauptung für $\Gamma(p)$ gezeigt haben, sehen wir, daß ψ eine Bijektion ist. Die Hintereinanderausführung der beiden Abbildung liefert eine Bijektion:

$$f: \quad \lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}]) \quad \longrightarrow \quad (\mathbb{Z}/p^k\mathbb{Z})^\star/\{\pm 1\},$$

so daß $\lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}])$ genau $p^{k-1}\frac{p-1}{2}$ Elemente hat. Da Γ transitiv auf $\mathbb{P}^1(\mathbb{Q})$ operiert, übertragen wir dieses Resultat wie in Abschnitt 4.1 auf die anderen Fasern und haben insgesamt gezeigt, daß in jeder Faser von λ genau $p^{k-1}\frac{p-1}{2}$ Bahnen von $\Gamma(p)$ liegen. □

Jetzt können wir die $p^{k-1}(p+1)p^{k-1}\frac{p-1}{2}$ Spitzenklassen von $\Gamma(p^k)$ nach den Fasern sortieren und erhalten eine Blockstruktur der Spitzenmenge.

5.1.1 Bildungsgesetze zu den einzelnen Blöcken

In diesem Abschnitt bestimmen wir für die Spitzen aus jedem Block die zugehörigen Bildungsgesetze der ersten Zeile der Streumatrix:

$$b_{1j}(c) = |\left\{[(\begin{smallmatrix}\star & \star\\c & \star\end{smallmatrix})] \in \left\langle T^{p^k}\right\rangle \setminus \Gamma(p^k)g_j/\left\langle T^{p^k}\right\rangle\right\}|$$

für $j \in \{1,\ldots,r\}$ und $c \in \mathbb{N}$.

Ein Bildungsgesetz für Spitzen aus den Fasern $\lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$ mit $t \equiv 0(p)$

Wir bestimmen in diesem Abschnitt die Bildungsgesetze für Spitzen aus einer Faser $\lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$ für $t \in \{1,\ldots,p^k-1\}$ mit $t \equiv 0(p)$. Sei $s_j = [\begin{smallmatrix}x\\y\end{smallmatrix}] \in \lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$, also mit $y \equiv 0(p)$. Da die zugehörige Matrix $g_j \in \Gamma$ mit $g_j\infty = s_j$ bis auf Multiplikation mit T^n von rechts eindeutig bestimmt ist, können wir $g_j = \begin{pmatrix}x & z_1\\y & z_2\end{pmatrix}$

so wählen, daß $z_1 \equiv t(p^k)$. Für $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(p^k)$ folgt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} g_j = \begin{pmatrix} ax + by & az_1 + b_z 2 \\ c' = cx + dy & cz_1 + dz_2 \end{pmatrix}$$

und wegen $c \equiv 0(p^k)$, $d \equiv \pm 1$ und $y \equiv t(p^k)$ gilt $cx + dy \equiv \pm t(p^k)$. Es kann also nur dann einen Repräsentanten einer Doppelnebenklasse geben, wenn die linke untere Ecke kongruent $\pm t$ modulo p^k ist.
Sei im Weiteren $c' \in \mathbb{N}$ mit $c' \equiv \pm t(p^k)$ fest.
Wie im Fall von $\Gamma(p)$ wollen wir eine Bijektion zwischen den Doppelnebenklassen und einer uns besser bekannten Menge herstellen. Dazu identifizieren wir jede Klasse zunächst mit ihrem oberen linken Eintrag, den wir modulo $c'p^k$ reduzieren:

$$\begin{array}{rccc} \Theta_{j,c'} : & \langle T^p \rangle \setminus \Gamma(p) g_j / \langle T^p \rangle & \longrightarrow & \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star \\ & \left[\begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix}\right] & \longmapsto & \alpha \bmod c'p^k. \end{array}$$

Mit Überlegungen wie in Abschnitt 4.1 sehen wir, daß diese Abbildung wohldefiniert und injektiv ist, und jetzt suchen wir eine Teilmenge von $\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$ so, daß wir eine Bijektion erhalten. Anders als bei den Überlegungen zu $\Gamma(p)$ sind jetzt hier verschiedene Fälle für t zu unterscheiden, da wir für die Bildmenge in Abhängigkeit von t unterschiedliche Kongruenzen verwenden müssen. Dies liegt daran, daß sich für verschiedene t dieselben Werte für c' ergeben können. Wir verdeutlichen dies an zwei Beispielen:

5.5 Beispiele:

1. $\Gamma(16)$ hat $r = 96$ Spitzen, die sich auf 24 Fasern von λ mit jeweils 4 Elementen verteilen. Bei den Bildungsgesetzen aus den Fasern $\lambda^{-1}(\left[\begin{smallmatrix} 1 \\ t \end{smallmatrix}\right])$ für $t \in \{0, 2, 4, 6, 8, 10, 12, 14\}$ gibt es jeweils nur für $c' \equiv \pm t(16)$ einen Eintrag, anders als bisher überschneiden sich diese Kongruenzen: So ist z.B. $c' \equiv \pm 2(16)$ gleichwertig zu $c' \equiv \pm 14(16)$. Es ergeben sich folgende Übereinstimmungen:

$$\begin{array}{llll} t = 0 & c' \equiv 0(16) & & \\ t = 2 & c' \equiv \pm 2(16) & \text{entspricht} & c' \equiv \pm 14(16) \\ t = 4 & c' \equiv \pm 4(16) & \text{entspricht} & c' \equiv \pm 12(16) \\ t = 6 & c' \equiv \pm 6(16) & \text{entspricht} & c' \equiv \pm 10(16) \\ t = 8 & c' \equiv \pm 8(16) & & \end{array}$$

2. $\Gamma(9)$ hat $r = 36$ Spitzen aus 12 Fasern von λ mit jeweils 3 Elementen. Für $t \in \{0, 3, 6\}$ gibt es jeweils nur für $c' \equiv \pm t(9)$ einen Eintrag, die Kongruenz $c' \equiv \pm 3(9)$ stimmt mit $c' \equiv \pm 6(9)$ überein.

Daher gibt es für $p = 2$ in $\Gamma(2^k)$ zwei Kongruenzen, die sich nicht in andere umformen lassen, und für $p > 2$ nur eine solche Kongruenz. Sei zunächst $t = 0$ für $p \neq 2$ und $t \in \{0, \frac{p^k}{2}\}$ für $p = 2$ und $s_j = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \lambda^{-1}(\left[\begin{smallmatrix} 1 \\ t \end{smallmatrix}\right])$ ein Repräsentant einer Spitzenklasse aus $\lambda^{-1}(\left[\begin{smallmatrix} 1 \\ t \end{smallmatrix}\right])$. Wir suchen jetzt eine geeignete Teilmenge von $\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$ so, daß $\Theta_{j,c'}$ eine Bijektion ist. Dazu sei:

$$U_{j,c'} := \{\alpha \in \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star : \alpha \equiv \pm\bar{x}(p^k)\}$$

mit $x \equiv \bar{x}(p^k)$ und $\bar{x} \in \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$. Dabei kann $\bar{x}$ nicht Null sein, da $y \equiv 0(p^k)$ und $ggt(x, y) = 1$. Wir betrachten jetzt:

$$\tilde{\Theta}_{j,c'} : \quad \langle T^p \rangle \setminus \Gamma(p) g_j / \langle T^p \rangle \quad \longrightarrow \quad U_{j,c'}$$

und sehen wie im Beweis zu Lemma 4.7, daß dies ein Isomorphismus ist. Dabei können wir den Beweis analog übernehmen, da $t = 0$ für $p > 2$ bzw. $t \in \{0, \frac{p^k}{2}\}$ für $p = 2$ und wir sehen schon, daß wir unsere Beschreibung der Menge $U_{j,c'}$ für die anderen t anpassen müssen. Hier haben wir unsere gesuchte Anzahl $b_{1j}(c')$ jetzt mit der Anzahl der Elemente in $U_{j,c'}$ identifiziert. Für $c' = c_0 p^{l+k}$ mit $c_0, l \in \mathbb{Z}$ und $p \nmid c_0$ folgt:

$$|\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star| = \varphi(c'p^k) = \varphi(c_0 p^{l+k}) = p^{l+k-1}(p-1)\varphi(c_0) = p^k\varphi(c').$$

In $\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$ gibt es genau $\varphi(p^k) = p^{k-1}(p-1)$ Möglichkeiten, kongruent $x \bmod p^k$ mit $x \neq 0$ zu sein, also sind es modulo ± 1 genau $\frac{\varphi(p^k)}{2} = \frac{p^{k-1}(p-1)}{2}$ Möglichkeiten und wir erhalten:

$$|U_{j,c'}| = \frac{p^k\varphi(c')}{\frac{p^{k-1}}{2}(p-1)} = \frac{2p^k}{p^{k-1}(p-1)}\varphi(c') = \frac{2p}{p-1}\varphi(c').$$

Insgesamt ist also gezeigt:

5.6 Satz: *Sei s_j eine Spitze aus der Faser von $\lambda^{-1}(\left[\begin{smallmatrix} 1 \\ t \end{smallmatrix}\right])$ mit $t = 0$ für $p \neq 2$ und $t \in \{0, \frac{p^k}{2}\}$ für $p = 2$. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \frac{2p}{p-1}\varphi(c) & \text{für } c \equiv t(p^k) \\ 0 & \text{für } c \not\equiv 0(p^k) \end{cases}$$

für $c \in \mathbb{N}$.

Jetzt betrachten wir die anderen Fasern von $\lambda^{-1}(\left[\begin{smallmatrix} 1 \\ t \end{smallmatrix}\right])$ für ein $t \equiv 0(p)$, $t \not\equiv 0(p^k)$ für $p > 2$ bzw. $t \notin \{0, \frac{p^k}{2}\}$ für $p = 2$ und wir wollen das folgende Bildungsgesetz zeigen:

5.7 Satz: *Sei s_j eine Spitze aus der Faser von $\lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$ mit $t \equiv 0(p)$, $t \not\equiv 0(p^k)$ für $p > 2$ bzw. $t \notin \{0, \frac{p^k}{2}\}$ für $p = 2$. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \frac{p}{p-1}\varphi(c) & \text{für } c \equiv \pm t(p^k) \\ 0 & \text{für } c \not\equiv 0(p^k) \end{cases}$$

für $c \in \mathbb{N}$.

Beweis:
Um aus $\Theta_{j,c'}$ eine Bijektion zu erhalten, definieren wir folgende Teilmenge von $\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$:

$$U_{j,c'} := \{\alpha \in \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star : \alpha \equiv \bar{x}(p^k)\}$$

mit $x \equiv \bar{x}(p^k)$ und $\bar{x} \in \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$. Der Unterschied zu der bisher verwendeten Teilmenge liegt am eindeutig geforderten Vorzeichen: Statt $\alpha \equiv \pm\bar{x}(p^k)$ fordern wir hier $\alpha \equiv \bar{x}(p^k)$, wie in dem Fall von $\Gamma(p)$ bei den Spitzen aus $\lambda^{-1}([\begin{smallmatrix}t\\1\end{smallmatrix}])$ mit $t \in \{0, \ldots, p-1\}$. Analog zu dem Beweis des dortigen Lemmas 4.10 ist durch die Kongruenz im Zähler der Spitzenklasse das Vorzeichen bereits festgelegt, so daß wir in $U_{j,c'}$ keine Wahl mehr haben. Damit haben wir die gesuchte Anzahl $b_{1j}(c')$ mit der Anzahl der Elemente in $U_{j,c'}$ identifiziert und da es in $\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$ genau $\varphi(p^k) = p^{k-1}(p-1)$ Möglichkeiten gibt, kongruent $\bar{x} \bmod p^k$ mit $\bar{x} \neq 0$ zu sein, erhalten wir insgesamt:

$$|U_{j,c'}| = |\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star| \frac{1}{\varphi(p^k)} = \frac{p^k\varphi(c')}{p^{k-1}(p-1)} = \frac{p}{p-1}\varphi(c')$$

□

Ein Bildungsgesetz für Spitzen aus $\lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$ mit $u \in \{1, \ldots, p^k - 1\}$

Wir bestimmen das Bildungsgesetz für Spitzen aus den Fasern $\lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$ mit $u \in \{1, \ldots, p^k - 1\}$. Dazu sei $s_j = [\begin{smallmatrix}x\\y\end{smallmatrix}] \in \lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$, also ein Repräsentant einer Spitzenklasse mit:

$$y \in \{1, \ldots, p^k - 1\} \text{ und } y \not\equiv 0(p)$$

und wir bestimmen für ein $c' \in \mathbb{N}$ die Anzahl der Doppelnebenklassen:

$$b_{1j}(c') = |\left\{[(\begin{smallmatrix}\star & \star\\ c' & \star\end{smallmatrix})] \in \langle T^{p^k}\rangle \setminus \Gamma(p^k)g_j/\langle T^{p^k}\rangle\right\}|.$$

Die Matrix $g_j = \begin{pmatrix} x & z_1 \\ y & z_2 \end{pmatrix}$ ist nach Satz 1.10 eindeutig bis auf Multiplikation mit T^n von rechts bestimmt, so daß wir hier g_j so wählen, daß $z_2 \equiv 0(p^k)$. Für $(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}) \in \Gamma(p^k)$ folgt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} g_j = \begin{pmatrix} ax + by & az_1 + b_z2 \\ c' = cx + dy & cz_1 + dz_2 \end{pmatrix}$$

und wegen $c \equiv 0(p^k)$ und $d \equiv \pm 1(p^k)$ erhalten wir: $cx+dy \equiv \pm y(p)$. Es kann also nur dann einen Repräsentanten einer Doppelnebenklasse geben, wenn die linke untere Ecke kongruent $\pm\bar{y}$ modulo p^k ist. Dabei durchläuft $\pm y \in \{1, \ldots, p^k - 1\}$ mit $y \not\equiv 0(p)$ in einer Faser $\lambda^{-1}(\begin{bmatrix} u \\ 1 \end{bmatrix})$ alle Möglichkeiten, modulo ± 1 sind dies $\frac{\varphi(p^k)}{2} = p^{k-1}\frac{p-1}{2}$ Möglichkeiten und damit eine mögliche Wahl für alle Repräsentanten einer Faser.
Sei im Weiteren $c' \in \mathbb{N}$ mit $c' \equiv \pm y(p^k)$ fest.
Unsere Abbildung $\Theta_{j,c'}$ identifiziert jede Klasse zunächst mit ihrem oberen linken Eintrag, den wir modulo $c'p^k$ reduzieren:

$$\begin{array}{rccc} \Theta_{j,c'}: & \langle T^p \rangle \setminus \Gamma(p) g_j / \langle T^p \rangle & \longrightarrow & \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star \\ & \left[\begin{pmatrix} \alpha & \beta \\ c' & \delta \end{pmatrix}\right] & \longmapsto & \alpha \bmod c'p^k \end{array}$$

und ist wegen der speziellen Wahl von g_j wohldefiniert und injektiv. Jetzt suchen wir eine Teilmenge von $\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star$ so, daß wir eine Bijektion erhalten:

$$U_{j,c'} := \{\alpha \in \left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star : \alpha \equiv u(p^k)\}.$$

Wir betrachten nun:

$$\tilde{\Theta}_{j,c'}: \ \langle T^p \rangle \setminus \Gamma(p) g_j / \langle T^p \rangle \ \longrightarrow \ U_{j,c'}$$

und sehen wie im Beweis zu Lemma 4.7, daß dies ein Isomorphismus ist. Damit haben wir unsere gesuchte Anzahl $b_{1j}(c')$ mit der Anzahl der Elemente in $U_{j,c'}$ identifiziert. Mit $|\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star| = p^k\varphi(c')$ folgt

$$|U_{j,c'}| = \frac{1}{p^k}|\left(\mathbb{Z}/c'p^k\mathbb{Z}\right)^\star| = \varphi(c'),$$

da es in $(\mathbb{Z}/c'p\mathbb{Z})^\star$ genau $\frac{1}{p^k}$ Möglichkeiten gibt, kongruent $u \bmod p^k$ zu sein. Insgesamt haben wir damit gezeigt:

5.8 Satz: *Sei $s_j = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ eine Spitze aus einer Faser $\lambda^{-1}(\left[\begin{smallmatrix} u \\ 1 \end{smallmatrix}\right])$ mit $u \in \{1, \ldots, p^k - 1\}$. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \varphi(c) & \text{für } c \equiv \pm y(p^k) \\ 0 & \text{für } c \not\equiv \pm y(p^k) \end{cases}$$

für $c \in \mathbb{N}$.

Jetzt möchten wir wieder eine Abbildung konstruieren, die zwei Repräsentanten von Spitzenklassen die Nummer des zugehörigen Bildungsgesetzes zuordnet.

Dazu überlegen wir uns zunächst, wie viele verschiedene Bildungsgesetze wir für $\Gamma(p^k)$ bestimmt haben:
Wir haben im zweiten Abschnitt in jeder der n Fasern der Gestalt $\lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$ für $u \in \{1, \ldots, p^k - 1\}$ genau $\frac{\varphi(p^k)}{2} = p^{k-1}\frac{p-1}{2}$ Bildungsgesetze bestimmt. Im ersten Abschnitt haben wir $p^k - \varphi(p^k)$ Fasern der Gestalt $\lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$ für $t \in \{1, \ldots, p^k - 1\}$ mit $t \equiv 0(p)$ untersucht.
Für $p > 2$ gibt es eine Faser mit dem Bildungsgesetz aus Satz 5.6 und für die anderen $p^k - \varphi(p^k) - 1$ Fasern stimmen jeweils zwei Kongruenzen der Bildungsgesetze aus Satz 5.7 überein, so daß wir hier $1 + \frac{p^k - \varphi(p^k) - 1}{2} = \frac{p^k - \varphi(p^k) + 1}{2}$ Bildungsgesetze bestimt haben. Insgesamt erhalten wir für $p > 2$ genau:

$$\frac{\varphi(p^k)}{2} + \frac{p^k - \varphi(p^k) + 1}{2} = \frac{p^k + 1}{2}$$

verschiedene Bildungsgesetze.
Für $p = 2$ gibt es zwei Fasern mit dem Bildungsgesetz aus Satz 5.6, so daß wir im ersten Abschnitt $\frac{p^k - \varphi(p^k) + 2}{2}$ Bildunsgesetze und damit insgesamt:

$$\frac{\varphi(p^k)}{2} + \frac{p^k - \varphi(p^k) + 2}{2} = \frac{p^k + 2}{2}$$

Bildungsgesetze gezeigt haben.
Für $\Gamma(p)$ folgte im vorherigen Kapitel noch ein Abschnitt 4.3. Dort haben wir eine spezielle Anordnung der Bildungsgesetze in der Streumatrix gezeigt. Diese Ergebnisse können wir so nicht auf $\Gamma(p^k)$ übetragen. Aber wir haben in diesem Abschnitt gesehen, daß sich die Matrix der Bildungsgesetze ebenfalls in Blöcken anordnen lässt. Wir beobachten, daß die Blöcke zu Spitzen aus Fasern der Gestalt $\lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$ mit $u \in \{1, \ldots, p^k - 1\}$ wieder nach links durchgeschobene Nummern der Bildungsgesetze enthalten. Im Unterschied zu $\Gamma(p)$ gibt es hier aber mehrere Blöcke mit jeweils identischen Bildungsgesetzen, die sich parallel zur Hauptdiagonalen anordnen lassen.
Als Beispiel geben wir hier die $\frac{8+2}{2} = 5$ Bildungsgesetze für $\Gamma(8)$ an:

