Galois-Operationen auf verallgemeinerten Macbeath-Hurwitz Kurven

Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften

vorgelegt beim Fachbereich Informatik und Mathematik
der Goethe–Universität in Frankfurt am Main

von
Frank Feierabend
aus Bochum

Frankfurt 2009
(D 30)

vom Fachbereich *Informatik und Mathematik* der

Johann Wolfgang Goethe–Universität als Dissertation angenommen.

Dekan: *Prof. Dr. Klaus Johannson*

Gutachter: *Prof. Dr. Jürgen Wolfart, Prof. Dr. Annette Werner*

Datum der Disputation: *8. Dezember 2008*

Einleitung

Kompakte Riemannsche Flächen vom Geschlecht $g > 1$ haben höchstens $84(g-1)$ viele Automorphismen. Die Flächen, deren Automorphismengruppe diese maximale Größe erreicht sind die *Hurwitz-Kurven* (kompakte Riemannsche Flächen sind glatte projektive Kurven über $\mathbb{C}$ und wenn im Folgenden von Kurven die Rede sein wird, sind stets kompakte Riemannsche Flächen gemeint); die zugehörigen Automorphismengruppen nennt man entsprechend *Hurwitz-Gruppen*. Diese Kurven werden durch torsionsfreie Normalteiler N in der Dreiecksgruppe $\Delta(2,3,7)$ uniformisiert, d.h. N ist ihre universelle Überlagerungsgruppe und die Kurven sind isomorph zu $N\backslash\mathfrak{U}$, wenn $\mathfrak{U}$ die obere Halbebene bezeichnet. Die Automorphismengruppen sind dann isomorph zu $\Delta(2,3,7)/N$.

Eine erste interessante unendliche Familie von Hurwitz-Gruppen wurde von Macbeath gefunden [M69]. Diese Gruppen sind alle isomorph zu $\mathrm{PSL}_2\mathbb{F}_q$, mit

(i) $q = 7$,
(ii) $q = p \equiv \pm 1 \bmod 7$,
(iii) $q = p^3$, $p \equiv \pm 2$ oder $\pm 3 \bmod 7$

für eine Primzahl p und es gibt keine anderen Werte q, für die $\mathrm{PSL}_2\mathbb{F}_q$ eine Hurwitz-Gruppe ist. Falls q vom Typ (i) oder (iii) ist, hat man nur eine zugehörige Riemannsche Fläche. Im Fall (ii) erhält man drei nicht-isomorphe Kurven mit der gleichen Automorphismengruppe. In einer Arbeit von Streit [St00] wird gezeigt, dass diese drei Kurven einen Orbit unter der Operation der absoluten Galoisgruppe bilden.

Quasiplatonische Kurven sind in gewisser Weise eine Verallgemeinerung der Hurwitz-Kurven. Im Modulraum bilden die Hurwitz-Kurven die absoluten Maxima bzgl. der Größe der Automorphismengruppe, die quasiplatonischen Kurven die lokalen Maxima. Vom Standpunkt der Uniformisierung aus gesehen ersetzt man die Gruppe $\Delta(2,3,7)$ durch eine beliebige andere Dreiecksgruppe. Inwiefern lassen sich obige Resultate über Galoiskonjugiertheit bei den Hurwitz-Kurven auf quasiplatonische Kurven mit einer Automorphismengruppe isomorph zu $\mathrm{PSL}_2\mathbb{F}_q$ übertragen?

Betrachtet man den Spurkörper E einer Dreiecksgruppe, so hat man eine Operation von $\mathrm{Gal}\,(E/\mathbb{Q})$ auf den Primidealen der Körpererweiterung. Gibt es einen Zusammenhang zwischen dieser Operation und der oben erwähnten Galoisoperation auf den Kurven? Schmidt und Smith [SS] betrachten Kurven, die durch Hauptkongruenzuntergruppen von Heckegruppen zu einem Primideal in einem Kreisteilungskörper uniformisiert werden. Diese Kurven bilden nicht nur einen Galoisorbit, die Operation der Galoisgruppe auf den Kurven stimmt auch mit der Operation auf den Primidealen überein. Kann man eine ähnliche Korrespondenz bei Hurwitz-Kurven bzw. quasiplatonischen Kurven wiederfinden?

Die Elemente mit Norm 1 in einer Ordnung einer Quaternionenalgebra, definiert über einem algebraischen Zahlkörper F, bilden eine arithmetische Gruppe. Erfüllt die Quaternionenalgebra ein gewisses Verzweigungsverhalten, dann erhält man sogar eine arithmetische Fuchssche Gruppe. In [D] zeigt Džambić, dass der Quotient einer solchen Gruppe nach einer Hauptkongruenzuntergruppe isomorph ist zu $\mathrm{PSL}_2\mathbb{F}_q$, wobei $\mathbb{F}_q$ der Restklassenkörper der Erweiterung $F/\mathbb{Q}$ bzgl. einem Primideal über der Charakteristik von $\mathbb{F}_q$ ist. Über $F = \mathbb{Q}(\cos(2\pi/7))$ kann man eine Quaternionenalgebra definieren, aus der man die arithmetische Fuchssche Gruppe $\Delta(2,3,7)$ erhält. In [D] wird außerdem gezeigt, dass man dann als Quotient nach den Hauptkongruenzuntergruppen gerade die Gruppen von Macbeath erhält. Offen bleibt die Frage, ob bzw. warum die Galoiskonjugation auf den Kurven und den Idealen übereinstimmt und ob eine Verallgemeinerung auf andere, unter Umständen sogar nicht-arithmetische, Dreiecksgruppen möglich ist.

In dieser Arbeit versuchen wir diese Fragen so weit wie möglich zu beantworten.

Der erste Teil der Arbeit befasst sich mit quasiplatonischen Riemannschen Flächen, die $\mathrm{PSL}_2\mathbb{F}_q$ als Automorphismengruppe besitzen, und deren Verhalten unter der Galoisoperation. In den ersten vier Abschnitten werden zunächst die dazu benötigten Werkzeuge vorgestellt.

In Abschnitt 1.1 werden die wichtigsten Fakten zusammengestellt, die wir über $\mathrm{PSL}_2\mathbb{F}_q$ benötigen.

Abschnitt 1.2 widmet sich der Frage, wann zwei Elemente g_0, g_1 aus $\mathrm{PSL}_2\mathbb{F}_q$ die ganze Gruppe erzeugen. Ist dies möglich, dann erhalten wir eine Projektion einer Dreiecksgruppe $\Delta(m_0, m_1, m_\infty)$ auf $\mathrm{PSL}_2\mathbb{F}_q$ mit $m_i = \mathrm{ord}\, g_i$, wobei $g_\infty = (g_0 g_1)^{-1}$. Die Resultate sind entweder bei [M69] oder [F] bewiesen. Ähnliche Ergebnisse findet man auch in [S].

In 1.3 betrachten wir den Spurkörper einer solchen Dreiecksgruppe, also die Körpererweiterung, die durch Adjungieren der Spuren von Elementen aus Δ an $\mathbb{Q}$ entsteht. Spurkörper zu Fuchsschen oder Kleinschen Gruppen

werden ausführlich in [MR] behandelt.