5.9 Beispiel: $\Gamma(8)$ ist eine Untergruppe vom Index 192 mit 24 Spitzen der Breite 8, die sich auf 12 Fasern mit je 2 Elementen verteilen, so daß sich der Spitzenvektor wie folgt sortieren läßt:

$$\begin{aligned}
S(\Gamma(8)) \;=\; & \lambda^{-1}\left(\begin{bmatrix}1\\0\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}3\\8\end{bmatrix}\right\} \;\cup\; \lambda^{-1}\left(\begin{bmatrix}1\\2\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\-2\end{bmatrix}\right\} \\
\cup\; & \lambda^{-1}\left(\begin{bmatrix}1\\4\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}3\\-4\end{bmatrix}\right\} \;\cup\; \lambda^{-1}\left(\begin{bmatrix}1\\6\end{bmatrix}\right) = \left\{\begin{bmatrix}3\\2\end{bmatrix}, \begin{bmatrix}1\\-2\end{bmatrix}\right\} \\
\cup\; & \lambda^{-1}\left(\begin{bmatrix}1\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}5\\-3\end{bmatrix}\right\} \;\cup\; \lambda^{-1}\left(\begin{bmatrix}2\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}2\\-3\end{bmatrix}\right\}
\end{aligned}$$

$$\cup \quad \lambda^{-1}\left(\begin{bmatrix}3\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\3\end{bmatrix}\begin{bmatrix}3\\1\end{bmatrix}\right\} \quad \cup \quad \lambda^{-1}\left(\begin{bmatrix}4\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\-3\end{bmatrix},\begin{bmatrix}4\\3\end{bmatrix}\right\}$$

$$\cup \quad \lambda^{-1}\left(\begin{bmatrix}5\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}3\\-1\end{bmatrix}\begin{bmatrix}1\\-3\end{bmatrix}\right\} \quad \cup \quad \lambda^{-1}\left(\begin{bmatrix}6\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}2\\-1\end{bmatrix},\begin{bmatrix}2\\3\end{bmatrix}\right\}$$

$$\cup \quad \lambda^{-1}\left(\begin{bmatrix}7\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}1\\-1\end{bmatrix},\begin{bmatrix}3\\5\end{bmatrix}\right\} \quad \cup \quad \lambda^{-1}\left(\begin{bmatrix}8\\1\end{bmatrix}\right) = \left\{\begin{bmatrix}0\\-1\end{bmatrix},\begin{bmatrix}8\\-3\end{bmatrix}\right\}$$

Wir erhalten folgende Bildungsgesetze:

$$b_0(c) = \begin{cases} 4\varphi(c) & \text{für } c \equiv 0(8) \\ 0 & \text{sonst} \end{cases}$$
$$b_1(c) = \begin{cases} \varphi(c) & \text{für } c \equiv \pm 1(8) \\ 0 & \text{sonst} \end{cases}$$
$$b_2(c) = \begin{cases} 2\varphi(c) & \text{für } c \equiv \pm 2(8) \\ 0 & \text{sonst} \end{cases}$$
$$b_3(c) = \begin{cases} \varphi(c) & \text{für } c \equiv \pm 3(8) \\ 0 & \text{sonst} \end{cases}$$
$$b_4(c) = \begin{cases} 4\varphi(c) & \text{für } c \equiv \pm 4(8) \\ 0 & \text{sonst} \end{cases}$$

Jetzt können wir die erste Zeile der Matrix der Bildungsgesetze angeben. Zur übersichtlicheren Darstellung identifizieren wir jedes Bildungsgesetz mit seiner entsprechenden Nummer:

$$B' = \begin{pmatrix} 0 & 0 & 2 & 2 & 4 & 4 & 2 & 2 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 \end{pmatrix}$$

Um zu sehen, wie sich diese Bildungsgesetze auf die Fasern verteilen, geben wir in folgender Tabelle zu jeder Faser die zu ihren Repräsentanten gehörenden Bildungsgesetze an:

Faser	Bildungsgesetze
$\lambda^{-1}\left(\begin{bmatrix}1\\0\end{bmatrix}\right)$	b_0
$\lambda^{-1}\left(\begin{bmatrix}1\\2\end{bmatrix}\right)$	b_2
$\lambda^{-1}\left(\begin{bmatrix}1\\4\end{bmatrix}\right)$	b_4
$\lambda^{-1}\left(\begin{bmatrix}1\\6\end{bmatrix}\right)$	b_2
$\lambda^{-1}\left(\begin{bmatrix}1\\1\end{bmatrix}\right)$	b_1, b_3
$\lambda^{-1}\left(\begin{bmatrix}2\\1\end{bmatrix}\right)$	b_1, b_3
$\lambda^{-1}\left(\begin{bmatrix}3\\1\end{bmatrix}\right)$	b_1, b_3
$\vdots$	
$\lambda^{-1}\left(\begin{bmatrix}8\\1\end{bmatrix}\right)$	b_1, b_3

Auf der nächsten Seite geben wir die Matrix der Bildungsgesetze von $\Gamma(8)$an, die die folgende Gestalt hat:

$$B := \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc|cc|cc|cc|cc|cc} 0&0&2&2&4&4&2&2&1&3&1&3&1&3&1&3&1&3&1&3&1&3\\ 0&0&2&2&4&4&2&2&3&1&3&1&3&1&3&1&3&1&3&1&3&1\\ \hline 2&2&0&0&2&2&4&4&1&3&1&3&1&3&1&3&1&3&1&3&1&3\\ 2&2&0&0&2&2&4&4&3&1&3&1&3&1&3&1&3&1&3&1&3&1\\ \hline 4&4&2&2&0&0&2&2&1&3&1&3&1&3&1&3&1&3&1&3&1&3\\ 4&4&2&2&0&0&2&2&3&1&3&1&3&1&3&1&3&1&3&1&3&1\\ \hline 2&2&4&4&2&2&0&0&1&3&1&3&1&3&1&3&1&3&1&3&1&3\\ 2&2&4&4&2&2&0&0&3&1&3&1&3&1&3&1&3&1&3&1&3&1\\ \hline 1&3&1&3&1&3&1&3&0&0&2&2&4&4&2&2&1&3&1&3&1&3\\ 1&3&1&3&1&3&1&3&0&0&2&2&4&4&2&2&3&1&3&1&3&1\\ \hline 1&3&1&3&1&3&1&3&2&2&0&0&2&2&4&4&1&3&1&3&1&3\\ 1&3&1&3&1&3&1&3&2&2&0&0&2&2&4&4&3&1&3&1&3&1\\ \hline 1&3&1&3&1&3&1&3&4&4&2&2&0&0&2&2&1&3&1&3&1&3\\ 1&3&1&3&1&3&1&3&4&4&2&2&0&0&2&2&3&1&3&1&3&1\\ \hline 1&3&1&3&1&3&1&3&2&2&4&4&2&2&0&0&1&3&1&3&1&3\\ 1&3&1&3&1&3&1&3&2&2&4&4&2&2&0&0&3&1&3&1&3&1\\ \hline 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&0&0&2&2&4&4&2&2\\ 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&0&0&2&2&4&4&2&2\\ \hline 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&2&2&0&0&2&2&4&4\\ 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&2&2&0&0&2&2&4&4\\ \hline 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&4&4&2&2&0&0&2&2\\ 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&4&4&2&2&0&0&2&2\\ \hline 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&2&2&4&4&2&2&0&0\\ 1&3&1&3&1&3&1&3&1&3&1&3&1&3&1&3&2&2&4&4&2&2&0&0 \end{array}\right)$$

5.2 Die Gruppen $\Gamma(n)$

Nachdem wir für eine Primzahlpotenz die Bildungsgesetze zur Hauptkongruenzgruppe $\Gamma(p^k)$ bestimmt haben, übertragen wir diese Ergebnisse jetzt auf $\Gamma(n)$ mit Primfaktorzerlegung $n = \prod_{i=1}^{m} p_i^{k_i}$, indem wir zunächst $\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ mit dem direkten Produkt der $\mathbb{P}^1(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$ identifizieren:

$$\begin{array}{rccc} f: & \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathbb{P}^1(\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \ldots \times \mathbb{P}^1(\mathbb{Z}/p_m^{k_m}\mathbb{Z}) \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & (\begin{bmatrix} x \\ y \end{bmatrix}_{p_1^{k_1}}, \ldots, \begin{bmatrix} x \\ y \end{bmatrix}_{p_m^{k_m}}) \end{array}$$

5.10 Satz: *Die Abbildung f ist ein Isomorphismus.*

Beweis:
f ist wohldefiniert:
Seien $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ mit $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \sim \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$, es existiert also ein $\lambda \in (\mathbb{Z}/n\mathbb{Z})^\star$ mit $x_1 = \lambda x_2$ und $y_1 = \lambda y_2$. Dann folgt für eine Komponente:

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}_{p_i^{k_i}} = \begin{bmatrix} \lambda x_2 \\ \lambda y_2 \end{bmatrix}_{p_i^{k_i}} = \bar{\lambda} \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}_{p_i^{k_i}}$$

mit $\lambda \equiv \bar{\lambda}(p_i^{k_i})$ und $\bar{\lambda} \in (\mathbb{Z}/n\mathbb{Z})^\star$, da $\lambda \not\equiv 0(p_i^{k_i})$. Injektivität und Surjektivität folgen genauso offensichtlich. □

Durch diesen Isomorphismus erhalten wir:

5.11 Satz: *Für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^m p_i^{k_i}$ gilt:*

$$|\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})| = \prod_{i=1}^m p_i^{k_i - 1}(p_i + 1)$$

Wir betrachten:

$$\begin{array}{rccc} \lambda: & \Gamma(n) \setminus \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{P}^1(\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \ldots \times \mathbb{P}^1(\mathbb{Z}/p_m^{k_m}\mathbb{Z}) \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & \left(\begin{bmatrix} x \\ y \end{bmatrix}_{p_1^{k_1}}, \ldots, \begin{bmatrix} x \\ y \end{bmatrix}_{p_m^{k_m}} \right) \end{array}$$

und untersuchen die Fasern dieser Abbildung, so daß wir offensichtlich folgenden Satz erhalten:

5.12 Satz: *Jede Faser von f hat $\prod_{i=1}^m p_i^{k_i - 1} \frac{p_i - 1}{2}$ Elemente.*

Jetzt können wir die

$$r = \prod_{i=1}^m p_i^{k_i - 1} \frac{p_i - 1}{2} \prod_{i=1}^m p_i^{k_i - 1}(p_i + 1)$$

Spitzenklassen von $\Gamma(n)$ nach den Fasern sortieren und erhalten wieder eine Blockstruktur der Bildungsgesetze. Um die Struktur der Fasern besser zu verstehen, suchen wir ein vollständiges Repräsentantensystem für die Aquivalenzklassen von $\mathbb{P}^1(Z/n\mathbb{Z})$. Dazu sei $m \neq 1$ und wir definieren:

$$\begin{array}{rcl} R & := & \left\{ \begin{bmatrix} 1 \\ t \end{bmatrix}, \begin{bmatrix} t \\ 1 \end{bmatrix} : t \in \mathbb{Z}/n\mathbb{Z}, \exists\ p_i \text{ mit } t \equiv 0(p_i) \right\} \bigcup \left\{ \begin{bmatrix} y \\ 1 \end{bmatrix} : y \in (\mathbb{Z}/n\mathbb{Z})^\star \right\} \\ & \bigcup & \left\{ \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} : t_1, t_2 \in \mathbb{Z}/n\mathbb{Z}, \exists\ p_i, p_j \text{ mit } t_1 \equiv 0(p_i), t_2 \equiv 0(p_j) \text{ und ggt } (t_1, t_2) = 1 \right\} \end{array}$$

Offensichtlich erzeugen alle Paare $< x, y >$ aus R ganz $\mathbb{Z}/n\mathbb{Z}$ und sind bezüglich der Äquivalenzrelation $\sim$ nicht zueinander äquivalent, da sie sich nicht durch ein $\lambda \in (\mathbb{Z}/n\mathbb{Z})^\star$ ineinander überführen lassen. Es bleibt noch zu zeigen, daß alle anderen Elemente $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{P}^1(\mathbb{Z}/n\mathbb{Z})$ zu einem Repräsentanten aus R äquivalent sind.

1. $y \equiv 0(p_i)$ für einen Primfaktor p_i und $x \not\equiv 0(p_j)$ für alle $1 \leq j \leq m$:
   Dann läßt sich $x \not\equiv 0(p_i)$ invertieren und wir erhalten $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ yx^{-1} \end{smallmatrix}\right]$ mit $yx^{-1} \in \mathbb{Z}/n\mathbb{Z}$, also ist $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ zu einem Element aus R äquivalent.
2. $x \equiv 0(p_i)$ für einen Primfaktor p_i und $x \not\equiv 0(p_j)$ für alle $1 \leq j \leq m$:
   Analog läßt sich x in $\mathbb{Z}/n\mathbb{Z}$ invertieren und $\left[\begin{smallmatrix} yx^{-1} \\ 1 \end{smallmatrix}\right]$ liegt in R.
3. $x, y \not\equiv 0(p)$: Dann ist y in in $\mathbb{Z}/n\mathbb{Z}$ invertierbar und $\left[\begin{smallmatrix} yx^{-1} \\ 1 \end{smallmatrix}\right]$ liegt in R.
4. $\exists i, j \in \{1, \ldots, m\}$ mit $x \equiv 0(p_i), y \equiv 0(p_j)$:
   Dann liegt $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ wegen $ggt(x, y) = 1$ in R.

Wir können also $\mathbb{P}^1(\mathbb{Z}/nZ)$ durch R repräsentieren.

5.13 Beispiel: Für $\mathbb{P}^1(\mathbb{Z}/15Z)$ können wir folgende Repräsentanten wählen:

$$\begin{aligned} \mathbb{P}^1(\mathbb{Z}/nZ) \quad = \quad & \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \end{bmatrix}, \begin{bmatrix} 5 \\ 1 \end{bmatrix}, \ldots, \begin{bmatrix} 14 \\ 1 \end{bmatrix}, \right. \\ & \left. \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 5 \end{bmatrix}, \begin{bmatrix} 1 \\ 6 \end{bmatrix}, \begin{bmatrix} 1 \\ 9 \end{bmatrix}, \begin{bmatrix} 1 \\ 10 \end{bmatrix}, \begin{bmatrix} 1 \\ 12 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 5 \\ 3 \end{bmatrix} \right\} \end{aligned}$$

5.2.1 Bildungsgesetze zu den einzelnen Blöcken

In diesem Abschnitt skizzieren wir für die Spitzen aus jedem Block, wie man die zugehörigen Bildungsgesetze der ersten Zeile der Streumatrix:

$$b_{1j}(c) = |\, \{[(\begin{smallmatrix} \star & \star \\ c & \star \end{smallmatrix})] \in \langle T^n \rangle \setminus \Gamma(n) g_j / \langle T^n \rangle\} \,|$$

für $j \in \{1, \ldots, r\}$ und $c \in \mathbb{N}$ bestimmt. Im Unterschied zu $\Gamma(p^k)$ kommen hier noch Kombinationen aus Potenzen der Primfaktoren hinzu. Wir können die Bildungsgesetze für die ersten beiden Arten von Fasern analog zu $\Gamma(p^k)$ zeigen:

Ein Bildungsgesetz für Spitzen aus $\lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$ mit $u \in \{1,\ldots,n-1\}$

Ganz analog zu dem entsprechenden Abschnitt für $\Gamma(p^k)$ betrachten wir eine Spitze $s_j = [\begin{smallmatrix}x\\y\end{smallmatrix}] \in \lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$, also einen Repräsentant einer Spitzenklasse mit:

$$y \in \{1,\ldots,n-1\}$$

und bestimmen für ein $c' \in \mathbb{N}$ die Anzahl der Doppelnebenklassen:

$$b_{1j}(c') = |\,\{[(\begin{smallmatrix}\star & \star\\ c' & \star\end{smallmatrix})] \in \langle T^n\rangle \setminus \Gamma(n)g_j/\langle T^n\rangle\}\,|.$$

Die Matrix $g_j = \begin{pmatrix} x & z_1 \\ y & z_2 \end{pmatrix}$ ist nach Satz 1.10 eindeutig bis auf Multiplikation mit T^n von rechts bestimmt, so daß wir hier g_j so wählen, daß $z_2 \equiv 0(n)$. Für $(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}) \in \Gamma(p^k)$ folgt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} g_j = \begin{pmatrix} ax+by & az_1+b_z2 \\ c'=cx+dy & cz_1+dz_2 \end{pmatrix}$$

und wegen $c \equiv 0(n)$ und $d \equiv \pm 1(n)$ erhalten wir: $cx+dy \equiv \pm y(n)$. Es kann also nur dann einen Repräsentanten einer Doppelnebenklasse geben, wenn die linke untere Ecke kongruent $\pm\bar{y}$ modulo n ist. Sei im Weiteren $c' \in \mathbb{N}$ mit $c' \equiv \pm y(n)$ fest. Durch Konstruktion analoger Abbildungen identifizieren wir die gesuchte Anzahl $b_{1j}(c')$ mit der Anzahl der Elemente in:

$$U_{j,c'} :=:= \{\alpha \in (\mathbb{Z}/c'n\mathbb{Z})^\star : \alpha \equiv u(n)\}.$$

und zeigen damit insgesamt:

5.14 Satz: *Sei $s_j = [\begin{smallmatrix}x\\y\end{smallmatrix}]$ eine Spitze aus einer Faser $\lambda^{-1}([\begin{smallmatrix}u\\1\end{smallmatrix}])$ mit $u \in \{1,\ldots,n-1\}$. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \varphi(c) & \text{für } c \equiv \pm y(n) \\ 0 & \text{für } c \not\equiv \pm y(n) \end{cases}$$

für $c \in \mathbb{N}$.

Ein Bildungsgesetz für Spitzen aus den Fasern $\lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$ mit $t \equiv 0(p_i)$

Wir bestimmen das Bildungsgesetz für Spitzen aus den Fasern $\lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$ mit $t \equiv 0(p_i)$ für ein $i \in \{1,\ldots,m\}$. Dazu sei $s_j = [\begin{smallmatrix}x\\y\end{smallmatrix}] \in \lambda^{-1}([\begin{smallmatrix}1\\t\end{smallmatrix}])$, also ein Repräsentant einer Spitzenklasse, zu der eine Teilmenge $V \subset \{1,\ldots,m\}$ existiert mit:

$$y \equiv 0(p_i)\ \forall\ i \in V \quad \text{und} \quad y \not\equiv 0(p_j)\ \forall\ j \notin V.$$

Die gesuchte Anzahl der Doppelnebenklassen ergibt sich ausgehend von den Primfaktoren p_i für $i \in V$ als Produkt über die entsprechenden Gesetze von $\Gamma(p^{k_i})$, wobei der Fall $p_i = 2$ wiederum gesondert betrachtet werden muss. Wir formulieren hier nur die Aussage für ungerades n, die durch Rückführung auf $\Gamma(p^{k_i})$ zu zeigen ist:

5.15 Satz: *Sei s_j eine Spitze aus der Faser von $\lambda^{-1}(\left[\begin{smallmatrix}1\\t\end{smallmatrix}\right])$ mit $y \equiv 0(p_i)\ \forall\ i \in V \quad$ und $\quad y \not\equiv 0(p_j)\ \forall\ j \notin V$. Dann folgt für das zugehörige Bildungsgesetz der ersten Zeile:*

$$b_{1j}(c) = \begin{cases} \prod_{i \in V} \frac{p_i}{p_i - 1}\varphi(c) & \text{für } c \equiv \pm t(n) \\ 0 & \text{für } c \not\equiv 0(p^k) \end{cases}$$

für $c \in \mathbb{N}$.

Wir führen sowohl für diese Aussage als auch für die noch fehlenden Spitzenklassen aus den Fasern von $\lambda^{-1}(\left[\begin{smallmatrix}t_1\\t_2\end{smallmatrix}\right])$ für $t_1, t_2 \in \mathbb{Z}/n\mathbb{Z}, \exists\ p_i, p_j$ mit $t_1 \equiv 0(p_i), t_2 \equiv 0(p_j)$ und ggt $(t_1, t_2) = 1$ keinen Beweis durch, geben aber als Beispiel die Bildungsgesetze für $\Gamma(15)$ an:

5.16 Beispiel: $\Gamma(15)$ hat 96 Spitzen, die sich auf 24 Fasern mit jeweils 4 Elementen verteilen. Ausgehend von dem in Beispiel 5.13 angegebenen Repräsentantensystem für $\mathbb{P}^1(\mathbb{Z}/15Z)$ erhalten wir folgende Bildungsgesetze:

1 15 Fasern mit $i \in \{1, 2, 4, 7\}$ $\quad b_i(c) = \begin{cases} \varphi(c) & \text{für } c \equiv \pm i(n) \\ 0 & \text{für } c \not\equiv \pm i(n) \end{cases}$

da $\frac{\varphi(15)}{2} = 4$

2 Für $\lambda^{-1}(\begin{bmatrix}1\\i\end{bmatrix})$ mit $i \in \{3, 6, 9, 12\}$: $\quad b_i(c) = \begin{cases} \frac{3}{2}\varphi(c) & \text{für } c \equiv \pm i(n) \\ 0 & \text{für } c \not\equiv \pm 3(n) \end{cases}$

3 Für $\lambda^{-1}(\begin{bmatrix}1\\i\end{bmatrix})$ mit $i \in \{5, 10\}$: $\quad b_i(c) = \begin{cases} \frac{5}{4}\varphi(c) & \text{für } c \equiv \pm i(n) \\ 0 & \text{für } c \not\equiv \pm 5(n) \end{cases}$

4 Für $\lambda^{-1}(\begin{bmatrix}1\\0\end{bmatrix})$: $\quad b_0(c) = \begin{cases} \frac{15}{4}\varphi(c) & \text{für } c \equiv \pm 0(n) \\ 0 & \text{für } c \not\equiv \pm 0(n) \end{cases}$

5 Für $\lambda^{-1}(\begin{bmatrix}3\\5\end{bmatrix})$: $\quad b_5(c) = \begin{cases} \frac{3}{2}\varphi(c) & \text{für } c \equiv \pm 5(n) \\ 0 & \text{für } c \not\equiv \pm 5(n) \end{cases}$

6 Für $\lambda^{-1}(\begin{bmatrix}5\\3\end{bmatrix})$: $\quad b_3(c) = \begin{cases} \frac{3}{2}\varphi(c) & \text{für } c \equiv \pm 3(n) \\ 0 & \text{für } c \not\equiv \pm 3(n) \end{cases}$

6 Die Determinante der Streumatrix für $\Gamma(p)$

Um die Determinante der Streumatrix zu einer Hauptkongruenzgruppe $\Gamma(p)$ mit $p \in \mathbb{N}$ zu bestimmen, versuchen wir zunächst, die Streumatrix so weit wie möglich zu diagonalisieren. Zu den $r = (p+1)\frac{p-1}{2}$ Spitzenklassen in $S_p := \Gamma(p)\backslash\mathbb{P}^1(\mathbb{Q})$ wählen wir ein vollständiges Repräsentantensystem $S(\Gamma(p)) = \{s_1, \ldots, s_r\}$, so daß die Streumatrix eine $r \times r-$Matrix ist. Wir werden sehen, daß wir sie bis auf einen $(p-1) \times (p-1)-$Block diagonalisieren können.

6.1 Transformation in eine Matrix kleinerer Dimension

In Kapitel 4 haben wir $\frac{p-1}{2} + 1$ verschiedene Bildungsgesetze für die Anzahlen der Doppelnebenklassen mit festem $c \in \mathbb{N}$ links unten bestimmt, die wir mit ihrer Nummer in $\mathbb{F}_p/\{\pm 1\}$ identifiziert haben. Anschließend haben wir eine Abbildung:

$$\begin{array}{rccccc} F: & S_p \times S_p & \xrightarrow{(h,h)} & \Sigma_p \times \Sigma_p & \xrightarrow{f} & \mathbb{F}_p/\{\pm 1\} \\ & (\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} u \\ v \end{bmatrix}) & & \longmapsto & & xv - uy \bmod p \end{array}$$

konstruiert, die zwei Repräsentanten s_i, s_j der Spitzenklassen $[s_i], [s_j]$ die Nummer des entsprechenden Bildungsgesetzes b_{ij} zuordnet. Damit kodiert $\mathbb{F}_p/\{\pm 1\}$ die folgenden Bildungsgesetze:

$$b_0(c) = \begin{cases} \frac{2p}{p-1}\varphi(c) & \text{für } c \equiv 0(p) \\ 0 & \text{für } c \not\equiv 0(p) \end{cases},$$

$$b_1(c) = \begin{cases} \varphi(c) & c \equiv \pm 1(p) \\ 0 & c \not\equiv \pm 1(p) \end{cases}, \ldots, \quad b_{\frac{p-1}{2}}(c) = \begin{cases} \varphi(c) & c \equiv \pm\frac{p-1}{2}(p) \\ 0 & c \not\equiv \pm\frac{p-1}{2}(p) \end{cases}.$$

Wir haben die Spitzen von $\Gamma(p)$ nach den Fasern von λ sortiert. Da jede der $p+1$ Fasern genau $\frac{p-1}{2}$ Spitzenklassen enthält, ergab dies eine Blockstruktur für die Streumatrix mit $(p+1) \times (p+1)$ Blöcken der Größe $(\frac{p-1}{2} \times \frac{p-1}{2})$. Anhand

der Eigenschaften von F haben wir gesehen, daß die $(\frac{p-1}{2} \times \frac{p-1}{2})-$dimensionalen Blöcke auf der Hauptdiagonalen die Gestalt:

$$u_0 := \begin{pmatrix} b_0 & \cdots & b_0 \\ \vdots & \ddots & \vdots \\ b_0 & \cdots & b_0 \end{pmatrix}$$

haben. Die anderen $(\frac{p-1}{2} \times \frac{p-1}{2})-$dimensionalen Blöcke enthalten in jeder Zeile und in jeder Spalte die übrigen $\frac{p-1}{2}$ Bildungsgesetze. Da die Gegendiagonale in jedem Block wegen der Struktur von F immer dasselbe Bildungsgesetz enthält, werden die Bildungsgesetze nach links durchgeschoben. Jede Nummer kann in der oberen linken Ecke stehen, so daß wir $\frac{p-1}{2}$ verschiedene Blöcke erhalten:

$$u_1 = \begin{pmatrix} b_1 & b_2 & \cdots & b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} \\ b_2 & b_3 & \cdots & b_{\frac{p-1}{2}} & b_1 \\ & & \iddots & \iddots & \\ & \iddots & \iddots & & \\ b_{\frac{p-1}{2}} & b_1 & \ldots & b_{\frac{p-1}{2}-2} & b_{\frac{p-1}{2}-1} \end{pmatrix}$$

$$u_2 = \begin{pmatrix} b_2 & b_3 & \cdots & b_{\frac{p-1}{2}} & b_1 \\ b_3 & b_4 & \cdots & b_1 & b_2 \\ & & \iddots & \iddots & \\ & \iddots & \iddots & & \\ b_1 & b_2 & \cdots & b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} \end{pmatrix}$$

$$\vdots$$

$$u_{\frac{p-1}{2}} = \begin{pmatrix} b_{\frac{p-1}{2}} & b_1 & \ldots & b_{\frac{p-1}{2}-2} & b_{\frac{p-1}{2}-1} \\ b_1 & b_2 & \cdots & b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} \\ & & \iddots & \iddots & \\ & \iddots & \iddots & & \\ b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} & \ldots & b_{\frac{p-1}{2}-3} & b_{\frac{p-1}{2}-2} \end{pmatrix}$$

In unserer $((p+1)\frac{p-1}{2} \times (p+1)\frac{p-1}{2})-$dimensionalen Matrix B der Bildungsgesetze von $\Gamma(p)$ sind in jeder Zeile und jeder Spalte $p+1$ dieser Blöcke gemäß den Eigenschaften von F angeordnet. Wenn wir jeden dieser Blöcke mit seiner Bezeichnung entsprechend der Nummer des Bildungsgesetzes in der linken oberen Ecke identifizieren, erhalten wir eine $((p+1) \times (p+1))-$dimensionale Matrix

U der Gestalt:

$$U = \begin{pmatrix} u_0 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & \cdots & u_1 & u_1 & u_1 & u_1 \\ u_1 & u_0 & u_1 & u_2 & u_3 & \cdots & u_{\frac{p-1}{2}} & u_{\frac{p-1}{2}} & \cdots & u_3 & u_2 & u_1 \\ u_1 & u_1 & u_0 & u_1 & u_2 & u_3 & \cdots & u_{\frac{p-1}{2}} & u_{\frac{p-1}{2}} & \cdots & u_3 & u_2 \\ u_1 & u_2 & u_1 & u_0 & u_1 & u_2 & u_3 & \cdots & u_{\frac{p-1}{2}} & u_{\frac{p-1}{2}} & \cdots & u_3 \\ \vdots & & \ddots & \ddots & \ddots & & & & & & & \\ & & & & & & & & & & & \\ \vdots & & & & & & & & \ddots & \ddots & \ddots & \\ u_1 & u_1 & u_2 & u_3 & \cdots & \frac{p-1}{2} & \frac{p-1}{2} & \cdots & u_3 & u_2 & u_1 & u_0 \end{pmatrix}$$

Durch Streichen der ersten Zeile und ersten Spalte erhalten wir einen $(p \times p)$-dimensionalen Block mit nach rechts durchgeschobenen Einträgen, den wir mit U_p bezeichnen:

$$U_p = \begin{pmatrix} u_0 & u_1 & u_2 & u_3 & \cdots & u_{\frac{p-1}{2}} & u_{\frac{p-1}{2}} & \cdots & u_3 & u_2 & u_1 \\ u_1 & u_0 & u_1 & u_2 & u_3 & \cdots & u_{\frac{p-1}{2}} & u_{\frac{p-1}{2}} & \cdots & u_3 & u_2 \\ u_2 & u_1 & u_0 & u_1 & u_2 & u_3 & \cdots & u_{\frac{p-1}{2}} & u_{\frac{p-1}{2}} & \cdots & u_3 \\ & \ddots & \ddots & \ddots & & & & & & & \\ & & & & & & & & & & \\ & & & & & & & \ddots & \ddots & \ddots & \\ u_1 & u_2 & u_3 & \cdots & \frac{p-1}{2} & \frac{p-1}{2} & \cdots & u_3 & u_2 & u_1 & u_0 \end{pmatrix}.$$

Jetzt wollen wir U so weit wie möglich diagonalisieren. Um die dabei entstehende Gestalt zu beschreiben, sind einige Vorbemerkungen nötig: Sei $\omega \in \mathbb{C}$ eine $n-$te primitive Einheitswurzel:

$$\omega = e^{\frac{2\pi i}{n}}.$$

Dann gilt:

$$\sum_{k=1}^{n} \omega^k = 0.$$

Wir definieren folgende $n \times n-$ Matrix:

6.1 Definition:

$$T_n := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & (\omega^2)^2 & \cdots & \omega^{2(n-1)} \\ 1 & \omega^3 & (\omega^2)^3 & \cdots & \omega^{3(n-1)} \\ \vdots & & & & \\ 1 & \omega^{n-1} & (\omega^{n-1})^2 & \cdots & \omega^{(n-1)^2} \end{pmatrix}.$$

für die $n-$te primitive Einheitswurzel $\omega = e^{\frac{2\pi i}{n}}$.

Die Determinante dieser Matrix hat die Form einer *Vandermonde-Determinante* und berechnet sich folgendermassen [Fis79]:

$$\det T_n = \prod_{0 \le i < j \le n-1} (\omega^i - \omega^j).$$

Anstatt dieses Produkt weiter zu vereinfachen, bestimmen wir die Determinante hier mit folgendem Lemma:

6.2 Lemma: *Für $T_n = (t_{ij})_{1 \le i,j \le n}$ wie oben definiert und $\overline{T_n} := (\overline{t_{ij}})_{1 \le i,j \le n}$ mit den komplex konjugierten Einträgen von T_n gilt:*

$$T_n \overline{T_n} = nE_n.$$

Beweis:
Die Behauptung folgt durch Ausmultiplizieren:

$$\begin{aligned} \widetilde{T}_n &:= (\widetilde{t}_{ij})_{1 \le i,j \le n} := T_n \overline{T_n} \\ &= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ \vdots & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & (\omega^{(n-1)^2}) \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(n-1)} \\ \vdots & & & & \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \cdots & (\omega^{-(n-1)^2}) \end{pmatrix} \end{aligned}$$

Für die einzelnen Einträge von $\widetilde{T}_n$ erhalten wir:

$\widetilde{t}_{11} = n$ und $\widetilde{t}_{1i} = 0$ für $2 \le i \le n$
$\widetilde{t}_{21} = 0$ und $\widetilde{t}_{22} = 1 + \omega\omega^{-1} + \cdots + \omega^{n-1}\omega^{-(n-1)}$ und $\widetilde{t}_{1i} = 0$ für $3 \le i \le n$

und so weiter. □

6.3 Korollar: *Für die Determinante von T_n folgt:*

$$\det(T_n) = \pm(\sqrt{n})^n.$$

Beweis:
Mit Lemma 6.2 erhalten wir:

$$\det T_n \det \overline{T_n} = n^n.$$

Aus der Formel der Vandermonde-Determinante folgt wegen $\overline{\omega} = \omega^{n-1}$:

$$\begin{aligned} \det \overline{T_n} &= \prod_{0 \le i < j \le n-1} (\overline{\omega}^i - \overline{\omega}^j) &&= \prod_{0 \le i < j \le n-1} \omega^{n-1}(\omega^i - \omega^j) \\ &= (\omega^{n-1})^n \prod_{0 \le i < j \le n-1} (\omega^i - \omega^j) \\ &= \det T_n. \end{aligned}$$

Damit ist die Determinante von T_n bis auf das Vorzeichen bestimmt. □

Wir erhalten einige Eigenschaften:

1. T_n ist invertierbar
2. $|\det \frac{1}{\sqrt{n}} T_n| = 1$
3. $(\frac{1}{\sqrt{n}} T_n)^{-1} = \frac{1}{\sqrt{n}} \overline{T_n}$, also $T_n^{-1} = \frac{1}{n} \overline{T_n}$

Über *Dirichlet-Charaktere* modulo n:

$$\chi : \quad \mathbb{Z}/n\mathbb{Z} \quad \longrightarrow \quad \mathbb{C}^\star,$$

die durch folgende Eigenschaften definiert sind [IR90]:

1. $\chi(m+n) = \chi(n)$ für alle $m \in \mathbb{Z}$
2. $\chi(km) = \chi(k)\chi(n)$ für alle $k, m \in \mathbb{Z}$
3. $\chi(m) \neq 1 \Leftrightarrow \text{ggt } (m,n) = 1$ für $m \in \mathbb{Z}$

können wir die Matrix T_n einfacher ausdrücken: Für $n = \prod_{i=1}^{l} p_i^{l_i}$ ist $\mathbb{Z}/n\mathbb{Z}$ direktes Produkt der zyklischen Gruppen $Z/p_i^{l_i}\mathbb{Z}$ und zu jeder dieser Gruppen existieren $p_i^{l_i}$ Charaktere [IR90], so daß wir als Charaktergruppe $\widehat{\mathbb{Z}/n\mathbb{Z}}$ zu $\mathbb{Z}/n\mathbb{Z}$ erhalten:

$$\widehat{\mathbb{Z}/n\mathbb{Z}} = \{\chi_1, \ldots, \chi_n\}.$$

Für die Charaktere gilt:

$$\chi_j(m) = e^{\frac{2\pi i j m}{n}}.$$

Damit ergibt sich die Matrix T_n als:

$$T_n = (\chi_i(j))_{1 \leq i,j \leq n}.$$

Mit dieser Matrix übertragen wir Lemma 3.6 aus einem Artikel von Elstrodt, Grunewald und Mennicke [EGM85] in unsere Notation:

6.4 Lemma: *Sei $G = \{g_1, \ldots, g_n\}$ eine endliche multiplikative abelsche Gruppe mit Charaktergruppe $\widehat{G} = \{\chi_1, \ldots, \chi_n\}$ und sei $f : G \longrightarrow \mathbb{C}$ eine Abbildung. Dann ist die zyklische Matrix $(f(g_i^{-1} g_j))_{1 \leq i,j \leq n}$ unitär äquivalent zu der Diagonalmatrix D mit den Diagonaleinträgen:*

$$D_{kk} = \sum_{i=1}^{n} f(g_i)\chi_k(g_i)$$

für $1 \leq k \leq n$, also:

$$(f(g_i^{-1} g j))_{1 \leq i,j \leq n} = T_n D T_n^{-1}$$

und:

$$\det((f(g_i^{-1}gj))_{1\leq i,j\leq n}) = \prod_{k=1}^{n}\sum_{l=1}^{n} f(g_l)\chi_k(g_l).$$

Wir benutzen dieses Lemma, um für die Teilmatrix U_p von U eine unitäre Äquivalenz zu zeigen:

6.5 Lemma: *$R := T_pU_pT_p^{-1}$ hat Diagonalgestalt mit:*

$$R_{kk} = u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i(\omega^{ki} + \omega^{-ki})$$

für $0 \leq k \leq p-1$.

Beweis:
Wir zeigen die Behauptung durch Rückführung auf Lemma 6.4:
Zu $G := \mathbb{Z}/p\mathbb{Z} = \{g_0, \ldots, g_{p-1}\}$ mit zugehöriger Charaktergruppe $\widehat{G} = \{\chi_0, \ldots, \chi_{p-1}\}$ und $M := \{u_0, u_1, \ldots, u_{\frac{p-1}{2}}\}$ definieren wir die Abbildung:

$$\begin{array}{rccl} f: & G & \longrightarrow & M \\ & g & \longmapsto & f(g) = \left\{ \begin{array}{ll} u_0 & \text{für } g = 0 \\ u_i & \text{für } g \equiv \pm i(p) \end{array} \right. . \end{array}$$

Damit erhalten wir:

$$U_p = (f(g_i^{-1}g_j))_{0\leq i,j\leq p-1}.$$

Da sich M durch $g(u_i) = i$ offensichtlich in $\mathbb{C}$ einbetten läßt, wenden wir Lemma 6.4 an:

$$R_{ij} = 0 \text{ für alle } 0 \leq i,j \leq p \text{ mit } i \neq j$$

und:

$$\begin{aligned} R_{kk} &= \sum_{i=0}^{p-1} f(g_i)\chi_k(g_i) \text{ für } 1 \leq k \leq p \\ &= u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i(\chi_k(g_i) + \chi_k(g_{-i})) \\ &= u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i(\omega^{ki} + \omega^{-ki}) \quad \text{wegen } \chi_k(g_i) = \omega^{ki} \end{aligned}$$

□

6.6 Bemerkung: *Da wir die Gruppe $G := \mathbb{Z}/p\mathbb{Z}$ als $G = \{g_0, \ldots, g_{p-1}\}$ notieren wollen, schreiben wir die $p \times p-$ Matrix R als:*

$$R = (r_{ij})_{0 \le i,j \le p-1}$$

und die Charaktergruppe $\widehat{G}$ als $\widehat{G} = \{\chi_0, \ldots, \chi_{n-1}\}$ mit dem trivialen Charakter $\chi_0 := \chi_n$.

Wir sind eigentlich an einer Diagonalisierung von U interessiert und haben jetzt eine Diagonalisierung von U_p erreicht. Wir werden sehen, daß wir U nur bis auf einen $2 \times 2-$ Block diagonalisieren können, indem wir:

$$AUA^{-1}$$

berechnen, wobei A eine $(p+1)\times(p+1)-$Matrix ist, die aus T_p durch Hinzufügen einer Zeile aus Einsen und einer Spalte aus Nullen entsteht:

$$D := \underbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & & & \\ \vdots & & T_p & \\ 0 & & & \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} u_0 & u_1 & \cdots & u_1 \\ u_1 & & & \\ \vdots & & U_p & \\ u_1 & & & \end{pmatrix}}_{U} \underbrace{\begin{pmatrix} 1 & -1 & 0 \cdots & 0 \\ 0 & & & \\ \vdots & & T_p^{-1} & \\ 0 & & & \end{pmatrix}}_{A^{-1}}.$$

Durch Ausmultiplizieren erhalten wir mit Lemma 6.5:

$$D = \begin{pmatrix} D_{11} & D_{12} & & & \\ D_{21} & D_{22} & & 0 & \\ & & R_{11} & & \\ & 0 & & \ddots & \\ & & & & R_{(p-1)(p-1)} \end{pmatrix}$$

mit:

$$\begin{aligned}
D_{11} &= u_0 + pu_1 \\
D_{12} &= (u_0 + pu_1, u_0 + u_1 + \sum_{i=1}^{\frac{p-1}{2}} u_i, \ldots, u_0 + u_1 + \sum_{i=1}^{\frac{p-1}{2}} u_i)(-1, \frac{1}{p}, \ldots, \frac{1}{p})^T \\
&= -(u_0 + pu_1) + \frac{1}{p}p(u_0 + u_1 + \sum_{i=1}^{\frac{p-1}{2}} u_i) \\
&= (1-p)u_1 + \sum_{i=1}^{\frac{p-1}{2}} u_i \\
&= (3-p)u_1 + \sum_{i=2}^{\frac{p-1}{2}} u_i \\
D_{21} &= (pu_1, u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i, \ldots, u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i)(1, 0, \ldots, 0)^T \\
&= pu_1 \\
D_{22} &= (pu_1, u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i, \ldots, u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i)(-1, \frac{1}{p}, \ldots, \frac{1}{p})^T \\
&= -pu_1 + u_0 + \sum_{i=1}^{\frac{p-1}{2}} u_i \\
&= -pu_0 + R_{00}
\end{aligned}$$

Damit ist der erste Schritt getan: Wir haben die Matrix U bis auf einen $2 \times 2-$Block diagonalisiert.