In Abschnitt 1.4 werden die Projektionen $\Delta \twoheadrightarrow \mathrm{PSL}_2\mathbb{F}_q$ mit unterschiedlichen Kernen gezählt, indem wir die Kerne durch die verschiedenen Spurtupel von g_0, g_1, g_∞ beschreiben, wobei hier die Spuren eines Tripels in $\mathrm{SL}_2\mathbb{F}_q$ mit $g_0 g_1 g_\infty = 1$ betrachtet werden, d.h. die Vorzeichen spielen hier eine Rolle. Genauer: Ändert man bei einer geraden Anzahl der $\operatorname{tr} g_i$ das Vorzeichen, so erhält man eine isomorphe Kurve; ändert man man das Vorzeichen bei einer ungeraden Anzahl, so erhält man eine nicht isomorphe Kurve. Die Vorzeichen spielen keine Rolle mehr, wenn eines der g_i Spur 0 hat. Diese Resultate findet man in [F].

In 1.5 geben wir eine Bedingung dafür an, dass verschiedene Kerne K in Δ auch zu verschiedenen Kurven $K\backslash\mathfrak{U}$ führen. Dabei werden Resultate in [GW] über den Konjugator zweier Dreiecksgruppen benutzt.

In Abschnitt 1.6 wird der Zusammenhang zwischen den Multiplikatoren und den Spuren eines Automorphismus beschrieben. Spielt das Vorzeichen bei den Spuren keine Rolle, dann kann man die verschiedenen Kerne/Kurven auch durch ein Tripel von Multiplikatoren beschreiben. Es zeigt sich, dass eine sorgfältige Analyse eines Beweises in [M73] zusammen mit den Eigenschaften von $\mathrm{PSL}_2\mathbb{F}_q$ aus dem ersten Abschnitt zu einer Verallgemeinerung des in [St00] zentralen Lemmas führt, so dass wir in 1.7 die Methoden von Streit zur Beschreibung der Galoisoperation auf unseren Kurven mit Hilfe der Multiplikatoren verwenden können. Spielt jedoch das Vorzeichen im Spurtupel eine Rolle, dann hat man zu einem Multiplikatortripel zwei verschiedene Kurven. Man kann die Galoisoperation in diesem Fall also nicht über das Verhalten der Multiplikatoren beschreiben.

Im zweiten Teil der Arbeit geht es um den Zusammenhang zwischen den Primidealen $\mathfrak{p}$ im Spurkörper über der Primzahl p und den verschiedenen Kurven in einer Galois-Bahn. Wir können nämlich die Kerne aus dem ersten Teil als Schnitt der Dreiecksgruppe mit einer Hauptkongruenzuntergruppe zu dem Ideal $\mathfrak{p}$ beschreiben. Es zeigt sich außerdem, dass die Galoisoperation auf den Kurven mit der Operation auf den Primidealen kompatibel ist. Die ersten drei Abschnitte dienen wieder einer Übersicht über die verwendeten Methoden.

In den Abschnitten 2.1 bzw. 2.2 werden die für uns wichtigen Fakten über Quaternionenalgebren bzw. Ordnungen in Quaternionenalgebren zusammengestellt. Mit Hilfe der allgemeinen Theorie über maximale Ordnungen in zentralen einfachen Algebren erhalten wir ein Reslutat, das die Rolle des Satzes aus [D] übernimmt.

In Abschnitt 2.3 ordnen wir einer Fuchsschen Gruppe eine Quaternionenalgebra über dem Spurkörper zu. Hier folgen wir der Darstellung in [MR].

In 2.4 werden Projektionen $\Delta \twoheadrightarrow \mathrm{PSL}_2\mathbb{F}_q$ über Quaternionenalgebren beschrieben. Der Kern einer solchen Projektion erweist sich als Schnitt der Dreiecksgruppe mit einer Hauptkongruenzuntergruppe zu einem Primideal $\mathfrak{p}$.

Im letzten Abschnitt wird die Korrespondenz zwischen der Galoisoperation auf den Primidealen und der Operation auf der Familie der entstehenden Kurven erklärt: Für jedes Primideal $\mathfrak{p}$ erhält man eine Projektion $\Delta \twoheadrightarrow \mathrm{PSL}_2\mathbb{F}_q$ über die Quaternionenalgebra von Δ. Das Spurtripel in $\mathrm{PSL}_2\mathbb{F}_q$ ist dabei gerade das Spurtripel aus Δ modulo $\mathfrak{p}$. Ändert man $\mathfrak{p}$, so erhält man ein anderes Spurtripel in $\mathrm{PSL}_2\mathbb{F}_q$, also auch einen anderen Kern.

Lassen sich die verschiedenen Kerne über die Tripel der Multiplikatoren beschreiben, dann ist die Galoisoperation auf diesen Tripeln, also die Galoisoperation auf den Kurven, verträglich mit der Operation, die die Primideale $\mathfrak{p} \mid \mathrm{char}\,\mathbb{F}_q$ permutiert.

Mein Dank gilt Herrn Prof. Dr. J. Wolfart für die Anregung zu dieser Arbeit und die Unterstützung während der vergangenen drei Jahre.

Inhaltsverzeichnis

Kapitel 1

Kerne und Kurven

1.1 $\mathrm{PSL}_2(\mathbb{F}_q)$

Sei p prim und $q = p^f$. Wir betrachten SL_2 bzw. PSL_2 über dem endlichen Körper mit q Elementen $\mathbb{F}_q$.

Definition 1.1.1. Sei $g \in \mathrm{SL}_2(\mathbb{F}_q)$ und $\chi_g(X) := X^2 - \mathrm{tr}\,(g)X + 1$ das charakteristische Polynom von g. Wir nennen g

parabolisch	$:\Leftrightarrow$	χ_g hat eine doppelte Nullstelle in $\mathbb{F}_q$,
hyperbolisch	$:\Leftrightarrow$	χ_g hat zwei verschiedene Nullstellen in $\mathbb{F}_q$,
elliptisch	$:\Leftrightarrow$	χ_g hat keine Nullstellen in $\mathbb{F}_q$.

Lemma 1.1.2. *Für alle $t \in \mathbb{F}_q^*$ gibt es eine Zerlegung $t = a + a^{-1}$, $a \in \mathbb{F}_{q^2}^*$, und diese ist eindeutig bis auf die Reihenfolge der Summanden.*

Beweis. Sei $t \in \mathbb{F}_q^*$. Die Gleichung $t = a+a^{-1}$ ist äquivalent zu $a^2-ta+1 = 0$. D.h. wir erhalten eine solche Zerlegung durch die Nullstellen des Polynoms X^2-tX+1. Da die Nullstellen durch das Polynom eindeutig bestimmt sind, ist auch die Zerlegung von t eindeutig. □

Korollar 1.1.3. $1 \neq g \in \mathrm{SL}_2(\mathbb{F}_q)$ *ist genau dann parabolisch, wenn* $\mathrm{tr}\, g = \pm 2$.