6.2 Rücktransformation auf die Matrix der Bildungsgesetze

Wir hatten die Matrix U aus der Matrix der Bildungsgesetze erhalten, indem wir ganze Blöcke durch die Nummer ihrer oberen linken Ecke codiert hatten. Diese Codierung wollen wir wieder rückgängig machen und im zweiten Schritt die u_i durch die entsprechenden $(\frac{p-1}{2} \times \frac{p-1}{2})-$Blöcke ersetzen. Diese Blöcke sind nicht im eigentlichen Sinn symmetrisch, aber symmetrisch bezüglich der Gegendiagonalen. Diese Symmetrie verhindert eine vernüftige Diagonalisierung, so daß wir die Blöcke zunächst mit folgender $(\frac{p-1}{2} \times \frac{p-1}{2})-$ Matrix $Q_{\frac{p-1}{2}}$ mit Determinante $\det(Q_{\frac{p-1}{2}}) = -1$ multiplizieren, die die Matrizen u_i um 90 Grad nach

links dreht:

$$Q_{\frac{p-1}{2}} := \begin{pmatrix} & & & & 1 \\ & 0 & & 1 & \\ & & \iddots & & \\ & 1 & & 0 & \\ 1 & & & & \end{pmatrix}.$$

Statt der u_i betrachten wir die jetzt so gedrehten Matrizen v_i:

$$v_i := Q_{\frac{p-1}{2}} u_i,$$

in denen die Bildungsgesetze nach rechts durchgeschoben werden:

$$v_0 = u_0,$$

$$v_1 = \begin{pmatrix} b_{\frac{p-1}{2}} & b_1 & \cdots & b_{\frac{p-1}{2}-2} & b_{\frac{p-1}{2}-1} \\ b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} & \cdots & b_{\frac{p-1}{2}-3} & b_{\frac{p-1}{2}-2} \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ b_1 & b_2 & \dots & b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} \end{pmatrix}$$

$$v_2 = \begin{pmatrix} b_1 & b_2 & \cdots & b_{\frac{p-1}{2}-1} & b_{\frac{p-1}{2}} \\ b_{\frac{p-1}{2}} & b_1 & \cdots & b_{\frac{p-1}{2}-2} & b_{\frac{p-1}{2}-3} \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ b_2 & b_3 & \dots & b_{\frac{p-1}{2}} & b_1 \end{pmatrix}$$

und so weiter.
Auch auf diese Matrizen wenden wir jetzt Lemma 6.4 an, indem wir $(\frac{p-1}{2})-$te Einheitswurzeln verwenden: Sei $\sigma = e^{\frac{2\pi i}{\frac{p-1}{2}}}$ eine $(\frac{p-1}{2})-$te primitive Einheitswurzel und wir zeigen:

6.7 Lemma: *Für* $1 \leq i \leq \frac{p-1}{2}$ *hat* $L(i) := T_{\frac{p-1}{2}} v_i T^{-1}_{\frac{p-1}{2}}$ *Diagonalgestalt mit:*

$$L(i)_{kk} = \sum_{n=0}^{\frac{p-1}{2}-1} f_i(g^n)\sigma^{kn}$$

für $0 \leq k \leq \frac{p-1}{2} - 1$.

Beweis:
Wir betrachten $G := \mathbb{F}_p^\star/\{\pm 1\} = \{g^0, g^1, \ldots, g^{\frac{p-1}{2}-1}\}$ mit zugehöriger Charaktergruppe $\widehat{G} = \{\lambda_0, \ldots, \lambda_{\frac{p-1}{2}-1}\}$ und $M = \{b_1, \ldots, b_{\frac{p-1}{2}}\}$ und definieren eine Abbildung:

$$\begin{array}{rccl} f_1: & G & \longrightarrow & M \\ & g^n & \longmapsto & \begin{cases} b_{\frac{p-1}{2}} & \text{für } n = 0 \\ b_n & \text{sonst} \end{cases} \end{array} .$$

Damit erhalten wir:

$$v_1 = f_1(g^n g^{-m})_{0 \le n,m \le \frac{p-1}{2}-1}.$$

Die für $2 \le i \le \frac{p-1}{2}$ zu konstruierenden Abbildungen führen wir auf f_1 zurück, indem wir folgende Abbildungen definieren:

$$\begin{array}{rccl} f_i: & G & \longrightarrow & M \\ & g^n & \longmapsto & f_1(g^{n+i-1}) \end{array}$$

und erhalten:

$$v_i = f_i(g^n g^{-m})_{0 \le n,m \le \frac{p-1}{2}-1}.$$

Wir wenden jetzt Lemma 6.4 an:

$$L(i)_{m,n} = 0 \text{ für alle } 0 \le m, n \le \frac{p-1}{2} - 1 \text{ mit } m \ne n$$

und erhalten für $0 \le k \le \frac{p-1}{2} - 1$:

$$\begin{aligned} L(i)_{kk} &= \sum_{n=0}^{\frac{p-1}{2}-1} f_i(g^n)\lambda_k(g^n) \\ &= \sum_{n=0}^{\frac{p-1}{2}-1} f_i(g^n)\sigma^{kn} \text{ wegen } \lambda_k(g^n) = \sigma^{kn} \end{aligned}$$

□

6.8 Bemerkung: *Wir fassen die Gruppe* $G := \mathbb{F}_p^\star/\{\pm 1\}$ *als* $G = \{g^0, \ldots, g^{\frac{p-1}{2}-1}\}$ *mit zugehöriger Charaktergruppe* $\widehat{G} = \{\lambda_0, \ldots, \lambda_{\frac{p-1}{2}-1}\}$ *und schreiben daher die* $(\frac{p-1}{2} \times \frac{p-1}{2})-$*Matrix* $L(i)$ *als:*

$$L(i) = (L(i)_{nm})_{0 \le n,m \le \frac{p-1}{2}-1}\,.$$

Den Fall v_0 betrachten wir gesondert:

6.9 Lemma: $L(0) := T_{\frac{p-1}{2}} v_0 T^{-1}_{\frac{p-1}{2}}$ *hat Diagonalgestalt mit:*

$$L(0)_{00} = \tfrac{p-1}{2} b_0 \quad \textit{und} \quad L(0)_{kk} = 0$$

für $1 \leq k \leq \frac{p-1}{2} - 1$.

Beweis:
Wir betrachten wie in Lemma 6.7 $G := \mathbb{F}_p^\star/\{\pm 1\} = \{g^0, g^1, \ldots, g^{\frac{p-1}{2}}\}$ mit zugehöriger Charaktergruppe $\widehat{G} = \{\lambda_0, \ldots, \lambda_{\frac{p-1}{2}-1}\}$ und $M = \{b_1, \ldots, b_{\frac{p-1}{2}}\}$ und definieren die Abbildung:

$$\begin{array}{rccc} f_0: & G & \longrightarrow & M \\ & g^n & \longmapsto & b_0. \end{array}$$

Damit erhalten wir:

$$v_0 = f_0(g^n g^{-m})_{0 \leq n,m \leq \frac{p-1}{2}-1}.$$

Wir wenden jetzt wieder Lemma 6.4 an:

$$L(0)_{m,n} = 0 \text{ für alle } 0 \leq m, n \leq \frac{p-1}{2} - 1 \text{ mit } m \neq n$$

und für $0 \leq k \leq \frac{p-1}{2} - 1$:

$$\begin{array}{rcccl} L(0)_{kk} & = & \sum_{n=0}^{\frac{p-1}{2}-1} f_0(g_n)\lambda_k(g_n) & = & \sum_{n=0}^{\frac{p-1}{2}-1} f_0(g_n)\sigma^{kn} \quad \text{wegen } \lambda_k(g^n) = \sigma^{kn} \\ & = & \sum_{n=0}^{\frac{p-1}{2}-1} b_0 \sigma^{kn} & = & b_0 \sum_{n=0}^{\frac{p-1}{2}-1} (\sigma^k)^n = \begin{cases} \frac{p-1}{2} b_0 & \text{für } k = 0 \\ 0 & \text{sonst} \end{cases} \end{array}$$

□

Wir haben jetzt für $0 \leq i \leq \frac{p-1}{2}$ jeden Block u_i durch Multiplikation mit $Q_{\frac{p-1}{2}}$ zu $L(i)$ transformiert und in den vorherigen beiden Lemmata unitäre Äquivalenz zu einer Diagonalmatrix gezeigt. Um dies in unserer zu diagonalisierenden Matrix der Bildungsgesetze verwenden zu können, benötigen wir einen Operator, der uns die dabei verwendeten Matrizen entsprechend vergrößert:

6.10 Definition:

$$\begin{array}{rccc} \hat{M}_n: & \mathbb{C}^\star & \longrightarrow & M(\mathbb{C}, n) \\ & z & \longmapsto & zE_n \end{array}$$

weisst einer komplexen Zahl z eine $n \times n-$*Matrix mit z auf der Hauptdiagonalen zu.*

Wir wenden diesen Operator für $n = \frac{p-1}{2}$ auf die Einträge unserer Matrix:

$$A := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & & & \\ \vdots & & T_p & \\ 0 & & & \end{pmatrix}$$

an, so daß wir jedem Eintrag eine $(\frac{p-1}{2} \times \frac{p-1}{2})-$Matrix zuordnen, und definieren dies als:

$$\hat{M}_{\frac{p-1}{2}}(A).$$

6.11 Definition: *Statt der Matrix B der Bildungsgesetze von $\Gamma(p)$ betrachten wir:*

$$C := \hat{M}_{\frac{p-1}{2}}(A)\ \tilde{T}\ \tilde{Q}\ B\ \tilde{T}^{-1}\ \hat{M}_{\frac{p-1}{2}}(A^{-1})$$

mit den $((p+1)\frac{p-1}{2} \times (p+1)\frac{p-1}{2})-$Matrizen:

$$\tilde{T} := \begin{pmatrix} T_{\frac{p-1}{2}} & & 0 & \\ & T_{\frac{p-1}{2}} & & \\ & & \ddots & \\ & 0 & & T_{\frac{p-1}{2}} \end{pmatrix}$$

und:

$$\tilde{Q} := \begin{pmatrix} Q_{\frac{p-1}{2}} & & 0 & \\ & Q_{\frac{p-1}{2}} & & \\ & & \ddots & \\ & 0 & & Q_{\frac{p-1}{2}} \end{pmatrix}$$

Unsere bisherigen Überlegungen führen zu folgender Darstellung dieser Matrix:

$$C = \begin{pmatrix} L(0)+pL(1) & (1-p)L(1)+\sum_{i=1}^{\frac{p-1}{2}} L(i) & & & & \\ pL(1) & L(0)-pL(1)+\sum_{i=1}^{\frac{p-1}{2}} L(i) & & 0 & & \\ & & C(1) & & & \\ & & & C(2) & & \\ & 0 & & & \ddots & \\ & & & & & C(p-1) \end{pmatrix}$$

mit:

$$C(k) := L(0) + \sum_{i=1}^{\frac{p-1}{2}} L(i)(\omega^{ki} + \omega^{-ki})$$

für $1 \leq k \leq p-1$, wobei die $L(i)$ für $1 \leq k \leq \frac{p-1}{2}$ nach Lemma 6.7 folgende Diagonalgestalt haben:

$$L(i) = \begin{pmatrix} \ddots & & 0 \\ & L(i)_{jj} & \\ 0 & & \ddots \end{pmatrix}$$

mit:

$$L(i)_{jj} = \sum_{n=0}^{\frac{p-1}{2}-1} f_i(g^n)\sigma^{jn}$$

für $0 \leq j \leq \frac{p-1}{2} - 1$ und:

$$L(0)_{00} = \tfrac{p-1}{2} b_0 \quad \text{und} \quad L(0)_{ll} = 0$$

für $1 \leq l \leq \frac{p-1}{2} - 1$. Damit sind die $C(k)$ also diagonale $(\frac{p-1}{2} \times \frac{p-1}{2})-$Matrizen und wir untersuchen jetzt $C(k)_{jj}$ für $1 \leq k \leq p-1$ und $0 \leq j \leq \frac{p-1}{2} - 1$ genauer:

$$\begin{aligned}
C(k)_{11} &= L(0)_{11} + \sum_{i=1}^{\frac{p-1}{2}} L(i)_{11}(\omega^{ki} + \omega^{-ki}) \\
&= \frac{p-1}{2} b_0 + \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})(\sum_{n=0}^{\frac{p-1}{2}-1} f_i(g^n)) \\
&= \frac{p-1}{2} b_0 + \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})(\sum_{n=1}^{\frac{p-1}{2}} b_i) \\
&= \frac{p-1}{2} b_0 + \sum_{n=1}^{\frac{p-1}{2}} b_i (\sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki}) \\
&= \frac{p-1}{2} b_0 - \sum_{n=1}^{\frac{p-1}{2}} b_i
\end{aligned}$$

und:

$$\begin{aligned}
C(k)_{22} &= L(0)_{22} + \sum_{i=1}^{\frac{p-1}{2}} L(i)_{22}(\omega^{ki} + \omega^{-ki}) \\
&= 0 + \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})(\sum_{n=0}^{\frac{p-1}{2}-1} f_i(g^n))\sigma^{2n} \\
&= \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})(\sum_{n=0}^{\frac{p-1}{2}-1} f_1(g^{n+i-1}))\sigma^{2n}) \\
&= \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})(\sum_{n=0}^{\frac{p-1}{2}-1} b_{n+i-1 \bmod \frac{p-1}{2}} \sigma^{2n})
\end{aligned}$$

Wir wählen als Repräsentantensystem modulo $\frac{p-1}{2}$ die Menge $\{1,\ldots,\frac{p-1}{2}\}$, da $f_i(g^n) \in \{b_1,\ldots,b_{\frac{p-1}{2}}\}$.
Die letzte Summe enthält alle Bildungsgesetze $b_1,\ldots,b_{\frac{p-1}{2}}$ und wir sortieren diese Summe entsprechend um: Der Koeffizient von b_1 enthält alle Summanden mit $n+i-1 \equiv 1 \bmod \frac{p-1}{2}$, also mit $n \equiv 2-i \bmod \frac{p-1}{2}$:

$$c(k,2)_1 := \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki}) \sigma^{2(2-i)}.$$

Allgemein enthält der Koeffizient von b_j alle Summanden mit:

$$n+i-1 \equiv j \bmod \frac{p-1}{2}, \quad \text{also mit} \quad n \equiv j-i+1 \bmod \frac{p-1}{2},$$

so daß sich die Gesamtdarstellung folgendermassen vereinfachen läßt:

$$C(k)_{22} = \sum_{n=1}^{\frac{p-1}{2}} c(k,2)_n b_n$$

mit:

$$c(k,2)_n = \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki}) \sigma^{2(n+1-i)}.$$

Wir können aus jedem Koeffizienten $c(k,2)_1$ ausklammern:

$$\begin{aligned} c(k,2)_n &= \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki}) \sigma^{2(n+1-i)} \\ &= \sigma^{2(j-1)} \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki}) \sigma^{2(2-i)} \\ &= \sigma^{2(j-1)} c(k,2)_1 \end{aligned}$$

Damit haben wir folgendes Lemma gezeigt:

6.12 Lemma: *Für $1 \le k \le p-1$ und $1 \le j \le \frac{p-1}{2}-1$ gilt:*

$$C(k)_{jj} = \sum_{n=1}^{\frac{p-1}{2}} c(k,j)_n b_n$$

mit:

$$c(k,j)_n = c(k,j)_1 \chi_j(n-1)$$

für $2 \leq n \leq \frac{p-1}{2}$ *und* $c(k,j)_1 = \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})\sigma^{j(2-i)}$. *Für den ersten Diagonaleintrag gilt:*

$$C(k)_{00} \quad = \quad \frac{p-1}{2} b_0 - \sum_{n=1}^{\frac{p-1}{2}} c(k,0)_n b_n = \frac{p-1}{2} b_0 - \sum_{n=1}^{\frac{p-1}{2}} b_n$$

mit:

$$c(k,0)_n = \chi_0(n-1)$$

für $2 \leq n \leq \frac{p-1}{2}$ *mit dem trivialen Charakter* χ_0 *und* $c(k,0)_1 = 1$.

Mit diesem Lemma verstehen wir alle Einträge auf der Diagonalen von C außerhalb des $(p+1) \times (p+1)-$Blockes oben links:

$$\widetilde{K} := \begin{pmatrix} L(0) + pL(1) & (1-p)L(1) + \sum_{i=1}^{\frac{p-1}{2}} L(i) \\ pL(1) & L(0) - pL(1) + \sum_{i=1}^{\frac{p-1}{2}} L(i) \end{pmatrix}$$

Um die Determinante dieser Teilmatrix zu bestimmen, addieren wir zunächst das $(-1)-$fache der ersten $\frac{p-1}{2}$ Zeilen zu den $\frac{p-1}{2}$ zweiten Zeilen, ohne dabei den Wert der Determinante zu ändern:

$$K := \begin{pmatrix} L(0) + pL(1) & (1-p)L(1) + \sum_{i=1}^{\frac{p-1}{2}} L(i) \\ -L(0) & L(0) - L(1) \end{pmatrix} =: \begin{pmatrix} K(1,1) & K(1,2) \\ K(2,1) & K(2,2) \end{pmatrix}$$

Jeder der $(\frac{p-1}{2}) \times (\frac{p-1}{2})-$Blöcke hat nach den bisherigen Überlegungen Diagonalgestalt und wir nummerieren wieder ausgehend von 0:

$$K(1,1) := (K(1,1)_{ij})_{0 \leq i,j \leq \frac{p-1}{2}-1}$$

und analog für die anderen Blöcke. Darüberhinaus hat $L(0)$ nur in der oberen linken Ecke einen Eintrag ungleich Null, so daß sich für die Determinante eine Laplace-Entwicklung nach der $(\frac{p-1}{2}+1)-$ten Zeile anbietet mit nur zwei Summanden ungleich Null.

$$\det K = (-1)^{2+\frac{p-1}{2}} K(2,1)_{00} \det \begin{pmatrix} K(1,1)_{11} & & & & & & \\ & \ddots & & & \star & & \\ & & K(1,1)_{\frac{p-1}{2}\frac{p-1}{2}} & & & & \\ & & & 0 & & & \\ & & & & K(2,2)_{11} & & \\ & 0 & & & \ddots & & \\ & & & & & & K(2,2)_{\frac{p-1}{2}\frac{p-1}{2}} \end{pmatrix}$$

$$+(-1)^{2(\frac{p-1}{2}+1)}K(2,2)_{00}\det\begin{pmatrix} K(1,1)_{00} & & & \star & & \\ & \ddots & & & & \\ & & K(1,1)_{\frac{p-1}{2}\frac{p-1}{2}} & & & \\ & & & K(2,2)_{11} & & \\ & 0 & & & \ddots & \\ & & & & & K(2,2)_{\frac{p-1}{2}\frac{p-1}{2}} \end{pmatrix}$$

Wegen der Null auf der Hauptdiagonalen des ersten Summanden benötigen wir für die Determinante nur den zweiten Summanden. Wir bestimmen zunächst die Einträge $K(1,1)_{00},\ldots,K(1,1)_{\frac{p-1}{2}\frac{p-1}{2}}$, $K(2,2)_{11},\ldots,K(2,2)_{\frac{p-1}{2}\frac{p-1}{2}}$ und den Koeffizienten $K(2,2)_{00}$. Mit:

$$\begin{aligned} L(1)_{jj} &= \sum_{n=0}^{\frac{p-1}{2}-1} f_1(g^n)\sigma^{jn} \\ &= \sum_{n=0}^{\frac{p-1}{2}-1} b_{n+1-1 \bmod \frac{p-1}{2}}\sigma^{jn} \\ &= \sum_{n=1}^{\frac{p-1}{2}} \sigma^{jn} b_n \end{aligned}$$

für $0 \leq j \leq \frac{p-1}{2}-1$ und:

$$L(0)_{00} = \tfrac{p-1}{2}b_0 \quad \text{und} \quad L(0)_{ll} = 0$$

erhalten wir:

$$\begin{aligned} K(1,1)_{00} &= \frac{p-1}{2}b_0 + p\sum_{n=1}^{\frac{p-1}{2}} b_n \\ K(1,1)_{11} &= p\sum_{n=1}^{\frac{p-1}{2}} \sigma^n b_n \\ &\vdots \\ K(1,1)_{\frac{p-1}{2}\frac{p-1}{2}} &= p\sum_{n=1}^{\frac{p-1}{2}} \sigma^{(\frac{p-1}{2}-1)n} b_n \end{aligned}$$

$$\begin{aligned} K(2,2)_{11} &= -\sum_{n=1}^{\frac{p-1}{2}} \sigma^n b_n \\ &\vdots \\ K(2,2)_{\frac{p-1}{2}\frac{p-1}{2}} &= -\sum_{n=1}^{\frac{p-1}{2}} \sigma^{(\frac{p-1}{2}-1)n} b_n \end{aligned}$$

und:

$$K(2,2)_{00} = \frac{p-1}{2} b_0 - \sum_{n=1}^{\frac{p-1}{2}} b_n.$$

Jetzt haben wir für die Matrix der Bildungsgesetze eine Form bestimmt, aus der wir die Determinante bestimmen können.