Beweis. Sei $\mathrm{tr}\, g = a + a^{-1}$. Dann sind a und a^{-1} die beiden Nullstellen von χ_g. Nach Voraussetzung hat χ_g eine doppelte Nullstelle, also $a = a^{-1}$ bzw. $a = \pm 1$ und somit $\mathrm{tr}\, g = \pm 2$. Umgekehrt hat $X^2 \mp 2X + 1 = (X \mp 1)^2$ eine doppelte Nullstelle. □

Bemerkung. Über gebrochen-lineare Transformationen lässt sich eine Operation von $\mathrm{PSL}_2(\mathbb{F}_q)$ auf $\mathrm{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ definieren, nämlich

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x := \frac{ax + b}{cx + d},$$

$a, b, c, d \in \mathbb{F}_q$, $ad - bc = 1$, $x \in \mathrm{P}^1(\mathbb{F}_q)$.

Diese Operation ist zweifach transitiv und ein Element $1 \neq g \in \mathrm{SL}_2(\mathbb{F}_q)$ ist genau dann parabolisch/hyperbolisch/elliptisch, wenn das zughörige Element $\overline{g} \in \mathrm{PSL}_2(\mathbb{F}_q)$ genau einen/genau zwei/keinen Fixpunkt in $\mathrm{P}^1(\mathbb{F}_q)$ besitzt. Des weiteren hat man folgende Normalformen:

Lemma 1.1.4. *Sei $1 \neq g \in \mathrm{SL}_2(\mathbb{F}_q)$. Dann gilt:*

- *Ist g parabolisch, dann ist g konjugiert zu $\pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, für ein $b \in \mathbb{F}_q^*$.*
- *Ist g hyperbolisch, dann ist g konjugiert zu $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, $a \neq 0, \pm 1$.*
- *Ist g elliptisch, dann ist g über $\mathbb{F}_{q^2}$ konjugiert zu $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$, mit $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Ist $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dann ist $bc \neq 0$.*

Satz 1.1.5. *Ist $p \neq 2$, dann zerfallen die parabolischen Elemente aus $\mathrm{SL}_2(\mathbb{F}_q)$ mit Spur 2 in drei Konjugationsklassen, nämlich die der Einheitsmatrix und den beiden Klassen, die repräsentiert werden durch*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

wobei a ein Nichtquadrat in $\mathbb{F}_q$ ist. Entsprechend für parabolische Elemente mit Spur -2.

Ist $p = 2$, dann zerfallen die parabolischen Elemente in zwei Konjugationsklassen, nämlich die der Einheitsmatrix auf der einen und allen anderen Matrizen mit Spur 0 auf der anderen Seite.

Die Besonderheit für $p = 2$ liegt daran, dass die multiplikative Gruppe von $\mathbb{F}_{2^f}$ eine zyklische Gruppe ungerader Ordnung ist. Daher ist jedes Element ein Quadrat und besitzt genau eine Wurzel in $\mathbb{F}_{2^f}$.

Beweis. Sei $1 \neq g$ parabolisch mit Spur 2. Dann ist g konjugiert zu $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $x \neq 0$. Weiteres Konjugieren ergibt

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1 - acx & a^2 x \\ -cx^2 & 1 + acx \end{pmatrix}.$$

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ ist also nur zu oberen Dreiecksmatrizen der Form $\begin{pmatrix} 1 & a^2 x \\ 0 & 1 \end{pmatrix}$ konjugiert. □

Satz 1.1.6. *Zwei nicht-parabolische Elemente in* $\mathrm{SL}_2(\mathbb{F}_q)$ *sind genau dann konjugiert in* $\mathrm{SL}_2(\mathbb{F}_q)$*, wenn sie die gleiche Spur haben.*

Beweis. Sind $g, h \in \mathrm{SL}_2(\mathbb{F}_q)$ konjugiert, dann haben sie auch die gleiche Spur.

Seien g, h hyperbolisch mit $\mathrm{tr}\,(g) = a + a^{-1} = \mathrm{tr}\,(h)$. g und h sind konjugiert zu

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix},$$

und diese beiden Matrizen sind durch $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ konjugiert.

Sei $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ elliptisch mit $\mathrm{tr}\,(g) = a + d =: t$. Da $bc \neq 0$ können wir konjugieren mit:

$$\begin{pmatrix} c & -a \\ 0 & c^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} c^{-1} & a \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & -c \\ c^{-1} & t \end{pmatrix}.$$

Es genügt also zu zeigen, dass Matrizen der Form $\begin{pmatrix} 0 & -c \\ c^{-1} & t \end{pmatrix}$ für beliebige $c \in \mathbb{F}_q^*$ miteinander konjugiert sind. Wir konjugieren:

$$\begin{aligned} &\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 0 & -c \\ c^{-1} & t \end{pmatrix} \begin{pmatrix} w & -y \\ -z & x \end{pmatrix} \\ &= \begin{pmatrix} c^{-1}yw + cxz - tyz & -c(x^2 - t\frac{y}{c}x + (\frac{y}{c})^2) \\ c^{-1}w^2 + cz^2 - tzw & -c^{-1}yw - cxz + txw \end{pmatrix}. \end{aligned}$$

Setzt man $x = w^{-1}$, $y = 0 = z$ so erhält man

$$\begin{pmatrix} 0 & -cx^2 \\ c^{-1}x^{-2} & t \end{pmatrix}.$$

Ist $p = 2$, so durchläuft $-cx^2$, $x \in \mathbb{F}_q^*$ ganz $\mathbb{F}_q^*$ und wir sind fertig. Ist $p \neq 2$, so muss man sich noch überlegen, wie man in der Gegendiagonalen ein Nichtquadrat als Faktor von $-c$ bzw. c^{-1} bekommt: Wir betrachten das charakteristische Polynom

$$\chi_g(X) = \left(X - \frac{t}{2}\right)^2 - \frac{(t-2)(t+2)}{4}.$$

Im Bildraum $\chi_g(\mathbb{F}_q)$ gibt es ein Nichtquadrat. Denn ist $-(t-2)(t+2)/4 \in \mathbb{F}_q^*$ ein Quadrat, dann gibt es ein Quadrat $\alpha^2 \in \mathbb{F}_q^*$, so dass die Summe der beiden Elemente ein Nichtquadrat ist, und daher ist $\chi(\alpha + \frac{t}{2})$ kein Quadrat. Ist $-(t-2)(t+2)/4$ kein Quadrat, dann ist $\chi_g(\frac{t}{2})$ kein Quadrat.