6.3 Reihendarstellungen

Zu den im vorherigen Abschnitt bestimmten Einträgen der Matrix der Bildungsgesetze entwickeln wir jetzt die entsprechenden Reihen. Dazu sind zunächst einige Vorüberlegungen erforderlich: Sei $\tilde{\chi}_j$ ein nichttrivialer Charakter der Charaktergruppe von $\mathbb{F}_p^\star/\{\pm 1\}$. Wir führen zu $\tilde{\chi}_j$ für $s \in \mathbb{H}$ mit $\operatorname{Re} s > 1$ folgende L-Reihen ein:

$$D_{\tilde{\chi}_j}(s) := \sum_{c=1}^{\infty} \sum_{i \in \mathbb{F}_p^\star/\{\pm 1\}} \frac{\tilde{\chi}_j(i) b_i(c)}{c^{2s}}.$$

Da für jedes $b_i(c) = \varphi(c)$ für $c \equiv \pm i(p)$ und $b_i(c) = 0$ sonst gilt, lassen sich diese L-Reihen sofort umformulieren zu:

$$D_{\tilde{\chi}_j}(s) = \sum_{c=1}^{\infty} \frac{\tilde{\chi}_j(c)\varphi(c)}{c^{2s}}.$$

Wir zeigen jetzt, wie sich diese L-Reihen mit ähnlichen Überlegungen wie im letzten Abschnitt von Kapitel 2 in die normalen *Dirichlet-L*-Reihen:

$$L_{\tilde{\chi}_j}(s) := \sum_{c=1}^{\infty} \frac{\tilde{\chi}_j(c)}{c^s},$$

umformen lassen, für die eine zur Zetafunktion analoge Euleridentität für $s \in \mathbb{H}$ mit $\operatorname{Re} s > 1$ gilt:

$$L_{\tilde{\chi}_j}(s) = \prod_{q \ prim} \frac{1}{1 - \tilde{\chi}_j(q) q^{-s}}$$

und die sich analog auf ganz $\mathbb{C}$ fortsetzen lassen [IR90].

6.13 Satz: *Sei $\tilde{\chi}_j$ ein nichttrivialer Charakter der Charaktergruppe von $\mathbb{F}_p^\star/\{\pm 1\}$ und $s \in \mathbb{H}$ mit $\operatorname{Re} s > 1$. Dann gilt:*

$$D_{\tilde{\chi}_j}(s) = \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)}$$

Beweis:

$$D_{\tilde{\chi}_j}(s) = \sum_{c=1}^{\infty} \frac{\tilde{\chi}_j(c)\varphi(c)}{c^{2s}} = \prod_{q \ prim} (1 + \frac{\tilde{\chi}_j(q)\varphi(q)}{q^{2s}} + \frac{\tilde{\chi}_j(q^2)\varphi(q^2)}{q^{4s}} + \ldots)$$

Mit $\Lambda_{\tilde{\chi}_j,q}(s) := \sum_{k=0}^{\infty} \frac{\tilde{\chi}_j(q^k)\varphi(q^k)}{q^{2ks}} \sum_{k=0}^{\infty} \frac{\tilde{\chi}_j(q)^k\varphi(q^k)}{q^{2ks}}$ folgt:

$$\sum_{c=1}^{\infty} \frac{\tilde{\chi}_j(c)\varphi(c)}{c^{2s}} = \prod_{q \ prim} \Lambda_{\tilde{\chi}_j,q}(s).$$

Nach Lemma 2.23 gilt $\Theta_q(T) := \sum_{k=0}^{\infty} \varphi(q^k)T^k = \frac{1-T}{1-qT}$ für $|qT| < 1$.
Für $T = \tilde{\chi}_j(q)q^{-2s}$ folgt $|\frac{q\tilde{\chi}_j(q)}{q^{2s}}| < 1$, da $s > 1$, und wir können Lemma 2.23 anwenden:

$$\Lambda_q(s) = \Theta_q(\tilde{\chi}_j(q)q^{-2s}) = \frac{1 - \tilde{\chi}_j(q)q^{-2s}}{1 - \tilde{\chi}_j(q)q^{1-2s}}$$

und insgesamt:

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{\tilde{\chi}_j(c)\varphi(c)}{c^{2s}} &= \prod_{q \ prim} \frac{1 - \tilde{\chi}_j(c)q^{-2s}}{1 - \tilde{\chi}_j(c)q^{1-2s}} \\
&= \prod_{q \ prim} \frac{1}{1 - \tilde{\chi}_j(c)q^{1-2s}} \prod_{q \ prim} (1 - \tilde{\chi}_j(c)q^{-2s}) \\
&= \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)}
\end{aligned}$$

□

Wir erweitern diese Überlegungen auf den trivialen Charakter, für den wir wegen der verschiedenen Bildungsgesetze zwei Reihendarstellungen definieren:

6.14 Satz: *Sei $\tilde{\chi}_0$ der trivialer Charakter der Charaktergruppe von $\mathbb{F}_p^\star/\{\pm 1\}$ und $s \in \mathbb{H}$ mit $\operatorname{Re} s > 1$. Dann gilt:*

$$D(0)_{\tilde{\chi}_0}(s) := \sum_{c=1, c\equiv 0(p)}^{\infty} \frac{b_0(c)}{c^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)} \frac{2p}{p^{2s}-1}.$$

Beweis:

$$\begin{aligned} D(0)_{\tilde{\chi}_0}(s) &= \sum_{c=1, c\equiv 0(p)}^{\infty} \frac{b_0(c)}{c^{2s}} \\ &= \sum_{c=1, c\equiv 0(p)}^{\infty} \frac{\frac{2p}{p-1}\varphi(c)}{c^{2s}} \\ &= \frac{2p}{p-1} Z_{11}(s) \qquad \text{nach Satz 2.25} \\ &= \frac{2p}{p-1} \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p-1}{p^{2s}-1} \end{aligned}$$

□

6.15 Satz: *Sei $\tilde{\chi}_0$ der trivialer Charakter der Charaktergruppe von $\mathbb{F}_p^\star/\{\pm 1\}$ und $s \in \mathbb{H}$ mit $\operatorname{Re} s > 1$. Dann gilt:*

$$D(1)_{\tilde{\chi}_0}(s) := \sum_{c=1, c\not\equiv 0(p)}^{\infty} \frac{\varphi(c)}{c^{2s}} = \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^{2s}-p}{p^{2s}-1}.$$

Beweis:

$$\begin{aligned} D(1)_{\tilde{\chi}_0}(s) &= \sum_{c=1, c\not\equiv 0(p)}^{\infty} \frac{\varphi(c)}{c^{2s}} \\ &= Z_{12} \qquad \text{nach Satz 2.24} \\ &= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^{2s}-p}{p^{2s}-1} \end{aligned}$$

□

Damit können wir aus jedem Eintrag der umgeformten Matrix der Bildungsgesetze:

$$C = \begin{pmatrix} K & & & & \\ & C(1) & & & \\ & & C(2) & & \\ & 0 & & \ddots & \\ & & & & C(p-1) \end{pmatrix}$$

die entspechenden Reihen entwickeln:

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{C(k)_{00}(c)}{c^{2s}} &= c(k,0)_1 \sum_{c=1}^{\infty} (\frac{\frac{p-1}{2} b_0(c)}{c^{2s}} - \sum_{n=1}^{\frac{p-1}{2}} \frac{b_n(c)}{c^{2s}}) \\
&= c(k,0)_1 (\frac{p-1}{2} D(0)_{\tilde{\chi}_0}(s) - D(1)_{\tilde{\chi}_0}(s)) \\
&= c(k,0)_1 \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^2 - p^{2s}}{p^{2s}-1}
\end{aligned}$$

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{C(k)_{jj}(c)}{c^{2s}} &= c(k,j)_1 \sum_{c=1}^{\infty} \sum_{n=1}^{\frac{p-1}{2}} \frac{\chi_j(n-1) b_n(c)}{c^{2s}} \\
&= c(k,j)_1 \sum_{c=1}^{\infty} \sum_{n=1}^{\frac{p-1}{2}} \frac{\tilde{\chi}_j(n) b_n(c)}{c^{2s}} \\
&= c(k,j)_1 D_{\tilde{\chi}_j}(s) \\
&= c(k,j)_1 \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)}
\end{aligned}$$

für $1 \leq k \leq p-1$ und:

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{K(1,1)_{00}(c)}{c^{2s}} &= \frac{p-1}{2} D(0)_{\tilde{\chi}_0}(s) + p D(1)_{\tilde{\chi}_0}(s) \\
&= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^{2s+1} - 2p + p^2}{p^{2s}-1}
\end{aligned}$$

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{K(1,1)_{jj}(c)}{c^{2s}} &= p D_{\tilde{\chi}_j}(s) \\
&= p \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)}
\end{aligned}$$

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{K(2,2)_{00}(c)}{c^{2s}} &= \frac{p-1}{2} D(0)_{\tilde{\chi}_0}(s) + p D(1)_{\tilde{\chi}_0}(s) \\
&= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^{2s+1} - 2p + p^2}{p^{2s}-1}
\end{aligned}$$

$$\begin{aligned}
\sum_{c=1}^{\infty} \frac{K(2,2)_{jj}(c)}{c^{2s}} &= \frac{p-1}{2} D(0)_{\tilde{\chi}_0}(s) - D(1)_{\tilde{\chi}_0}(s) \\
&= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^2 - p^{2s}}{p^{2s}-1}
\end{aligned}$$

Die Determinante der Reihendarstellung unserer umgeformten Matrix C ergibt sich jetzt als Produkt der oben aufgeführten Faktoren, die wir der Übersicht wegen wie folgt zusammenfassen:

$$
\begin{aligned}
F_0 &:= \prod_{k=1}^{p-1} \sum_{c=1}^{\infty} \frac{C(k)_{00}(c)}{c^{2s}} \\
&= \left(\prod_{k=1}^{p-1} c(k,0)_1 \right) \left(\frac{\zeta(2s-1)}{\zeta(2s)} \right)^{p-1} \left(\frac{p^2-p^{2s}}{p^{2s}-1} \right)^{p-1} \\
&= \left(\frac{\zeta(2s-1)}{\zeta(2s)} \right)^{p-1} \left(\frac{p^2-p^{2s}}{p^{2s}-1} \right)^{p-1} \qquad \text{wegen } \prod_{k=1}^{p-1} c(k,0)_1 = 1 \\
F_1 &:= \prod_{k=1}^{p-1} \prod_{j=1}^{\frac{p-1}{2}-1} \sum_{c=1}^{\infty} \frac{C(k)_{jj}(c)}{c^{2s}} \\
&= \left(\prod_{k=1}^{p-1} \prod_{j=1}^{\frac{p-1}{2}-1} c(k,j)_1 \right) \left(\prod_{\tilde{\chi}_j} \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)} \right)^{p-1} \\
F_2 &:= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^{2s+1}-2p+p^2}{p^{2s}-1} \\
F_3 &:= \prod_{j=1}^{\frac{p-1}{2}-1} \sum_{c=1}^{\infty} \frac{K(1,1))_{jj}(c)}{c^{2s}} \\
&= p^{\frac{p-1}{2}-1} \prod_{\tilde{\chi}_j} \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)} \\
F_4 &:= (-1)^{\frac{p-1}{2}-1} \prod_{\tilde{\chi}_j} \frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)} \\
F_5 &:= \sum_{c=1}^{\infty} \frac{K(2,2)_{00}(c)}{c^{2s}} \\
&= \frac{\zeta(2s-1)}{\zeta(2s)} \frac{p^2-p^{2s}}{p^{2s}-1}
\end{aligned}
$$

Für die Determinante der Streumatrix von $\Gamma(p)$ fehlen noch die Determinanten der Matrizen, die wir beim Umformen benutzt haben.
Wegen:

$$C := \hat{M}_{\frac{p-1}{2}}(A)\ \tilde{T}\ \widetilde{Q}\ B\ \tilde{T}^{-1}\ \hat{M}_{\frac{p-1}{2}}(A^{-1})$$

nach Definition 6.11 ergibt sich mit:

$$\det \widetilde{Q} = \left(\det Q_{\frac{p-1}{2}}\right)^{p+1} = (-1)^{p+1} = 1$$

für die Determinante der Sterumatrix insgesamt folgender Satz:

6.16 Satz: *Die Determinante der Streumatrix von $\Gamma(p)$ hat die Gestalt:*

$$\begin{aligned}\det(\Phi(\Gamma(p),s)) &= YF_0F_1F_2F_3F_4F_5 \\ &= XYZ\left(\frac{\zeta(2s-1)}{\zeta(2s)}\right)^{p+1}\left(\prod_{\tilde{\chi}_j}\frac{L_{\tilde{\chi}_j}(2s-1)}{L_{\tilde{\chi}_j}(2s)}\right)^{p+1}\end{aligned}$$

Mit

$$X := \left(\prod_{k=1}^{p}\prod_{\tilde{\chi}_j} c(k,j)_1\right) p^{\frac{p-1}{2}-1}$$

und:

$$Y := \left(\pi^{\frac{1}{2}}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\right)^{(p+1)\frac{p-1}{2}}$$

und:

$$Z := \left(\frac{p^2-p^{2s}}{p^{2s}-1}\right)^{p-1}\left(\frac{p^{2s+1}-2p+p^2}{p^{2s}-1}\right)^2.$$

Jetzt untersuchen wir den Koeffizienten X näher, in dem wir in obiger Darstellung alle Faktoren aus F_0, F_1, F_2, F_3, F_4 und F_5 zusammengefasst haben, die aus $c(k,j)_1$ für $1 \le k \le p-1$ und $1 \le j \le \frac{p-1}{2} - 1$ bestehen. Umformen der Definition von $c(k,j)_1$ liefert:

$$\begin{aligned}c(k,j)_1 &= \sum_{i=1}^{\frac{p-1}{2}}(\omega^{ki}+\omega^{-ki})\sigma^{j(2-i)} \\ &= \sigma^{2j}\sum_{i=1}^{p-1}\omega^{ki}\sigma^{-ji} \\ &= \sigma^{2j}\sum_{i=1}^{p-1}\omega^{ki}\tilde{\chi}_{-j}(i),\end{aligned}$$

wobei $\tilde{\chi}_j$ ein Charakter aus $\widehat{\mathbb{F}}_p^\star/\{\pm 1\}$ ist. Dies führt uns auf *Gauss-Summen* [IR90]:

6.17 Definition: *Sei χ_j ein Charakter aus $\widehat{\mathbb{F}}_p$, $\omega = e^{\frac{2\pi i}{p}}$ und $j \in \mathbb{F}_p$. Dann heisst:*

$$g_j(\chi_j) := \sum_{i=1}^{p-1} \chi_j(i)\omega^{ji}$$

die Gauss-Summe von $\mathbb{F}_p$ zum Charakter χ_j.

Für $j \neq 0$ und χ nicht der triviale Charakter von $\mathbb{F}_p$ gilt:

$$g_j(\chi) = \chi(j^{-1})g_1(\chi)$$

und bezüglich komplexer Konjugation bestehen folgende Zusammenhänge [IR90]:

$$\overline{g_j(\chi)} = \chi(-1)g_j(\overline{\chi})$$

und:

$$\overline{g_1(\chi)}g_1(\chi) = p.$$

Damit vereinfacht sich unsere Darstellung:

$$c(k,j)_1 \;=\; \sigma^{2j} g_k(\chi_{-j})$$

und wir erhalten für X:

$$\begin{aligned}
X &= \prod_{k=1}^{p} \prod_{j=1}^{\frac{p-1}{2}-1} \sigma^{2j} \sum_{i=1}^{\frac{p-1}{2}} (\omega^{ki} + \omega^{-ki})\sigma^{-ji} \\
&= \prod_{k=1}^{p} \prod_{j=1}^{\frac{p-1}{2}-1} \sigma^{2j} g_k(\chi_{-j}) \\
&= \prod_{k=1}^{p} \prod_{j=1}^{\frac{p-1}{2}-1} g_k(\chi_{-j}) \\
&= \prod_{k=1}^{p} \prod_{j=1}^{\frac{p-1}{2}-1} g_1(\chi_{-j})\chi_{-j}(k^{-1}) \\
&= \left(\prod_{k=1}^{p} \prod_{j=1}^{\frac{p-1}{2}-1} \chi_{-j}(k^{-1}) \right) \left(\prod_{j=1}^{\frac{p-1}{2}-1} g_1(\chi_{-j}) \right)^{p-1}
\end{aligned}$$

$$= \left(\prod_{j=1}^{\frac{p-1}{2}-1} g_1(\chi_{-j}) \right)^{p-1}$$
$$= \left(\prod_{\tilde{\chi} \in V} g_1(\tilde{\chi}) \right)^{p-1},$$

wobei das Produkt über alle Charaktere $\tilde{\chi}$ von $\mathbb{F}_p^\star/\{\pm 1\}$ ohne den trivialen Charakter läuft:

$$V := \{\tilde{\chi} \in \widehat{\mathbb{F}}_p^\star/\{\pm 1\} : \tilde{\chi} \neq \chi_0\}.$$

Auf V operiert die komplexe Konjugation, kann dort aber Fixpunkte haben. Wir zerlegen V daher als:

$$V := V_0 \cup V_1$$

mit:

$$V_0 := \{\chi \in \widehat{\mathbb{F}}_p^\star/\{\pm 1\} : \overline{\chi} = \chi\}$$

und:

$$V_1 := \{\chi \in \widehat{\mathbb{F}}_p^\star/\{\pm 1\} : \overline{\chi} \neq \chi\}.$$

Dann läßt sich V_1 weiter zerlegen in $V_1 = W \cup \overline{W}$, wobei:

$$W := V_1/\sim$$

mit $\chi_i \sim \chi_j \Leftrightarrow \chi_i = \overline{\chi_j}$.