Wir setzen also $y = c$ und wählen x so, dass $\chi_g(x)$ kein Quadrat ist. Schließlich bestimmt man z, w so, dass $w + zc(x - t) = 0$ und $xw - yz = 1$ erfüllt sind. Da g als elliptisch vorausgesetzt wurde, kann man die Gleichungen tatsächlich lösen. □

Korollar 1.1.7. *Sei $\pm 1 \neq g \in \mathrm{SL}_2(\mathbb{F}_q)$. Die Anzahl der zu g konjugierten Elemente beträgt:*

$(p,2)(q^2-1)/2$, *falls g parabolisch ist,*
$q(q+1)$, *falls g hyperbolisch ist,*
$q(q-1)$, *falls g elliptisch ist.*

Beweis. Sei g parabolisch und o.B.d.A. $\mathrm{tr}\,(g) = 2$. Wir zählen alle Elemente mit Spur 2, also alle $\begin{pmatrix} a & b \\ c & 2-a \end{pmatrix}$ mit $2a - a^2 - bc = 1$ bzw. $-bc = (a-1)^2$. Wir haben die Wahlmöglichkeiten

$$(a = 1 \text{ und } bc = 0) \quad \text{oder} \quad (a \neq 1 \text{ und } bc \in \mathbb{F}_q^*).$$

Das ergibt

$$1 \cdot (1 + 2(q-1)) + (q-1) \cdot (q-1) = q^2$$

Elemente mit Spur 2. Davon müssen wir 1 für die Identität abziehen und im Fall $p \neq 2$ noch durch 2 teilen.

Jetzt sei g nicht parabolisch, d.h. $\mathrm{tr}\,(g) := t \neq \pm 2$. Wir zählen alle Elemente mit Spur t, also $\begin{pmatrix} a & b \\ c & t-a \end{pmatrix}$ mit $at - a^2 - bc = 1$ bzw. $-bc = a^2 - ta + 1 = \chi_g(a)$.

Ist g hyperbolisch, dann seien x, x^{-1} mit $t = x + x^{-1}$ die beiden Nullstellen von χ_g. Wir haben dann die Wahlmöglichkeiten

$$(a = x, x^{-1} \text{ und } bc = 0) \quad \text{oder} \quad (a \neq x, x^{-1} \text{ und } bc \in \mathbb{F}_q^*).$$

Das ergibt

$$2 \cdot (1 + 2(q-1)) + (q-2) \cdot (q-1) = q(q+1)$$

Elemente mit Spur t.

Ist g elliptisch, dann ist $\chi_g(a) \neq 0$ für alle $a \in \mathbb{F}_q$. Wir können also $a \in \mathbb{F}_q$ und $b \in \mathbb{F}_q^*$ beliebig wählen. Dann ist c über die Determinante bestimmt und wir haben $q(q-1)$ Elemente mit Spur t. □

Korollar 1.1.8 (vgl. [M73])**.** *Sei $\pm 1 \neq g \in \mathrm{SL}_2(\mathbb{F}_q)$ und $\overline{g}$ sei das zugehörige Element aus $\mathrm{PSL}_2(\mathbb{F}_q)$. Dann ist die Anzahl der Elemente im Normalisator von $\langle \overline{g} \rangle$ in $\mathrm{PSL}_2(\mathbb{F}_q)$ gleich:*

$(pf,2)\,q\,(p-1)/2$, *falls g parabolisch ist,*
$(p,2)\,(q-1)$, *falls g hyperbolisch ist,*
$(p,2)\,(q+1)$, *falls g elliptisch ist.*

Beweis. Die Anzahl der Elemente im Normalisator von $\langle\overline{g}\rangle$ ist gleich dem Produkt der Anzahl von Elementen in $\langle\overline{g}\rangle$, zu denen g konjugiert ist mit der Anzahl von Elementen, die g unter Konjugation fix lassen.

Sei g parabolisch und o.B.d.A. konjugiert zu $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Dann ist g konjugiert zu $(p-1)/2$ vielen Elementen g^k, wenn keine Quadratwurzel zu $\mathbb{F}_p$ adjungiert wurde, also wenn $2 \nmid f$ und $p \neq 2$. Hingegen ist g konjugiert zu $(p-1)$ vielen Elementen g^k, wenn eine Quadratwurzel zu $\mathbb{F}_p$ adjungiert wurde, also wenn $2 \mid f$ oder $p = 2$.

$\mathrm{PSL}_2(\mathbb{F}_q)$ operiert durch Konjugation auf sich. Die Länge der Bahnen unter dieser Operation haben wir in Korollar 1.1.7 berechnet. Die Gruppenordnung beträgt

$$|\mathrm{PSL}_2(\mathbb{F}_q)| = (p,2)(q-1)q(q+1)/2.$$

Damit erhalten wir für die Ordnung des Stabilisators von g

$$|\mathrm{Stab}\, g| = q.$$

Für die Ordnung des Normalisators folgt daraus obige Formel.

Ist g hyperbolisch/elliptisch, dann ist g nur zu den beiden g-Potenzen g und g^{-1} konjugiert. Für die Ordnung des Stabilisators folgt

$$|\mathrm{Stab}\, g| = (p,2)(q \mp 1)/2,$$

und damit die Formeln für die Ordnung des Normalisators. □

Satz 1.1.9. *Sei* $\pm 1 \neq g \in \mathrm{SL}_2(\mathbb{F}_q)$ *und* $\overline{g}$ *das entsprechende Element aus* $\mathrm{PSL}_2(\mathbb{F}_q)$ *mit* $n = \mathrm{ord}\,\overline{g}$. *Dann gilt:*

g *ist parabolisch*	$\Leftrightarrow$	$p = n$.	
g *ist hyperbolisch*	$\Leftrightarrow$	$q \equiv 1 \bmod 2n$	*bzw.* mod n, *falls* $p = 2$.
g *ist elliptisch*	$\Leftrightarrow$	$q \equiv -1 \bmod 2n$	*bzw.* mod n, *falls* $p = 2$.

Beweis. Sei g parabolisch. g ist konjugiert zu $\pm\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $b \neq 0$, und damit $\mathrm{ord}(\overline{g}) = \mathrm{char}\,\mathbb{F}_q = p$.

Sei g hyperbolisch, d.h. konjugiert zu $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Ist $n \equiv 1\,(2)$, dann sei $a = \zeta_n$ o.B.d.A. eine primitive n-te Einheitswurzel und $\zeta_n \in \mathbb{F}_q$, d.h. $\zeta_n^q = \zeta_n$, also $q \equiv 1\,(n)$. Da $(2,n) = 1$, gilt sogar $q \equiv 1\,(2n)$, sofern $p \neq 2$. Ist $n \equiv 0\,(2)$, $p \neq 2$, dann ist $a = \zeta_{2n}$ eine primitive $2n$-te Einheitswurzel, und wie oben folgt $q \equiv 1\,(2n)$. Im Fall $p = 2$ ist a eine primitive n-te Einheitswurzel.