6.18 Lemma:

$$X = \begin{cases} \left(\sqrt{p}\, p^{\frac{p-5}{2}}\right)^{p-1} & \text{für } p \equiv 1 \bmod 4 \\ \left(p^{\frac{p-3}{2}}\right)^{p-1} & \text{für } p \equiv 3 \bmod 4 \end{cases}$$

Beweis:
Da in der Darstellung von X das Produkt über alle Charaktere $\tilde{\chi}$ von $\mathbb{F}_p^\star/\{\pm 1\}$ ohne den trivialen Charakter läuft, erhalten wir:

$$X = \left(\prod_{\tilde{\chi} \in V} g_1(\tilde{\chi}) \right)^{p-1}$$
$$= \left(\prod_{\chi \in V_0}^{\frac{p-1}{2}-1} g_1(\chi) \prod_{\chi \in W}^{\frac{p-1}{2}-1} g_1(\chi) \prod_{\chi \in \overline{W}}^{\frac{p-1}{2}-1} g_1(\chi) \right)^{p-1}$$

$$
\begin{aligned}
&= \left(\prod_{\chi \in V_0}^{\frac{p-1}{2}-1} g_1(\chi) \prod_{\chi \in W}^{\frac{p-1}{2}-1} g_1(\chi) \prod_{\chi \in W}^{\frac{p-1}{2}-1} g_1(\overline{\chi}) \right)^{p-1} \\
&= \left(\prod_{\chi \in V_0}^{\frac{p-1}{2}-1} g_1(\chi) \prod_{\chi \in W}^{\frac{p-1}{2}-1} g_1(\chi) \prod_{\chi \in W}^{\frac{p-1}{2}-1} \overline{g_1(\chi)} \right)^{p-1} \qquad \text{wegen } \chi(-1) = 1 \text{ in } \mathbb{F}_p^\star/\{\pm 1\} \\
&= \left(\sqrt{p}^{|V_0|} p^{\frac{|V_1|}{2}} \right)^{p-1}
\end{aligned}
$$

Dabei hängt die Anzahl der Fixpunkte unter der komplexen Konjugation von p ab: Ein Charakter $\tilde{\chi} \in V$ bleibt unter komplexer Konjugation fest, wenn $\tilde{\chi}(n) \in \mathbb{R}$ gilt, also:

$$\tilde{\chi}(n) = \pm 1 \quad \forall n \in \mathbb{F}_p^\star/\{\pm 1\}$$

Damit gibt es für $p \equiv 1 \bmod 4$ einen Fixpunkt und für $p \equiv 3 \bmod 4$ keinen. □

Insgesamt läßt sich Satz 6.16 vereinfachen zu:

6.19 Satz: *Die Determinante der Streumatrix von* $\Gamma(p)$ *hat die Gestalt:*

$$\det(\Phi(\Gamma(p), s))$$

$$= G(s) C \left(\frac{p^2 - p^{2s}}{p^{2s} - 1} \right)^{p-1} \left(\frac{p^{2s+1} - 2p + p^2}{p^{2s} - 1} \right)^2 \left(\frac{\zeta(2s-1)}{\zeta(2s)} \right)^{p+1} \left(\prod_{\chi_j \in V} \frac{L_{\chi_j}(2s-1)}{L_{\chi_j}(2s)} \right)^{p+1}$$

wobei das Produkt über alle Charaktere $\chi \in V := \{\chi \in \widehat{\mathbb{F}}_p^\star/\{\pm 1\} : \chi \neq \chi_0\}$ *läuft mit:*

$$G(s) := \left(\pi^{\frac{1}{2}} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \right)^{(p+1)\frac{p-1}{2}}$$

und:

$$C = \begin{cases} \left(\sqrt{p}\, p^{\frac{p-5}{2}} \right)^{p-1} & \text{für } p \equiv 1 \bmod 4 \\ \left(p^{\frac{p-3}{2}} \right)^{p-1} & \text{für } p \equiv 3 \bmod 4 \end{cases} .$$

6.20 Beispiel: Wir verdeutlichen unsere Ergebnisse am Beispiel von $\Gamma(7)$, weil dies die kleinste Primzahl ist, für die wir in der Matrix der Bildungsgesetze alle oben aufgeführten Strukturen zeigen können. Die 24×24 Matrix B mit den Nummern aller Bildungsgesetze haben wir bereits in Kapitel 4 als Beispiel

4.14 vorgestellt. Die verkürzte Matrix $\tilde{B}$, die jedem Block die Nummer des Bildungsgesetzes in der linken oberen Ecke zuordnet, hat folgende Gestalt:

$$\tilde{B} = \begin{pmatrix} u_0 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 \\ u_1 & u_0 & u_1 & u_2 & u_3 & u_3 & u_2 & u_1 \\ u_1 & u_1 & u_0 & u_1 & u_2 & u_3 & u_3 & u_2 \\ u_1 & u_2 & u_1 & u_0 & u_1 & u_2 & u_3 & u_3 \\ u_1 & u_3 & u_2 & u_1 & u_0 & u_1 & u_2 & u_3 \\ u_1 & u_3 & u_3 & u_2 & u_1 & u_0 & u_1 & u_2 \\ u_1 & u_2 & u_3 & u_3 & u_2 & u_1 & u_0 & u_1 \\ u_1 & u_1 & u_2 & u_3 & u_3 & u_2 & u_1 & u_0 \end{pmatrix}$$

In dieser codierten Form ergibt sich für die primitive 7.-te Einheitswurzel w die Matrix:

$$T = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & w & w^2 & w^3 & w^4 & w^5 & w^6 \\ 0 & 1 & w^2 & w^4 & w^6 & w^8 & w^{10} & w^{12} \\ 0 & 1 & w^3 & w^6 & w^9 & w^{12} & w^{15} & w^{18} \\ 0 & 1 & w^4 & w^8 & w^{12} & w^{16} & w^{20} & w^{24} \\ 0 & 1 & w^5 & w^{10} & w^{15} & w^{20} & w^{25} & w^{30} \\ 0 & 1 & w^6 & w^{12} & w^{18} & w^{24} & w^{30} & w^{36} \end{pmatrix},$$

deren Einträge sich natürlich offensichtlich vereinfachen lassen, hier aber wegen der allgemeinen Form so aufgeführt sind. $H = T_P V T_p^{-1}$ hat folgende Gestalt:

$$H = \begin{pmatrix} A & & & \\ & D_1 & 0 & \\ & & D_2 & \\ & 0 & \ddots & \\ & & & D_6 \end{pmatrix}$$

mit:

$$\begin{aligned} A &= \begin{matrix} u_0 + 7u_1 & -4u_1 + 2u_2 + 2u_3 \\ 7u_1 & u_0 - 5u_1 + 2u_2 + 2u_3 \end{matrix} \\ D_1 &= u_0 + (-\omega^5 - \omega^4 - \omega^3 - \omega^2 - 1)u_1 1 + (\omega^5 + \omega^2)u_2 + (\omega^4 + \omega^3)u_3 \\ D_2 &= a + (\omega^5 + \omega^2)u_1 + (\omega^4 + \omega^3)u_2 + (-\omega^5 - \omega^4 - \omega^3 - \omega^2 - 1)u_3 \\ D_3 &= u_0 + (\omega^4 + \omega^3)u_1 + (-\omega^5 - \omega^4 - \omega^3 - \omega^2 - 1)u_2 + (\omega^5 + \omega^2)u_3 \\ D_4 &= u_0 + (\omega^4 + \omega^3)u_1 + (-\omega^5 - \omega^4 - \omega^3 - \omega^2 - 1)u_2 + (\omega^5 + \omega^2)u_3 \\ D_5 &= u_0 + (\omega^5 + \omega^2)u_1 + (\omega^4 + \omega^3)u_2 + (-\omega^5 - \omega^4 - \omega^3 - \omega^2 - 1)u_3 \\ D_6 &= u_0 + (-\omega^5 - \omega^4 - \omega^3 - \omega^2 - 1)u_1 + (\omega^5 + \omega^2)u_2 + (\omega^4 + \omega^3)u_3 \end{aligned}$$

Rücksubstitution und Drehen der einzelnen Blöcke geschieht mit folgenden Matrizen, wobei $\sigma = e^{\frac{2\pi i}{3}}$:

$$\tilde{T} = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc|ccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \sigma & \sigma^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \sigma^2 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \sigma & \sigma^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \sigma^2 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma & \sigma^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma^2 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma & \sigma^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma^2 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma & \sigma^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma^2 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma & \sigma^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma^2 & \sigma & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma & \sigma^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma^2 & \sigma & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma & \sigma^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \sigma^2 & \sigma \end{array}\right)$$

und

$$\tilde{Q} = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc|ccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

Die Determinante der so transformierten Matrix der Bildungsgesetze von $\Gamma(7)$ läßt sich folgendermassen faktorisieren, wobei in Klammern die Vielfachheit angegeben ist:

$$\begin{array}{ll} b_1 + (-\omega^7 - 1)b_2 + \omega^7 b_3 & (8) \\ b_1 + \omega^7 b_2 + (-\omega^7 - 1)b_3 & (8) \\ b_0 - 1/3b_1 - 1/3b_2 - 1/3b_3 & (7) \\ b_0 + 7/3b_1 + 7/3b_2 + 7/3b_3 & (1) \end{array}$$

7 Beobachtungen und Ausblick

Im Rahmen dieser Arbeit wurde eine Datenbank angelegt mit den ersten 6.000 Untergruppen von Γ, geordnet nach aufsteigendem Index. Diese Datenbank wurde mit verschiedenen in GAP geschriebenen Programmen erzeugt und umfaßt Gruppen bis zum Index 19, von denen ungefähr zwanzig Prozent nur eine Spitze, knapp die Hälfte zwei Spitzen und dreissig Prozent drei Spitzen haben. Der weitaus größere Teil dieser Gruppen sind Nichtkongruenzuntergruppen:

Spitzen	Gruppen	davon Kongruenzgruppen	davon Nichtkongruenzgruppen
1	1150	30	1120
2	2627	35	2592
3	1780	9	1771
4	417	9	408
5	26	0	26
	6000	83	5917

Die Datenbank charakterisiert alle Gruppen durch ihre Erzeuger, gibt neben dem Spitzenvektor, dem Vektor der Spitzenbreiten und dem möglichen Level an, ob es sich um einen Kongruenzuntergruppe handelt, und enthält für viele Gruppen auch die ersten Einträge der Streumatrix.
Es gibt Untersuchungen über die Struktur der Untergruppen der Modulgruppe (vergleiche z.B. [Mil69],[Pet71] und [Iwa02]) und Abschätzungen darüber, wie viele Untergruppen zu einem vorgegebenen Index zu erwarten sind ([New77], [Atk78] oder [MSP05]). Darüberhinaus gibt es eine Datenbank von Cunnings und Pauli [CP03], die alle Untergruppen der Modulgruppe mit Geschlecht kleiner oder gleich 24 klassifiziert haben. Allgemein gibt es deutlichst mehr Nichtkongruenz- als Kongruenzguntergruppen, wobei es Abschätzungen für die Anzahl der Kongruenzgruppen mit bestimmtem Index [Pet74] oder Geschlecht [GLP04] gibt.
Für zykloide Gruppen mit nur einer Spitze der Breite $w \in \mathbb{N}$ läßt sich die Streumatrix mit Satz 3.8 sofort angeben, unabhängig davon, ob es sich um eine Kongruenzuntergruppe handelt oder nicht. Bei Gruppen mit mehr als einer Spitzenklasse müssen wir diese Fälle unterscheiden. Zusätzlich zu den Gruppen aus der Datenbank wurden andere Untergruppen der Modulgruppe untersucht, sobald es möglich war, ihre Erzeuger anzugeben. So lassen sich z.B. in MAGMA Erzeuger

für Hauptkongruenzuntergruppen, $\Gamma_0(n)$ und andere Klassen von Untergruppen bestimmen, so daß wir die im Anhang aufgeführten GAP-Programme auf diese Gruppen anwenden können.

7.1 Kongruenzuntergruppen

Für Kongruenzuntergruppen ist nach Satz 3.5 klar, daß es für alle Einträge der Streumatrix Bildungsgesetze gibt, die sich durch Aufsummieren der Bildungsgesetze der zugehörigen Hauptkongruenzgruppe ergeben. Die Bildungsgesetze lassen sich also durch Kongruenzen modulo dem Level der Kongruenzuntergruppe ausdrücken und sind Vielfache der Eulerschen $\varphi-$Funktion:

$$b_{ij}(c) = \begin{cases} k_0\varphi(c) & c \equiv 0(n) \\ k_1\varphi(c) & c \equiv \pm 1(n) \\ \dots & \\ k_r\varphi(c) & c \equiv \pm r(n). \end{cases}$$

Dabei können die k_i durchaus rational sein, dann kürzt sich der Nenner gegen $\varphi(c)$ weg, so daß das Ergebnis eine nichtnegative ganze Zahl ist. Für kleine Spitzenanzahlen haben wir experimentelle Belege dafür gefunden, daß sich dieses abstrakte Gesetz deutlich vereinfachen läßt:
Sei Δ eine Kongruenzuntergruppe mit genau zwei Spitzen, Spitzenvektor $S(\Delta) = [s_1 = \infty, s_2 = g_2\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, w_2]$ mit $w_1 > w_2$. Dann ist Δ eine Kongruenzuntergruppe vom Level w_1 und w_2 teilt w_1 nach Satz 1.14 und Satz 1.16. Bei einer Gruppe mit zwei Spitzen wird die Streumatrix durch ihren ersten Eintrag vollständig beschrieben, da sich aus $b_{11}(c)$ mit Theorem 2.13 der Koeffizient $b_{12}(c)$ ergibt als $b_{12}(c) = w_1\varphi(c) - b_{11}(c)$. Dann können auch $b_{21}(c) = b_{12}(c)$ wegen der Symmetrie und $b_{22}(c)$ mit Theorem 2.13 bestimmt werden.

7.1 Vermutung: *Sei Δ eine Kongruenzuntergruppe mit genau zwei Spitzen, Spitzenvektor $S(\Delta) = [s_1 = \infty, s_2 = g_2\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, w_2]$. Dann gilt:*

$$b_{11}(c) = \begin{cases} w_1\varphi(c) & c \equiv 0 \bmod \frac{w_1}{w_2} \\ (w_1 - w_2)\varphi(c) & \textit{sonst} \end{cases} .$$

7.2 Bemerkung: *Für die übrigen Anzahlen der Doppelnebenklassen ergibt sich:*

$$b_{12}(c) = \begin{cases} 0 & c \equiv 0 \bmod \frac{w_1}{w_2} \\ w_2\varphi(c) & \textit{sonst} \end{cases}$$
$$b_{22}(c) = \begin{cases} w_2\varphi(c) & c \equiv 0 \bmod \frac{w_1}{w_2} \\ 0 & \textit{sonst.} \end{cases}$$

Dabei werden keine weiteren Informationen über die Gruppe benötigt, insbesondere scheint sich aus dem Spitzenvektor zu ergeben, welche Spitzen von $\Gamma(n)$ unter Δ äquivalent werden. Bisher hat sich dieses Bildungsgesetz ebenso wie die weiter unten aufgeführten allen Beweisversuchen widersetzt, so daß wir es hier nur als Vermutung aufführen. Für den Fall, daß w_1 eine Primzahl ist, beweisen wir dieses Gesetz im nächsten Unterabschnitt, eine Verallgemeinerung auf beliebige w_1, w_2 ist aber bisher nicht geglückt. Ähnliche Gesetz lassen sich für Gruppen mit gleichen Spitzenbreiten angeben, wobei die Kongruenzen bezüglich den Teilern der Spitzenbreiten formuliert werden.
Auch für Kongruenzgruppen mit mehr als zwei Spitzen vermuten wir ähnlich strukturierte Bildungsgesetze. Wir geben hier noch eine Vermutung für Gruppen mit genau drei Spitzen an, deren Spitzenbreiten gewisse Teilbarkeiten erfüllen. Sei Δ eine Kongruenzuntergruppe mit genau drei Spitzen, Spitzenvektor $S(\Delta) = [s_1 = \infty, s_2 = g_2\infty, s_3 = g_3\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, w_2, w_3]$ mit $w_1 > w_2 > w_3$. Dann ist Δ eine Kongruenzuntergruppe vom Level w_1 und wir haben beobachtet, daß $(w_2 + w_3)|w_1$ folgt.

7.3 Vermutung: *Sei Δ eine Kongruenzuntergruppe mit genau drei Spitzen, Spitzenvektor $S(\Delta) = [s_1 = \infty, s_2 = g_2\infty, s_3 = g_3\infty]$ und Spitzenbreiten $W(\Delta) = [w_1, w_2, w_3]$ mit $w_1 > w_2 > w_3$ und $(w_2 + w_3)|w_1$. Dann gilt:*

$$b_{11}(c) = \begin{cases} w_1\varphi(c) & c \equiv 0 \bmod \frac{w_1}{w_2+w_3} \\ (w_1 - (w_2 + w_3))\varphi(c) & \textit{sonst} \end{cases}$$
$$b_{12}(c) = \begin{cases} 0 & c \equiv 0 \bmod \frac{w_1}{w_2+w_3} \\ w_2 & \textit{sonst} \end{cases}$$
$$b_{13}(c) = \begin{cases} 0 & c \equiv 0 \bmod \frac{w_1}{w_2+w_3} \\ w_3 & \textit{sonst.} \end{cases}$$

7.1.1 Nochmal $\Gamma_0(p)$

Sei Δ eine Kongruenzuntergruppe vom Level p mit genau zwei Spitzenklassen unterschiedlicher Breite, also $S(\Delta) = [s_1, s_2]$ und $W(\Delta) = [w_1, w_2]$ mit $w_1 > w_2$. Dann gilt nach Satz 1.16 $w_1 = p$ und w_2 teilt die Breite w_1, so daß $w_2 = 1$ gelten muß. Bis auf Konjugation sind die einzigen Gruppen mit zwei Spitzen und Spitzenvektor $[p, 1]$ die in Abschnitt 2.3 betrachteten Gruppen $\Gamma_0(p)$, für die wir jetzt die dort konstruierten Bildungsgesetze analog zu Vermutung 7.1 formulieren und hier beweisen.
$\Gamma_0(p)$ hat zwei Spitzen $s_1 = \infty$ und $s_2 = 0$ der Breiten $w_1 = 1$ und $w_2 = p$. Damit wir den Satz in der aufgestellten Form anwenden können, müsste die Spitzenklasse von ∞ die größere Breite haben und dafür müssten wir $\Gamma_0(p)$ entsprechend konjugieren: Mit $g_2 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \Gamma$ hat $g_2^{-1}\Gamma_0(p)g_2$ die Spitzen

$s_1 = \infty$ und $s_2 = 0$ der Breiten $w_1 = p$ und $w_2 = 1$. Um jetzt aber weiterhin mit $\Gamma_0(p)$ rechnen zu können, formulieren wir Vermutung 7.1 statt für $s_1 = \infty$ für $s_2 = 0$ mit $w_2 > w_1$ entsprechend um:

7.4 Satz: *Für $\Gamma_0(p)$ bestimmt sich das erste Bildungsgesetz als:*

$$b_{11}(c) = \begin{cases} \varphi(c) & c \equiv 0 \bmod p \\ 0 & \textit{sonst} \end{cases} .$$