Sei schließlich g elliptisch. In $\mathrm{SL}_2(\mathbb{F}_{q^2})$ ist g hyperbolisch, d.h. dort ist g konjugiert zu einer Matrix $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ mit einer n-ten (bzw. $2n$-ten Einheitswurzel) $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, also mit $\alpha^q \neq \alpha$. Andererseits liegt die Spur in $\mathbb{F}_q$, d.h. $(\alpha + \alpha^{-1})^q = \alpha^q + \alpha^{-q} = \alpha + \alpha^{-1}$. Mit Lemma 1.1.2 folgt daraus $\alpha^q = \alpha^{-1}$, also $q \equiv -1 \bmod n$ (bzw. $2n$). □

1.2 Erzeugende von $\mathrm{PSL}_2(\mathbb{F}_q)$

Sei p prim und q eine p-Potenz. In $G := \mathrm{PSL}_2(\mathbb{F}_q)$ wollen wir nun solche Tripel von Elementen (g_0, g_1, g_∞) mit $g_0 g_1 g_\infty = 1$ betrachten, die ganz G erzeugen. Ist $m_i = \mathrm{ord}\,(g_i)$, dann kann man eine Abbildung der Dreiecksgruppe

$$\Delta = \Delta(m_0, m_1, m_\infty) = \langle \gamma_0, \gamma_1, \gamma_\infty \mid \gamma_0^{m_0} = \gamma_1^{m_1} = \gamma_\infty^{m_\infty} = \gamma_0\gamma_1\gamma_\infty = 1 \rangle$$

auf G mit torsionsfreiem Kern durch $\gamma_i \mapsto g_i$ definieren.

Unter welchen Bedingungen ganz G erzeugt wird, und wie viele verschiedene torsionsfreie Kerne es bei Projektionen von Δ auf G gibt, ist Gegenstand der Arbeiten [M69] und [F]. Wir wollen die für uns relevanten Ergebnisse hier noch einmal zusammenstellen.

Definition 1.2.1. Ein $\mathrm{SL}_2(\mathbb{F}_q)$-*Tripel* ist ein geordnetes Tripel (g_0, g_1, g_∞) von Elementen $g_0, g_1, g_\infty \in \mathrm{SL}_2(\mathbb{F}_q)$, das die Bedingung $g_0 g_1 g_\infty = 1$ erfüllt.

Ein *Spurtripel* ist ein Tripel von Elementen aus $\mathbb{F}_q$. (Tatsächlich gibt es zu jedem Tripel $(\tau_0, \tau_1, \tau_\infty) \in \mathbb{F}_q^3$ ein $\mathrm{SL}_2(\mathbb{F}_q)$-Tripel, dessen Elemente die Spuren $\tau_0, \tau_1, \tau_\infty$ besitzen. [M69], Theorem 1)

Ein *Ordnungstripel* ist ein Tripel bestehend aus drei natürlichen Zahlen (m_0, m_1, m_∞), die die Ordnungen von g_0, g_1, g_∞ aus dem $\mathrm{SL}_2(\mathbb{F}_q)$-Tripel in $\mathrm{PSL}_2(\mathbb{F}_q)$ angeben.

Definition 1.2.2. Ein $\mathrm{SL}_2(\mathbb{F}_q)$-Tripel (g_0, g_1, g_∞) heißt *singulär*, wenn die dem zugehörigen Spurtripel $(\tau_0, \tau_1, \tau_\infty)$ zugeordnete quadratische Form

$$Q_{\tau_0,\tau_1,\tau_\infty}(x, y, z) := x^2 + y^2 + z^2 + \tau_0 yz + \tau_1 xz + \tau_\infty xy$$

singulär ist. Damit ist in diesem Zusammenhang eine quadratische Form gemeint, bei der die Matrix der zugehörigen Bilinearform Rang 1 hat, bzw. eine Form, die sich zerlegen lässt als

$$Q_{\tau_0,\tau_1,\tau_\infty}(x, y, z) = (x + vy + uz)(x + v^{-1}y + u^{-1}z),$$

mit u, v im algebraischen Abschluss von $\mathbb{F}_q$.

Ein Ordnungstripel heißt singulär, wenn ein singuläres $\mathrm{SL}_2(\mathbb{F}_q)$-Tripel mit den entsprechenden Ordnungen existiert.

Für die singulären Tripel gilt:

Satz 1.2.3 ([M69], Theorem 2)**.** *Ein* $\mathrm{SL}_2(\mathbb{F}_q)$*-Tripel ist genau dann singulär, wenn es in* $\mathrm{PSL}_2(\mathbb{F}_q)$ *eine Untergruppe erzeugt, die konjugiert ist zu einer Untergruppe der oberen Dreiecksmatrizen oder über* $\mathbb{F}_{q^2}$ *konjugiert ist zu einer Untergruppe von* $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$, ζ *eine* $(q+1)$*te Einheitswurzel in* $\mathbb{F}_{q^2}$*.*

Eine weitere Sorte von Untergruppen in $\mathrm{PSL}_2(\mathbb{F}_q)$ sind die endlichen Dreiecksgruppen, also Untergruppen die isomorph zu $\Delta(m_0, m_1, m_\infty)$ sind mit

$$\frac{1}{m_0} + \frac{1}{m_1} + \frac{1}{m_\infty} > 1.$$

M.a.W. Untergruppen isomorph zu:

$(2,2,n)$		Diedergruppe des n-Ecks
$(2,3,3)$	$\cong A_4 \cong \mathrm{PSL}_2\mathbb{F}_3$	Tetraedergruppe
$(2,3,4)$	$\cong S_4$	Oktaedergruppe
$(2,3,5)$	$\cong A_5 \cong \mathrm{PSL}_2\mathbb{F}_4 \cong \mathrm{PSL}_2\mathbb{F}_5$	Ikosaedergruppe

Es gilt

Satz 1.2.4 ([M69], 8.)**.** *Ein* $\mathrm{SL}_2(\mathbb{F}_q)$*-Tripel, das eine endliche Dreiecksgruppe erzeugt, besitzt ein Ordnungstripel aus der Liste*

$$(2,2,n)\ n \in \mathbb{N}, (2,3,3), (3,3,3), (3,4,4), (2,3,4), (2,5,5)$$
$$(5,5,5), (3,3,5), (3,5,5), (2,3,5)$$

Ordnungstripel dieser Form nennen wir Ausnahmetripel*.*

In [Di], Abschnitt 260, werden alle Untergruppen von $\mathrm{PSL}_2(\mathbb{F}_q)$ klassifiziert. Die einzigen Untergruppen, die nicht zu singulären und/oder Ausnahmetripeln gehören, sind Untergruppen konjugiert zu $\mathrm{PSL}_2(k)$ oder $\mathrm{PGL}_2(k)$ mit $k \leq \mathbb{F}_q$. Daraus folgt

Satz 1.2.5 ([M69], Theorem 4)**.** *Ein* $\mathrm{PSL}_2(\mathbb{F}_q)$*-Tripel, das weder ein Ausnahmetripel noch singulär ist, erzeugt eine projektive Untergruppe von* $\mathrm{PSL}_2(\mathbb{F}_q)$*; genauer:*

Ist das Spurtripel $(\tau_0, \tau_1, \tau_\infty)$ *nicht singulär und gehört nicht zu einem Ausnahmetripel, dann sind die von* $\mathrm{SL}_2(\mathbb{F}_q)$*-Tripeln mit Spuren* $\tau_0, \tau_1, \tau_\infty$ *erzeugten Untergruppen in* $\mathrm{PSL}_2(\mathbb{F}_q)$ *isomorph zu*

$$\mathrm{PSL}_2(k) \quad \text{oder} \quad \mathrm{PGL}_2(k_0),$$

wobei k *der Körper* $\mathbb{F}_p(\tau_0, \tau_1, \tau_\infty)$ *und* $k_0 \leq k$ *ein Unterkörper mit* $|k : k_0| \geq 2$ *ist.*

Definition 1.2.6. Wir wollen ein Ordnungstripel (m_0, m_1, m_∞) *p-zulässig* nennen, wenn die m_i teilerfremd zu oder gleich p sind und wenn (m_0, m_1, m_∞) nicht singulär und kein Ausnahmetripel ist.

Der Körper $k = \mathbb{F}_p(\tau_0, \tau_1, \tau_\infty)$ lässt sich noch etwas genauer bestimmen. Es gilt

Satz 1.2.7 ([F], Korollar 2.4)**.** *Sei (g_0, g_1, g_∞) ein $\mathrm{SL}_2(\mathbb{F}_q)$-Tripel mit p-zulässigem Ordnungstripel (m_0, m_1, m_∞). Dann ist der zugehörige Spurkörper gleich*

$$\mathbb{F}_p(\tau_0, \tau_1, \tau_\infty) = \mathbb{F}_{p^f}$$

mit $f = \mathrm{kgV}(f_0, f_1, f_\infty)$, wobei

$$f_i = \begin{cases} 1, & \text{falls } m_i = p \\ f_i \text{ ist minimal mit } p^{f_i} \equiv \pm 1 \bmod 2m_i, & \text{falls } m_i \neq p \neq 2 \\ f_i \text{ ist minimal mit } p^{f_i} \equiv \pm 1 \bmod m_i, & \text{falls } m_i \neq p = 2 \end{cases}$$

Bemerkung. Wählt man für $q = p^f$ ein p-zulässiges SL_2-Tripel so, dass für die Spuren $\mathbb{F}_p(\tau_0, \tau_1, \tau_\infty) = \mathbb{F}_q$ gilt, dann erzeugt das Tripel in PSL_2 entweder $\mathrm{PSL}_2(\mathbb{F}_q)$ oder $\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$.

Wir wollen jetzt noch zwischen Tupeln, die $\mathrm{PSL}_2(\mathbb{F}_q)$ bzw. $\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$ erzeugen, unterscheiden. Es ist

$$\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\pm E_2 \leq \mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\mathbb{F}_q^* \cdot E_2.$$

Können wir aus q die Wurzel ziehen, dann finden wir auch $\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$ in $\mathrm{PSL}_2(\mathbb{F}_q)$ wieder: Zu einem beliebigen $g \in \mathrm{GL}_2(\mathbb{F}_{\sqrt{q}})$ mit $\det g = \delta \neq 0$ ist $\sqrt{\delta}^{-1} g$ der zugehörige Repräsentant in PGL_2 mit Determinante 1, d.h. g lässt sich als Element einer PSL_2 auffassen, wenn man aus δ die Wurzel ziehen kann.

An der Determinante kann man auch ablesen, dass das Produkt von $g, h \in \mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}}) \setminus \mathrm{PSL}_2(\mathbb{F}_{\sqrt{q}})$ in $\mathrm{PSL}_2(\mathbb{F}_{\sqrt{q}})$ liegt, denn das Produkt zweier Nichtquadrate ist wieder ein Quadrat.

Die Spur von g, aufgefasst als Element in $\mathrm{PSL}_2(\mathbb{F}_q)$, ist $\sqrt{\delta}^{-1} \mathrm{tr}\, g = \sqrt{\delta^{-1} \mathrm{tr}^2 g}$, liegt also in $\mathbb{F}_{\sqrt{q}}$, wenn $g \in \mathrm{PSL}_2(\mathbb{F}_{\sqrt{q}})$, und ist die Wurzel eines Nichtquadrats in $\mathbb{F}_{\sqrt{q}}$ oder 0, wenn $g \in \mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}}) \setminus \mathrm{PSL}_2(\mathbb{F}_{\sqrt{q}})$.

Sei nun $k = \mathbb{F}_q$ der Spurkörper des p-zulässigen Tripels $g_0, g_1, g_\infty \in \mathrm{PSL}_2(\mathbb{F}_q)$ und k sei quadratische Erweiterung eines Unterkörpers $k_0 \leq k$. Wenn g_0, g_1, g_∞ nicht $\mathrm{PSL}_2(k)$ sondern $\mathrm{PGL}_2(k_0)$ erzeugen, dann müssen also genau zwei der Erzeugenden aus $\mathrm{PGL}_2(k_0)$ und das dritte Element aus $\mathrm{PSL}_2(k_0)$ sein. Das motiviert die folgende

Definition 1.2.8. Ein Spurtripel $(\tau_0, \tau_1, \tau_\infty)$ heißt *irregulär*, wenn der Körper $k = \mathbb{F}_p(\tau_0, \tau_1, \tau_\infty)$ quadratische Erweiterung eines Unterkörpers k_0 ist, und wenn ein Element des Tripels in k_0 liegt, wohingegen die anderen beiden Elemente des Tripels Wurzeln in k von Nichtquadraten aus k_0 oder 0 sind.

Ist $g \in \mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}}) \setminus \mathrm{PSL}_2(\mathbb{F}_{\sqrt{q}})$, dann hat g gerade Ordnung, denn andernfalls wäre $\langle g \rangle$ eine zyklische Gruppe ungerader Ordnung, d.h. es gäbe ein $g' \in \langle g \rangle$ mit $g'^2 = g$ und $\det g = (\det g')^2$ wäre ein Quadrat in $\mathbb{F}_{\sqrt{q}}$. Das zeigt die eine Richtung von

Satz 1.2.9 ([F], Satz 3.2)**.** *Sei $p \neq 2$ und das Ordnungstripel (m_0, m_1, m_∞) zu dem SL_2-Tripel (g_0, g_1, g_∞) mit Spurtripel $(\tau_0, \tau_1, \tau_\infty)$ sei p-zulässig. Außerdem sei $k = \mathbb{F}_p(\tau_0, \tau_1, \tau_\infty) = \mathbb{F}_{p^f}$, f gerade und k_0 der Unterkörper $\mathbb{F}_{p^{f/2}}$.*

Die von (g_0, g_1, g_∞) erzeugte Untergruppe ist isomorph zu $\mathrm{PGL}_2(k_0)$ genau dann, wenn o.B.d.A. m_0, m_1 gerade sind, $\tau_\infty \in k_0$ ist und entweder

- *$m_0 = 2$ und $\tau_1 \notin k_0$ oder*
- *$m_0, m_1, m_\infty \neq 2$ und $\tau_0, \tau_1 \notin k_0$*

gilt.