Die in $\Gamma_0(p)$ enthaltene Hauptkongruenzuntergruppe $\Gamma(p)$ hat den Index $\mu = p(p+1)\frac{p-1}{2}$ und besitzt in Γ genau $r = (p+1)\frac{p-1}{2}$ Spitzenklassen, die alle dieselbe Breite p haben. Von diesen r Spitzenklassen in $\Gamma(p)$ seien r_1 und r_2 die Anzahlen derjenigen Spitzen von $\Gamma(p)$, die in $\Gamma_0(p)$ zu s_1 beziehungsweise s_2 äquivalent werden. Es gilt also $r_1 + r_2 = r$ und $S(\Gamma(p))$ lässt sich anordnen als:

$$S(\Gamma(p)) = [s_1^1, \ldots, s_1^{r_1}, s_2^1, \ldots, s_2^{r_2}]$$

mit $s_i^j \sim_{\Gamma_0(p)} s_i$. Diejenigen Spitzen von $\Gamma(p)$, die in $\Gamma_0(p)$ zueinander äquivalent werden, haben offensichtlich dieselbe relative Spitzenbreite v_i^j in $\Gamma_0(p)$, die sich nach Definition 3.1 und Bemerkung 3.2 bestimmt als die Breite der Spitze in Γ dividiert durch die Breite der Spitze von $\Gamma_0(p)$ in Γ:

$$v_1^j = \frac{p}{w_1} = p \quad \text{und} \quad v_2^j = \frac{p}{w_2} = 1.$$

Wir erhalten:

$$\begin{array}{rcccl} [\Gamma_0(p) : \Gamma(p)] & = & \sum_{j=1}^{r_1} v_1^j & = & pr_1 \\ & = & \sum_{j=1}^{r_2} v_2^j & = & r_2. \end{array}$$

Mit Hilfe der Gradformel:

$$[\Gamma : \Gamma(p)] = [\Gamma : \Gamma_0(p)][\Gamma_0(p) : \Gamma(p)]$$

bestimmen wir die Anzahlen r_1 und r_2 derjenigen Spitzen von $\Gamma(p)$, die in $\Gamma_0(p)$ zu s_1 beziehungsweise s_2 äquivalent werden:

$$\mu = (w_1 + w_2)pr_1 \Leftrightarrow r_1 = \frac{\mu}{p(w_2 + w_2)} = \frac{p-1}{2}$$

und:

$$\mu = (w_1 + w_2)r_2 \Leftrightarrow r_2 = \frac{\mu}{w_1 + w_2} = p\frac{p-1}{2}.$$

Jetzt betrachten wir eine andere Aufteilung der Spitzen von $\Gamma(p)$, nämlich nach den Fasern:

$$\begin{array}{rcl} \lambda_p^{-1}(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]) & = & \{\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{F}) : y \equiv 0(p)\} \\ \lambda_p^{-1}(\left[\begin{smallmatrix}t\\1\end{smallmatrix}\right]) & = & \{\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right] \in \mathbb{P}^1(\mathbb{F}) : x \equiv yt(p), y \not\equiv 0(p)\}, \quad t \in \{0, 1, \ldots, p-1\} \end{array}$$

der Abbildung:

$$\begin{array}{rccc} \lambda: & \Gamma(p)\backslash\mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_p) \\ & \begin{bmatrix} x \\ y \end{bmatrix} & \longmapsto & \begin{bmatrix} x \\ y \end{bmatrix}_p := \begin{bmatrix} x \bmod p \\ y \bmod p \end{bmatrix} \end{array}$$

aus Kapitel 4. Für die zugehörigen Bildungsgesetze ergibt sich nach Abschnitt 4.2:

$$\begin{array}{lll} s_j^k \in \lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}]) & \Rightarrow & b_{11}^{jk}(c) = \begin{cases} \frac{2p}{p-1}\varphi(c) & c \equiv 0 \bmod p \\ 0 & \text{sonst} \end{cases} \\ s_j^k = [\begin{smallmatrix}x\\y\end{smallmatrix}] \in \lambda^{-1}([\begin{smallmatrix}t\\1\end{smallmatrix}]) & \Rightarrow & b_{11}^{jk}(c) = \begin{cases} \varphi(c) & c \equiv \pm y \bmod p \\ 0 & \text{sonst.} \end{cases} \end{array}$$

Mit Satz 3.5 lässt sich das Bildungsgesetz $b_{11}(c)$ von $\Gamma_0(p)$ aus den Bildungsgesetzen b_{11}^{jk} von $\Gamma_0(p)$ berechnen als:

$$v_1^k b_{11}(c) = \sum_{j=1}^{r_1} b_{11}^{jk}$$

mit $v_1^k = p$. Um die zugehörigen Bildungsgesetze aufsummieren zu können, benötigen wir eine experimentelle Beobachtung für die Spitzen einer Faser von λ: Wenn eine der Spitzen einer Faser $\Gamma_0(p)-$äquivalent zu einer Spitze s_i wird, dann folgt dies auch für alle anderen Spitzen dieser Faser. Wir formulieren diese Aussage hier für die Spitze ∞:

7.5 Lemma: *Sei $s_j^k \in \lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}])$. Dann existiert ein $\gamma \in \Gamma_0(p)$ mit $\gamma\infty = s_j^k$, d.h $s_j^k \sim_{\Gamma_0(p)} \infty$.*

Beweis:
Aus $s_j^k = [\begin{smallmatrix}x\\y\end{smallmatrix}] \in \lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}])$ folgt $y \equiv 0 \bmod p$ und nach Satz 1.10 existiert ein $g_j^k \in \Gamma$ mit $g_j^k\infty = s_j^k$, wobei g_j^k die Gestalt $g_j^k = \left(\begin{smallmatrix} x & b \\ y & d \end{smallmatrix}\right)$ hat. Wegen $y \equiv 0 \bmod p$ folgt $\gamma := g_j^k \in \Gamma_0(p)$. □

Die Beobachtung, daß aus der $\Delta-$Äquivalenz einer Spitze s_i^j von $\Gamma(n)$ zu einer Spitze s_i von Δ dieselbe Äquivalenz für alle anderen Spitzen derselben Faser folgt, haben wir für echte Obergruppen von Hauptkongruenzuntzergruppen mit genau zwei Spitzen zwar gemacht, aber nur für den Fall von $\Delta = \Gamma_0(p)$ zeigen können. Auch andere Beweisansätze ließen sich bisher nicht auf alle Gruppen übertragen.
Insgesamt haben wir $r_1 = \frac{p-1}{2}$ Spitzen von $\Gamma(p)$, die unter $\Gamma_0(p)$ äquivalent zur Spitze $s_1 = \infty$ werden. Nach obigem Lemma sind andererseits zumindest alle Spitzen der Faser $\lambda^{-1}([\begin{smallmatrix}1\\0\end{smallmatrix}])$ unter $\Gamma_0(p)$ äquivalent zur Spitze $s_1 = \infty$. Da jede Faser genau $\frac{p-1}{2}$ Elemente hat, folgt die Gleichheit. Wir kennen jetzt also die r_1

Spitzen genau und können ihre zugehörigen Bildungsgesetze aufsummieren:

$$\begin{aligned} pb_{11}(c) &= \sum_{j=1}^{r_1} b_{11}^{jk} = \tfrac{p-1}{2} \begin{cases} \frac{2p}{p-1}\varphi(c) & c \equiv 0 \bmod p \\ 0 & \text{sonst} \end{cases} \\ &= p \begin{cases} \varphi(c) & c \equiv 0 \bmod p \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

7.2 Nichtkongruenzuntergruppen

Für Nichtkongruenzuntergruppen Δ haben wir keine offensichtlichen Untergruppen zur Verfügung, aus denen wir wie im Fall der Kongruenzuntergruppen Bildungsgesetze konstruieren können. Es ist daher naheliegend, daß es für Nichtkongruenzuntergruppen im Allgemeinen keine Bildungsgesetze für die Eingänge der Streumatrix gibt.
Trotzdem haben wir einige Nichtkongruenzuntergruppen Δ gefunden, deren Bildungsgesetze wir genau angeben können. So erfüllen einige Gruppen mit genau zwei Spitzen unterschiedlicher Breite das in Vermutung 7.1 angegebene Bildungsgesetz. Der Grund bei den von uns beobachteten Untergruppen war, daß Δ Untergruppe einer Kongruenzuntergruppe mit genau denselben Spitzenklassen ist. Für solche Gruppen haben wir in Satz 3.9 gesehen, daß sich die Bildungsgesetze von Δ aus denen von Λ durch Multiplikation mit dem Index $[\Lambda : \Delta]$ ergeben. So gilt z.B. für alle in Beispiel 3.10 aufgeführte Gruppen das in Vermutung 7.1 angegebene Bildungsgesetz, weil es für die Obergruppe Λ vom Level 2, erzeugt von:

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \right\}$$

efüllt ist. Wir können die Nichtkongruenzuntergruppen in zwei Typen einteilen: Zum Einen haben wir Nichtkongruenzuntergruppen, deren Spitzenbreiten all diejenigen Eigenschaften erfüllen, die auch für Kongruenzuntergruppen gelten. Wenn wir wie in Kapitel 1 den erweiterten Level $n(\Delta)$ einer beliebigen Untergruppe Δ von Γ als das kleinste gemeinsame Vielfache ihrere Spitzenbreiten definieren, so haben diese Nichtkongruenzuntergruppen eine Spitze der Breite $n(\Delta)$. Wir haben vermutet, daß es für einige Nichtkongruenzuntergruppen von diesem Typ möglich ist, die Bildungsgesetze ihrer Streumatrix als Vielfache der Eulerschen $\varphi-$Funktion anzugeben. Unter anderem haben wir uns mit folgender Untergruppe beschäftigt:

7.6 Beispiel: Sei Δ die Nichtkongruenzuntergruppe vom Index 7 mit den Erzeugern:

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 4 & -3 \end{pmatrix} \right\}$$

dem Spitzenvektor $S(\Delta) = \left[\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}\right]$, dem Vektor $W(\Delta) = [6, 1]$ der Spitzenbreiten und dem erweiterten Level $n(\Delta) = 6$.

Zu dieser Gruppe ist es uns aber nicht gelungen, Bildungsgesetze anzugeben. Unter anderem haben wir experimentell die ersten 2000 Einträge der Dirichletreihen in der Streumatrix berechnet und wir konnten zumindest gewisse Abschätzungen beobachten:

7.7 Beobachtung: *Für $n \in \{1, \ldots, 6000\}$ gilt:*

$$5\varphi(c) \leq b_{11}(c) \leq 6\varphi(c).$$

Dabei ist die obere Schranke offensichtlich, da für die Summe der ersten Zeile gelten muß:

$$b_{11}(c) + b_{12}(c) = 6\varphi(c).$$

Würde das in Vermutung 7.1 angegebene Bildungsgesetz für Δ gelten, so hätte b_{11} die Gestalt:

$$b_{11}(c) = \begin{cases} 6\varphi(c) & c \equiv 0 \bmod 6 \\ 5\varphi(c) & \text{sonst} \end{cases}.$$

Wir haben also beobachtet, daß die tatsächliche Anzahl der Doppelnebenklassen innerhalb dieses Gesetzes schwankt, wobei sich die einzelnen Werte nicht immer als Vielfache der Eulerschen $\varphi-$Funktion angeben lassen. Auch die Gleichheit wird nicht an ohne Weiteres zu klassifizierenden Stellen angenommen, tritt aber mit wachsendem n immer seltener auf. Speziell diese Untergruppe sollte noch Gegenstand weiterer Untersuchungen sein.
Zu dem anderen Typ der Nichtkongruenzuntergruppen gehören solche Gruppen Δ, deren Spitzenvektoren keine Spitze mit der Breite des erweiterten Levels besitzen. Das Beispiel mit kleinstem Index ist die folgende Untergruppe:

7.8 Beispiel: Sei Δ die Untergruppe vom Index 7 erzeugt von:

$$\left\{\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}, \begin{pmatrix}0 & -1\\1 & -3\end{pmatrix}, \begin{pmatrix}4 & -3\\7 & -5\end{pmatrix}\right\}$$

dem Spitzenvektor $S(\Delta) = \left[\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}\right]$, dem Vektor $W(\Delta) = [4, 3]$ der Spitzenbreiten und dem erweiterten Level $n(\Delta) = 12$.

Hier vermuten wir, daß sich zu dieser und anderen Untergruppen von diesem Typ kein Bildungsgesetz angeben läßt, aber eventuell ergeben sich auch für solche Nichtkongruenzuntergruppen Möglichkeiten, die Einträge zumindest abzuschätzen - auch wenn dies z.B. für Untersuchungen der Determinante der Streumatrix nicht unbedingt hilfreich ist.

Dann gibt es noch die Nichtkongruenzuntergruppen, die sich nach Satz 3.11 teilweise wie eine Kongruenzgruppe verhalten. Dann gelten für diese Einträge der Streumatrix ebenfalls die vermuteten Bildungsgesetze für Kongruenzuntergruppen gelten.

7.9 Beispiel: Sei Δ die Untergruppe erzeugt von

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -2 & -3 \end{pmatrix} \begin{pmatrix} 2 & 9 \\ -1 & -4 \end{pmatrix} \right\}.$$

Δ ist eine Nichtkongruenzuntergruppe vom Index 9 mit dem Spitzenvektor $S(\Delta) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right]$ und Spitzenbreiten $W(\Delta) = [6, 2, 1]$. Darüberhinaus ist Δ ebenso wie die in Beispiel 3.10 betrachteten Gruppen mit zwei Spitzen, Untergruppe der Kongruenzuntergruppe Λ vom Level 2, erzeugt von

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \right\}$$

mit dem Spitzenvektor $S(\Lambda) = \left[\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right]$ und Spitzenbreiten $W(\Lambda) = [2, 1]$. Unter Λ werden die Spitzen aus den beiden Spitzenklassen $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ und $\begin{bmatrix} 1 \\ 3 \end{bmatrix}$ von Δ zueinander äquivalent. Daher ergeben sich die Bildungsgesetze von Δ in der ersten Zeile und damit auch in der ersten Spalte der Streumatrix aus denen von Λ und sind Vielfache der Eulerschen $\varphi-$Funktion. Das Bildungsgesetz in der oberen linken Ecke der Streumatrix ist das Dreifache des entspechenden Bildungsgesetzes von Λ aus Vermutung 7.1, da $[\Lambda : \Delta] = 3$. Für die anderen beiden Bildungsgesetze der ersten Zeile bestimmen wir die relativen Spitzenbreiten $w_2^1 = 2$ und $w_2^2 = 1$ und erhalten damit die Bildungsgesetze als die entsprechenden Vielfache von:

$$b_{12}(c) = \begin{cases} 0 & c \equiv 0 \bmod 2 \\ \varphi(c) & \text{sonst} \end{cases},$$

also hier:

$$b_{11}^{11}(c) = \begin{cases} 6\varphi(c) & c \equiv 0 \bmod \frac{6}{2+1}, \text{ also } c \equiv 0 \bmod 2 \\ 3\varphi(c) & \text{sonst} \end{cases},$$

$$b_{12}^{11}(c) = \begin{cases} 0 & c \equiv 0 \bmod \frac{6}{2+1}, \text{ also } c \equiv 0 \bmod 2 \\ 2\varphi(c) & \text{sonst} \end{cases},$$

$$b_{12}^{12}(c) = \begin{cases} 0 & c \equiv 0 \bmod \frac{6}{2+1}, \text{ also } c \equiv 0 \bmod 2 \\ \varphi(c) & \text{sonst} \end{cases}$$

Diese Bildungsgesetze entsprechen der Vermutung 7.1, angewendet auf diese Nichtkongruenzuntergruppe.

8 Anhang: Programme

Ein Ziel dieser Arbeit war es, die Streumatrix für Untergruppen der Modulgruppe am Computer zu realisieren.
Dazu wurden zunächst Programme entwickelt, die für eine vorgegebene Untergruppe Δ von $\mathrm{PSL}(2,\mathbb{Z})$ mit endlichem Index ein Repräsentantensystem der Spitzen und ihre Breiten bestimmen und dann die für die Streumatrix benötigten Anzahlen der Doppelnebenklassen bis zu einer bestimmten Grenze berechnen. Diese Programme sind unabhängig davon, ob es sich bei Δ um eine Kongruenzuntergruppe handelt oder nicht.
Ein weiteres Programm entscheidet, ob Δ eine Kongruenzuntergruppe ist.
Die hier aufgeführten Programme wurden in GAP realisiert und können neben weiteren Programmen und Beispieldateien von meiner homepage **ckeil.de** heruntergeladen werden.

8.1 $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$ erzeugen

```
#############################################################################################
# Γ als freie Gruppe mit B=G.1, S=G.2
#############################################################################################
F := FreeGroup( "B", "S" );;
# Relationen
G := F / [ F.1^2,F.2^3];;
B:=G.1;; S:=G.2;;
# häufig benutze Matrizen
BB:=[[0,1],[-1,0]];;
SS:=[[0,1],[-1,1]];;
T:=S^2*B;;
TT:=Matrixdarstellung(T);;
```

8.2 Darstellung einer Matrix als Produkt aus Erzeugern von Γ und umgekehrt

```
#############################################################################################
```

```
# Proc_Matrix2Wort
# Funktion, um eine gegebene 2 × 2 Matrix als Wort in B und S darzustellen
#########################################################################################
Wortdarstellung:=function(A)
        local Wort_A,help;
        Wort_A:=B∧2*B∧2;;
        while (A[1][1]<>0 and A[2][1]<>0 and A[1][2]<>0 and A[2][2]<>0) do
                if A[1][1]<0 then
                A:=BB∧2*A;;
                        Wort_A:=B∧2*Wort_A;;
                elif A[2][1]>0 and A[1][1]>=A[2][1] then
                        A:=BB∧2*BB*SS*A;;
                        Wort_A:=B∧2*B*S*Wort_A;;
                elif A[2][1]>0 and A[1][1]<A[2][1] then
                        A:=BB∧2*BB*SS∧2*BB∧2*A;;
                        Wort_A:=B∧2*B*S∧2*B*B*Wort_A;;
                elif A[2][1]<0 then
                        A:=BB∧2*BB*SS∧2*BB*A;;
                        Wort_A:=B∧2*B*S∧2*B*Wort_A;;
                fi;
        od;
        if A[1][1]=0 and A[2][1]=1 then help:=B∧2*B*((S∧2*B)∧A[2][2]);;
        elif A[1][1]=0 and A[2][1]=-1 then help:=B*((S∧2*B)∧(-A[2][2]));;
        elif A[2][1]=0 and A[1][1]=1 then help:=(S∧2*B)∧A[1][2];;
        elif A[2][1]=0 and A[1][1]=-1 then help:=B∧2*((S∧2*B)∧(-A[1][2]));;
        elif A[1][2]=0 and A[1][1]=1 then help:=B∧2*B*((S∧2*B)∧(-A[2][1]))*B;;
        elif A[1][2]=0 and A[1][1]=-1 then help:=B*((S∧2*B)∧A[2][1])*B;;
        elif A[2][2]=0 and A[2][1]=1 then help:=B∧2*((S∧2*B)∧A[1][1])*B;;
        elif A[2][2]=0 and A[2][1]=-1 then help:=((S∧2*B)∧(-A[1][1]))*B;;
        fi;
        Wort_A:=((Wort_A)∧-1)*help;;
        return Wort_A;
        end;;
```

```
##############################################################################################
# Proc_Wort2Matrix
# Funktion, um eine Matrix A gegeben in B und S als 2x2-Matrix darzustellen
##############################################################################################
Matrixdarstellung:=function (A)
        local help;
        if A=«identity ...>then help:=B∧2*B∧2;
        else
                help:=A;
                help:=ReplacedString(String(help),"B","BB");
                help:=ReplacedString(String(help),SS",SSS");
                help:=EvalString(help);
                if (help[1][1]<0) then help:=-1*help;
                fi;
        fi;
        return help;
        end;
```

8.3 Die Spitzenmenge $S(\Delta)$ und den Vektor der Spitzenbreiten $W(\Delta)$ bestimmen

```
##############################################################################################
# Diese Prozedur bestimmt für eine durch ihre Erzeuger gegebene Untergruppe
# Δ <_f Γ die Spitzenmenge S(Δ) und die Spitzenbreiten W(Δ)
##############################################################################################
# Bestimmung der Restklassen RC von Δ \ Γ und Repraesentanten
RC:=RightCosets(Γ,Δ);;
RC_Anzahl:=Length(RC);;
Repraesentanten:=List([1..RC_Anzahl],i->1);;
for i in [1..RC_Anzahl] do
        Repraesentanten[i]:=Representative(RC[i]);;
od;
# Bestimmung der n_i
n:=List([1..RC_Anzahl], i->1);;
for i in [1..RC_Anzahl] do
        if      (String(Repraesentanten[i])="<identity ...>")=true then
                        Repraesentanten[i]:=B∧ 2;
        fi;
        while (Repraesentanten[i]*T∧ n[i]*Repraesentanten[i]∧ (-1) in Δ) =false do
```

```
                n[i]:=n[i]+1;;
        od;
od;
♯Bestimmung des kleinsten gemeinsamen Vielfaches der n_i
help:=n[1];;
for i in [2..RC_Anzahl] do
        help:=LcmInt(help,n[i]);
        i:=i+1;
od;
kgv_n:=help;;
♯Repraesentatensystem fuer Δ \ Γ/Γ∞ bestimmen, indem diejenigen Elemente
♯ aus dem Repraesentantensystem fuer Δ \ Γ gestrichen werden, die modulo Γ∞
♯ uebereinstimmen
s_help:=List([1..RC_Anzahl], i->1);;
for i in [1..RC_Anzahl] do
        for l in [i+1..RC_Anzahl] do
                for j in [1..kgv_n] do
                if (Repraesentanten[i]*T∧ j*Repraesentanten[l]∧ (-1) in Δ)=true then
                        s_help[l]:=0;
                else j:=j+1;
                fi;
                od;
        od;
od;
♯Repraesentatensystem fuer Δ \ Γ/Γ∞zusammenfassen:
AnzahlSpitzen:=0;;
for i in [1..RC_Anzahl] do
        AnzahlSpitzen:=AnzahlSpitzen+s_help[i];
od;
Repraesentanten_Spitzen:=List([1..AnzahlSpitzen], i->0);;
j:=1;;
for i in [1..RC_Anzahl] do
        if s_help[i]=1 then
                Repraesentanten_Spitzen[j]:=Repraesentanten[i];
        j:=j+1;
                fi;
od;
♯Spitzenbreiten bestimmen:
♯Finde zu jeder Spitze minimals w_i, so dass g_i*T∧ w_i*g_i∧ -1 in Δ liegt
Spitzenbreiten:=List([1..AnzahlSpitzen],i->1);;
for i in [1..AnzahlSpitzen] do
        while (Repraesentanten_Spitzen[i]*T∧ Spitzenbreiten[i]*
```

```
                Repraesentanten_Spitzen[i]∧ -1 in Δ)=false do
                Spitzenbreiten[i]:=Spitzenbreiten[i]+1;
        od;
od;
♯Umrechnen der g_i in die Spitzen: g_i*unendlich=s_i
help:=List([1..AnzahlSpitzen], i->0);;
for i in [1..AnzahlSpitzen] do
        help[i]:=Matrixdarstellung(Repraesentanten_Spitzen[i]);
od;
glistematrix:=help;
♯Umrechnen der Repraesentanten s_i der Spitzenklassen
help:=List([1..AnzahlSpitzen], i->0);;
for i in [1..AnzahlSpitzen] do
        help[i]:=[glistematrix[i][1][1],glistematrix[i][2][1]];
od;
Spitzenliste:=help;
```

8.4 Die Anzahlen b_{ij} berechnen

```
#############################################################################################
♯ Diese Prozedur berechnet für Δ die Werte der b_ij(c)
♯ bis zu einer vorgegebenen Grenze
#############################################################################################
♯ Bereitstellung der benoetigten Variablen
b:=List([1..AnzahlSpitzen]);
for i in [1..AnzahlSpitzen] do
        b[i]:=List([1..AnzahlSpitzen]);
        for k in [1..AnzahlSpitzen] do
        b[i][k]:=List([1..Grenze],i ->0);
        od;
od;
#####################################################
♯ Schleife ueber c
for c in [1..Grenze] do
♯ Liste der Woerter ueber c
W_c:=List([1..Phi(c)], i->0);;
i:=1;
for a in [1..c] do
        if GcdInt(a,c)=1 then
                ♯ Bestimmung von W_c[i]:=X(a,c)
```

```
                Euklid_d:=GcdRepresentation(Integers,a,c) mod c;;
                d:=Euklid_d[1];;
                bb:=(a*d-1)/c;;
                W_c[i]:=[[a,bb],[c,d]];;
                i:=i+1;;
        fi;
od;
#################################################
# Schleifen ueber Spitzenanzahl
for zeile in [1..AnzahlSpitzen] do
for spalte in [zeile..AnzahlSpitzen] do
#################################################
# Eintrag b[zeile,spalte] bestimmen
# Zuerst Liste aller Woerter von rechts und von links multipliziert mit
# Potenzen von T bis zur jeweiligen Spitzenbreite
N_ij:=List([1..Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]], i->0);;
j:=1;
for i in [1..Phi(c)] do
        for n in [1..Spitzenbreiten[zeile]] do
                for m in [1..Spitzenbreiten[spalte]] do
                        N_ij[j]:=TT^ n*W_c[i]*TT^ m;
                        j:=j+1;
                od;
        od;
od;
# doppelte Matrizen streichen
for i in [1..Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]] do
        for k in [i+1..Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]] do
                if (N_ij[i]=N_ij[k])=true then
                        N_ij[k]:=0;
                fi;
        od;
od;
# Neue Liste aller Woerter mit Potenzen von T multipliziert
# ohne doppelte Eintraege
Doppelte:=0;
for i in [1..Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]] do
        if N_ij[i]=0 then
                Doppelte:=Doppelte+1;
        fi;
od;
N_Neu:=List([1..(Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]-Doppelte)], i->0);;
```

```
k:=1;;
for i in [1..Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]] do
        if (N_ij[i]=0)=false then
                N_Neu[k]:=N_ij[i];
                k:=k+1;
        fi;
od;
# Zaehlen: fuer jedes Wort A aus N_Neu ueberpruefen, ob
# g_zeile*A*g_spalte^ -1 in Δ liegt
N_Boolean:=List([1..(Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]-Doppelte )], i->0);;
for i in [1..(Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]-Doppelte)] do
        help:=glistematrix[zeile]*N_Neu[i]*glistematrix[spalte]^ -1;
        if Wortdarstellung(help) in Δ then
                N_Boolean[i]:=1;
        fi;
od;
# Aufsummieren
help:=0;;
for i in [1..(Phi(c)*Spitzenbreiten[zeile]*Spitzenbreiten[spalte]-Doppelte)] do
        help:= help + N_Boolean[i];
od;
b[zeile][spalte][c]:=help;
#####################################################
# Ende Schleifen ueber Spitzenanzahl
od;
od;
#####################################################
# Ende Schleife ueber c
od;
```

8.5 Bestimmen, ob Δ eine Kongruenzuntergruppe ist

```
#############################################################################################
# Diese Prozedur überprüft, ob Δ eine Kongruenzuntergruppe ist,
# und gibt gegebenenfalls ihren Level an.
# Der Algorithmus beruht im Wesentlichen auf einem Artikel von Tim Hsu [Hsu96].
#############################################################################################
cs:=true;
```

```
♯ Bestimmung des moeglichen Levels
N:=Lcm(Spitzenbreiten);
factors:=FactorsInt(N);
lang:=Length(factors);
ee:=0;
m:=1;
for i in [1..lang] do
        if factors[i]=2 then
                ee:=ee+1;
        fi;
        if factors[i]>2 then
                m:=m*factors[i];
        fi;
od;
##################################################
♯ Kann die Untergruppe theoretisch eine Kongruenzuntergruppe sein ?
♯ Nach Lemma 1.17 muß es dann eine Spitze mit Spitzenbreite N geben.
spitzentest:=0;
for i in [1..AnzahlSpitzen] do
        if N=Spitzenbreiten[i] then
                spitzentest:=spitzentest+1;
        fi;
od;
if spitzentest=0 then
        cs:=false;
fi;
if (spitzentest=0)=false then
##################################################
♯ Fallunterscheidung bezueglich ee und m
♯ N=2∧ ee*m
♯ Bestimmung der Restklassen RC von Δ \ Γ und der Repraesentanten
RC:=RightCosets(G,D);;
RC_Anzahl:=Length(RC);;
RC_D:=List([1..RC_Anzahl],i->1);;
for i in [1..RC_Anzahl] do
        RC_D[i]:=Representative(RC[i]);;
od;
##################################################
if ee=0 then
        ♯ Print( “Fall: N ungerade ohne Zweierpotenz\ n”);
        x:=0;
        for i in [1..2*N] do
```

```
                if (2*i) mod N =1 then
                        x:=i;
                        break;
                fi;
        od;
        a:=T;
        b:=(B*T*B)∧ (-1);
        Relationen:=List([1..4]);
        Relationen[1]:=a∧ N;
        Relationen[2]:=(a*b∧ (-1)*a)∧ 4;
        Relationen[3]:=(b∧ (-1)*a)∧ 3*(a*b∧ (-1)*a)∧ (-2);
        Relationen[4]:=(b∧ 2*a∧ (-x))∧ 3*(a*b∧ (-1)*a)∧ (-2);
        for i in [1..Indexgruppe] do
                for ii in [1..4] do
                        test:=RC_D[i]*Relationen[ii]*(RC_D[i]∧ (-1));
                        testtest:=test in D;
                        if testtest=false then
                                cs:=false;
                        fi;
                od;
        od;

fi;
##################################################
if (m=1 and (ee=0)=false) then
        Print("Fall: N gerade \ n");
        y:=0;
        for i in [1..5*N] do
                if (5*i) mod N =1 then
                        y:=i;
                        break;
                fi;
        od;
        l:=T;
        r:=(B*T*B)∧ (-1);
        s:=l∧ 20*r∧ y*l∧ (-4)*r∧ (-1);
        Relationen:=List([1..6]);
        Relationen[1]:=l∧ N;
        Relationen[2]:=(l*r∧ (-1)*l)∧ 4;
        Relationen[3]:=(r∧ (-1)*l)∧ 3*(l*r∧ (-1)*l)∧ (-2);
        Relationen[4]:=(l*r∧ (-1)*l)∧ (-1)*s*(l*r∧ (-1)*l)*s;
        Relationen[5]:=s∧ (-1)*r*s*r∧ (-25);
```

```
        Relationen[6]:=(s*r∧ 5*l*r∧ (-1)*l)∧ 3*(l*r∧ (-1)*l)∧ (-2);
        for i in [1..Indexgruppe] do
                for ii in [1..6] do
                        test:=RC_D[i]*Relationen[ii]*(RC_D[i]∧ (-1));
                        testtest:=test in D;
                        if testtest=false then
                                cs:=false;
                        fi;
                od;
        od;
fi;
##################################################
if ((ee=0)=false and (m=1)=false) then
        Print("Fall: N ungerade und enthaelt Zweierpotenz \ n");
        x:=0;
        y:=0;
        c:=0;
        d:=0;
        for i in [1..2*N] do
                if (2*i) mod m =1 then
                        x:=i;
                        break;
                fi;
        od;
        for i in [1..5*N] do
                if (5*i) mod 2∧ ee =1 then
                        y:=i;
                        break;
                fi;
        od;
        for i in [1..m*N] do
                if (2∧ ee*i) mod m =1 then
                        c:=2∧ ee*i;
                        break;
                fi;
        od;
        for i in [1..2∧ ee*N] do
                if (m*i) mod 2∧ ee =1 then
                        d:=m*i;
                        break;
                fi;
        od;
```

```
        L:=T;
        R:=(B*T*B)^ (-1);
        a:=L^ c;
        b:=R^ c;
        l:=L^ d;
        r:=R^ d;
        s:=l^ 20*r^ y*l^ (-4)*r^ (-1);

        Relationen:=List([1..11]);
        Relationen[1]:=L^ N;
        Relationen[2]:=a^ (-1)*r^ (-1)*a*r;
        Relationen[3]:=b^ (-1)*l^ (-1)*b*l;
        Relationen[4]:=(a*b^ (-1)*a)^ 4;
        Relationen[5]:=(b^ (-1)*a)^ 3*(a*b^ (-1)*a)^ (-2);
        Relationen[6]:=(b^ 2*a^ (-x))^ 3*(a*b^ (-1)*a)^ (-2);
        Relationen[7]:=(l*r^ (-1)*l)^ 4;
        Relationen[8]:=(r^ (-1)*l)^ 3*(l*r^ (-1)*l)^ (-2);
        Relationen[9]:=s^ (-1)*(l*r^ (-1)*l)^ (-1)*s^ (-1)*(l*r^ (-1)*l);
        Relationen[10]:=r^ 25*s^ (-1)*r^ (-1)*s;
        Relationen[11]:=(s*r^ 5*l*r^ (-1)*l)^ 3*(l*r^ (-1)*l)^ (-2);

        for i in [1..Indexgruppe] do
                for ii in [1..11] do
                        test:=RC_D[i]*Relationen[ii]*(RC_D[i]^ (-1));
                        testtest:=test in D;
                        if testtest=false then
                                cs:=false;
                        fi;
                od;
        od;
fi;
##################################################
fi;
```

Literaturverzeichnis

[Apo76] Apostol, Tom M.: *Modular functions and Dirichlet series in number theory.* Springer Verlag, 2 Auflage, 1976.

[Atk78] Atkin, A. O. L.: *The Number of Subgroups of the Classical Modular Group of Index N.* Mathematics of Computation., 32(141), 1978.

[BM68] Behr, H. und J. Mennicke: *A presentation of the groups* PSL(2, p). Canad. J. Math., 20:1432–1438, 1968.

[CP03] Cummins, C. J. und S. Pauli: *Congruence subgroups of* PSL$(2, \mathbb{Z})$ *of genus less than or equal to 24.* Experiment. Math., 12(2):243–255, 2003.

[DS05] Diamond, Fred und Jerry Shurman: *A first course in modular forms*, Band 228 der Reihe *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2005.

[EGM85] Elstrodt, Jürgen, Fritz Grunewald und Jens Mennicke: *Eisenstein series on three-dimensional hyperbolic space and imaginary quadratic number fields.* J. Reine Angew. Math., 360:160–213, 1985.

[FB95] Freitag, Eberhard und Rolf Busam: *Funktionentheorie.* Springer-Verlag, 1995.

[Fis79] Fischer, Gerd: *Lineare Algebra*, Band 17 der Reihe *Grundkurs Mathematik [Foundational Course in Mathematics].* Friedr. Vieweg & Sohn, Braunschweig, Fifth Auflage, 1979. In collaboration with Richard Schimpl.

[FS74] Fischer, Gerd und Reinhard Sacher: *Einführung in die Algebra.* B.G. Teubner Stuttgart, 1974.

[GAP] GAP: *turnbull.mcs.st-and.ac.uk/∼gap/.*

[GLP04] Goldfeld, Dorian, Alexander Lubotzky und László Pyber: *Counting congruence subgroups.* Acta Math., 193(1):73–104, 2004.

[Gun62] Gunning, R.C.: *Lectures on modular forms.* Princeton Univ. Press, 1962.

[Hej76] Hejhal, Dennis A.: *The Selberg trace formula for* PSL$(2, R)$. *Vol. I*, Band 548 der Reihe *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1976.

[Hej83] Hejhal, Dennis A.: *The Selberg trace formula for* PSL$(2, \mathbf{R})$. *Vol. II*, Band 1001 der Reihe *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1983.

[HR64] Hardy, G. H. und M. Riesz: *The general theory of Dirichlet's series*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 18. Stechert-Hafner, Inc., New York, 1964.

[Hsu96] Hsu, Tim: *Identifying congruence subgroups of the modular group*. Proc. Amer. Math. Soc., 124(5):1351–1359, 1996.

[HW58] Hardy, Godfrey H. und Edward M. Wright: *Einführung in die Zahlentheorie*. Oldenbourg, 1958.

[IR90] Ireland, Kenneth und Michael Rosen: *A classical introduction to modern number theory*, Band 84 der Reihe *Graduate Texts in Mathematics*. Springer-Verlag, New York, Second Auflage, 1990.

[Iwa02] Iwaniek, Hentyk: *Spectral methods of automorphic forms*. American Mathematical Socuety, 2002.

[Kei02] Keil, Caroline: *Calculations of* $H^1(PSL(2, \mathbb{Z}), M_n)$. Diplomarbeit, 2002.

[KF66] Klein, Felix und Robert Fricke: *Vorlesungen über die Theorie der elliptischen Modulfunktionen*, Band 1. Johnson Reprint, B.G.Teubner, 1966.

[KK98] Koecher, Max und Aloys Krieg: *Elliptische Funktionen und Modulformen*. Springer-Verlag, Berlin, 1998.

[Kob84] Koblitz, Neal: *Introduction to elliptic Curves and modular forms*. Springer-Verlag, 1984.

[Kub73] Kubota, Tomio: *Elementary Theory of Eisenstein Series*. Kodansha Ltd. (Halstad Press), 1973.

[Lan74] Lang, Serge: *Algebra*. Addison-Wesley, 1974.

[Lan76] Lang, Serge: *Introduction to modular forms*. Springer-Verlag, 1976.

[Lar82] Larcher, H.: *The cusp amplitudes of the congruence subgroups of the classical modular group*. Illinois J. Math., 26(1):164–172, 1982.

[Leh64] Lehner, Joseph: *Discontinous groups and automorpic functions.* American Math. Soc., 1964.

[Maa49] Maass, Hans: *Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen.* Math. Ann., 121:141–183, 1949.

[Mil69] Millington, M. H.: *Subgroups of the classical modular group.* J. London Math. Soc. (2), 1:351–357, 1969.

[MSP05] Müller, T. W. und J.-C. Schlage-Puchta: *Divisibility properties of subgroup numbers for the modular group.* New York J. Math., 11:205–224 (electronic), 2005.

[New63] Newman, Morris: *Normal congruence subgroups of the modular group.* Amer. J. Math. 85 (1963), 419-427; errata, ibid. 85 (1963), 753;, 86:465, 1963.

[New64] Newman, Morris: *A complete description of the normal subgroups of genus one of the modular group.* Amer. J. Math., 86:17–24, 1964.

[New67] Newman, Morris: *Classification of normal subgroups of the modular group.* Trans. Amer. Math. Soc., 126:267–277, 1967.

[New77] Newmann, Morris: *The Number of Subgroups of the Classical Modular Group of Index N.* Mathematics of Computation, 31(138), 1977.

[Pet71] Petersson, Hans: *Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe.* J. Reine Angew. Math., 250:182–212, 1971.

[Pet74] Petersson, Hans: *Konstruktionsprinzipien für Untergruppen der Modulgruppe mit einer oder zwei Spitzenklassen.* J. Reine Angew. Math., 268/269:94–109, 1974. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.

[Pet82] Petersson, Hans: *Modulfunktionen und quadratische Formen.* Springer-Verlag, 1982.

[Ran77] Rankin, Robert A.: *Modular forms and functions.* Cambridge University Press, Cambridge, 1977.

[Sch74] Schoeneberg, Bruno: *Elliptic modular functions: an introduction.* Springer-Verlag, New York, 1974. Translated from the German by J. R. Smart and E. A. Schwandt, Die Grundlehren der mathematischen Wissenschaften, Band 203.

[Sel56] Selberg, Atle: *Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series*. J. Indian Math. Soc. (N.S.), 20:47–87, 1956.

[Sel89] Selberg, Atle: *Collected papers*, Band 1. Springer Verlag, 1989.

[Sel91] Selberg, Atle: *Collected papers*, Band 2. Springer Verlag, 1991.

[Shi71] Shimura, Goro: *Introduction to the Arithmetic Theory of Automorphic Functions*. IwanaShoten and Princeton University Press, 1971.

[Ter85] Terras, Audrey: *Harmonic analysis on symmetric spaces and applications. I.* Springer-Verlag, New York, 1985.

[Ven81] Venkov, Aleksej B.: *Spectral theory of automorphic functions*. Proceedings of the Steklov Institute of Mathematics, 153(4), 1981.

[Ver] Verrill, Helena A.: *Algorithm for Drawing Fundamental Domains*. math.lsu.edu/∼verrill/.

[Woh64] Wohlfahrt, Klaus: *An extension of F. Klein's level concept*. Illinois J. Math., 8:529–535, 1964.

[Woh89] Wohlfahrt, Klaus: *Über die Spitzenbreiten von Kongruenzuntergruppen der rationalen Modulgruppe*. Abh. Math. Sem. Univ. Hamburg, 59:89–92, 1989.