Außerdem folgt:

Satz 1.2.10 ([M69], Theorem 5)**.** *Ein $\mathrm{SL}_2(\mathbb{F}_q)$-Tripel, das nicht singulär, kein Ausnahmetripel und nicht irregulär ist, erzeugt in $\mathrm{PSL}_2(\mathbb{F}_q)$ eine Gruppe isomorph zu $\mathrm{PSL}_2(k)$, wobei k der von den Spuren über $\mathbb{F}_p$ erzeugte Körper ist.*

1.3 Spurkörper

Wir interessieren uns für Abbildungen von einer (Fuchsschen) Dreiecksgruppe $\Delta = \Delta(m_0, m_1, m_\infty)$ nach $\mathrm{PSL}_2(\mathbb{F}_q)$ und wollen uns nun dem Spurkörper von Δ zuwenden.

Definition 1.3.1. Sei $\Gamma \leq \mathrm{PSL}_2(\mathbb{R})$ eine nicht-elementare Untergruppe, dann nennen wir

$$\mathbb{Q}(\mathrm{tr}\,\Gamma) = \mathbb{Q}(\pm \mathrm{tr}\,\gamma \mid \gamma \in \Gamma)$$

den *Spurkörper* von Γ.

Bemerkung. $\mathbb{Q}(\mathrm{tr}\,\Gamma)$ ist zwar invariant unter Konjugation in $\mathrm{PSL}_2(\mathbb{R})$, im allgemeinen ist $\mathbb{Q}(\mathrm{tr}\,\Gamma)$ jedoch keine Invariante der Kommensurabilitätsklasse

in $\mathrm{PSL}_2(\mathbb{R})$. Möchte man den Spurkörper als Invariante der Kommensurabilitätsklasse von Γ definieren, so muss man zu

$$\mathbb{Q}(\operatorname{tr}\Gamma^{(2)}), \quad \text{mit } \Gamma^{(2)} = \left\langle \gamma^2 \mid \gamma \in \Gamma \right\rangle$$

übergehen (siehe [MR], Theorem 3.3.4).

Ist Γ endlich erzeugt, so lässt sich der Spurkörper aus den Spuren der Erzeugenden bestimmen. Es gilt nämlich:

Lemma 1.3.2 ([MR], 3.5.1)**.** *Sei* $\Gamma = \langle \gamma_1, \ldots, \gamma_n \rangle$ *und* $\gamma \in \Gamma$*. Dann ist* $\operatorname{tr}\gamma$ *enthalten in*

$$\mathbb{Z}[\{\operatorname{tr}(\gamma_{i_1} \cdots \gamma_{i_r}) \mid r \geq 1 \text{ und } 1 \leq i_1 < \cdots < i_r \leq n\}]$$

Korollar 1.3.3. *Für* $\Gamma = \langle \gamma_0, \gamma_1 \rangle$ *ist der Spurkörper*

$$\mathbb{Q}(\operatorname{tr}\Gamma) = \mathbb{Q}(\operatorname{tr}\gamma_0, \operatorname{tr}\gamma_1, \operatorname{tr}\gamma_0\gamma_1).$$

Für den Spurkörper einer Dreiecksgruppe $\Delta = \Delta(m_0, m_1, m_\infty)$ gilt somit

$$\mathbb{Q}(\operatorname{tr}\Delta) = \mathbb{Q}(\cos\tfrac{\pi}{m_0}, \cos\tfrac{\pi}{m_1}, \cos\tfrac{\pi}{m_\infty}).$$

Der invariante Spurkörper lässt sich auch aus den Spuren der Erzeugenden bestimmen (siehe [MR], 3.5.7) und für Δ gilt:

$$\mathbb{Q}(\operatorname{tr}\Delta^{(2)}) = \mathbb{Q}(\cos\tfrac{2\pi}{m_0}, \cos\tfrac{2\pi}{m_1}, \cos\tfrac{2\pi}{m_\infty}, \cos\tfrac{\pi}{m_0}\cos\tfrac{\pi}{m_1}\cos\tfrac{\pi}{m_\infty}).$$

Wir wollen nun noch das Zerfällungsverhalten von Primidealen in diesen Zahlkörpern genauer untersuchen.

1.3.1 Kreisteilungskörper

Dazu bezeichne ζ im folgenden immer eine primitive Einheitswurzel. Das Zerfällungsverhalten von Primzahlen in $\mathbb{Q}(\zeta)$ wird ausführlich behandelt in [Wa] oder [N]. Die für uns wichtigsten Fakten sind.

Satz 1.3.4 ([N], (10.2))**.** *Der Ring der ganzen Zahlen in* $\mathbb{Q}(\zeta)$ *ist* $\mathbb{Z}[\zeta]$.

Lemma 1.3.5 ([N], (10.1))**.** *Sei* $n = p^m$*,* p *prim und* $\lambda = 1 - \zeta$*. Dann ist das Hauptideal* (λ) *in* $\mathbb{Z}[\zeta]$ *ein Primideal vom Trägheitsgrad 1, und es gilt*

$$p\mathbb{Z}[\zeta] = (\lambda)^d, \text{ wobei } d = \varphi(p^m) = |\mathbb{Q}(\zeta) : \mathbb{Q}|.$$

Die Basis $1, \zeta, \ldots, \zeta^{d-1}$ *der Erweiterung hat die Diskriminante*

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm p^s, \text{ mit } s = p^{m-1}(mp - m - 1).$$

Satz 1.3.6 ([N], (10.3))**.** *Sei $n = \prod_p p^{\nu_p}$ die Primzerlegung von n und für jedes p sei f_p die kleinste natürliche Zahl, so dass*

$$p^{f_p} \equiv 1 \bmod n/p^{\nu_p}.$$

Dann zerlegt sich p in $\mathbb{Q}(\zeta)$ als

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})},$$

wobei die $\mathfrak{p}_i$ verschiedene Primideale von gleichem Trägheitsgrad f_p sind.

Der Beweis dieses Satzes liefert außerdem, dass die n-ten Einheitswurzeln mod $\mathfrak{p}$ verschieden sind, sofern $\mathfrak{p} \mid p$ und $p \nmid n$.

Schließlich hat man noch die folgenden Spezialfälle:

Satz 1.3.7 ([N], (10.4))**.** *Für eine Primzahl im n-ten Kreisteilungskörper gilt:*

- *p ist verzweigt $\Leftrightarrow p \mid n$; ausgenommen $p = 2 = (4, n)$.*
- *p ist vollzerlegt $\Leftrightarrow p \equiv 1 \bmod n$. (Die 2 ist somit nie vollzerlegt im n-ten Kreisteilungskörper.)*

Für den reellen Teil eines Kreisteilungskörpers ist die Situation ähnlich:

Satz 1.3.8 ([Wa], Prop. 2.16)**.** *Der Ring der ganzen Zahlen in $\mathbb{Q}(\zeta + \zeta^{-1})$ ist $\mathbb{Z}[\zeta + \zeta^{-1}]$.*

Satz 1.3.9 ([Wa], Prop. 2.15)**.** *Sei $n \not\equiv 2 \bmod 4$. Dann gelten:*

- *Ist $n = p^m$, dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})$ verzweigt in der einzigen Primstelle von $\mathbb{Q}(\zeta)$ über p und unverzweigt über allen anderen Primstellen.*
- *Ist n keine Primpotenz, dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})$ unverzweigt, d.h. alle Primstellen von $\mathbb{Q}(\zeta + \zeta^{-1})$ sind unverzweigt.*

Satz 1.3.7 nimmt bei $\mathbb{Q}(\zeta) \cap \mathbb{R}$ die folgende Gestalt an:

Satz 1.3.10. *Für eine Primzahl p in $\mathbb{Q}(\zeta + \zeta^{-1})$ gilt:*

- *p ist verzweigt $\Leftrightarrow p \mid n$; ausgenommen $p = 2 = (4, n)$.*
- *p ist vollzerlegt $\Leftrightarrow p \equiv \pm 1 \bmod n$.*

Beweis. • Ist p verzweigt in $\mathbb{Q}(\zeta+\zeta^{-1})$, dann auch in $\mathbb{Q}(\zeta)$ und es folgt $p \mid n$ mit Satz 1.3.7.

Gilt andererseits $p \mid n$ so betrachten wir zwei Fälle: Ist n eine Primzahlpotenz, also $n = p^m$, so findet eine Verzweigung nur über p statt und zwar nach Satz 1.3.5 mit Verzweigungsindex $\varphi(n) = |\mathbb{Q}(\zeta) : \mathbb{Q}|$. Der Verzweigungsindex in $\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}$ ist damit $\varphi(n)/2 > 1$. Ist n keine Primzahlpotenz, dann ist p in $\mathbb{Q}(\zeta)/\mathbb{Q}$ verzweigt, aber nach Satz 1.3.9 findet keine Verzweigung in $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})$ statt, d.h. die Verzweigung muss schon in $\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}$ stattgefunden haben.

- p ist vollzerlegt, wenn entweder

$$p \text{ vollzerlegt in } \mathbb{Q}(\zeta) \quad \Leftrightarrow \quad p \equiv 1 \bmod n$$

oder

$$\begin{array}{c} p \text{ vollzerlegt in } \mathbb{Q}(\zeta+\zeta^{-1}) \text{und der} \\ \text{Trägheitsgrad von } \mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1}) \text{ ist } 2 \end{array} \overset{(*)}{\Leftrightarrow} \quad p \equiv -1 \bmod n$$

gilt. Zu zeigen bleibt $(*)$.

Sei zunächst der Trägheitsgrad von $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})$ gleich 2. Der Restklassenkörper von $\mathbb{Q}(\zeta+\zeta^{-1})$ ist $\mathbb{F}_p$, d.h. $\zeta^p + \zeta^{-p} \equiv \zeta + \zeta^{-1}$ modulo $\mathfrak{p}$. Die Zerlegung von $a \in \mathbb{F}_p^*$ als $a = \alpha + \alpha^{-1}$ ist eindeutig bis auf Reihenfolge, da α, α^{-1} die Nullstellen des Polynoms $X^2 - aX + 1$ sind. Es folgt $\zeta = \zeta^p$ oder $\zeta = \zeta^{-p}$ modulo $\mathfrak{p}$. Da der Restklassenkörper von $\mathbb{Q}(\zeta)$ isomorph zu $\mathbb{F}_{p^2}$ ist, ist $\zeta \not\equiv \zeta^p$ und es bleibt nur $\zeta \equiv \zeta^{-p}$ bzw. $\zeta^{-1} \equiv \zeta^p$, also $p \equiv -1 \bmod n$.

Ist andererseits $p \equiv -1 \bmod n$, so ist $p^2 \equiv 1 \bmod n$ und 2 ist minimal bzgl. dieser Eigenschaft, d.h. nach Satz 1.3.6 ist der Trägheitsgrad von $\mathbb{Q}(\zeta)/\mathbb{Q}$ gleich 2. Des weiteren folgt aus $p \equiv -1\ (n)$, dass modulo $\mathfrak{p}$ gilt: $(\zeta+\zeta^{-1})^p = \zeta^p + \zeta^{-p} = \zeta^{-1} + \zeta$, d.h. $\zeta + \zeta^{-1} \in \mathbb{F}_p$ und der Trägheitsgrad von $\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}$ ist folglich 1. □

Korollar 1.3.11. *Sei $\eta_{n_i} := \zeta_{n_i} + \zeta_{n_i}^{-1}$, dann gilt:*

$$p \text{ ist vollzerlegt in } \mathbb{Q}(\eta_{n_1}, \ldots, \eta_{n_k}) \ \Leftrightarrow\ p \equiv \pm 1 \bmod n_i \text{ für } 1 \le i \le k.$$

Beweis. „⇒“ folgt aus obigem Satz, da p insbesondere vollzerlegt in jedem Zwischenkörper $\mathbb{Q}(\eta_{n_i})$ ist.

„⇐“: Da $p \nmid n_i$, ist p unverzweigt in $\mathbb{Q}(\zeta_{n_1 \cdots n_k})$, also erst recht im Zwischenkörper $\mathbb{Q}(\eta_{n_1}, \ldots, \eta_{n_k})$. Wie im Beweis oben folgt $(\eta_{n_i})^p \equiv \eta_{n_i}$, d.h. $\eta_{n_i} \in \mathbb{F}_p$ und der Trägheitsgrad ist somit gleich 1. □

Allgemeiner gilt

Satz 1.3.12. *p sei kein Teiler von n. Der Trägheitsgrad von p in $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ ist das minimale f mit*

$$p^f \equiv \pm 1 \bmod n$$

Beweis. Der Restklassenkörper ist $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]/\mathfrak{p} \cong \mathbb{F}_p(\zeta_n + \zeta_n^{-1})$ und der Trägheitsgrad ist $f = |\mathbb{F}_p(\zeta_n + \zeta_n^{-1})/\mathbb{F}_p|$, d.h. f ist minimal mit $x^{p^f} = x$ für alle $x \in \mathbb{F}_p(\zeta_n+\zeta_n^{-1})$. M.a.W. f ist minimal mit $(\zeta_n+\zeta_n^{-1})^{p^f} = \zeta_n+\zeta_n^{-1} \bmod \mathfrak{p}$ bzw. mit $\zeta_n^{p^f} = \zeta_n$ oder $\zeta_n^{p^f} = \zeta_n^{-1}$. □

1.3.2 Spurkörper einer Dreiecksgruppe

Wir wollen nun die Ergebnisse auf den Spurkörper

$$E := \mathbb{Q}(\cos\tfrac{\pi}{m_0}, \cos\tfrac{\pi}{m_1}, \cos\tfrac{\pi}{m_\infty})$$

einer Dreiecksgruppe mit Signatur (m_0, m_1, m_∞) anwenden. Dabei erweist es sich als nützlich, zunächst den Körper

$$F := \mathbb{Q}(\cos\tfrac{2\pi}{m_0}, \cos\tfrac{2\pi}{m_1}, \cos\tfrac{2\pi}{m_\infty})$$

zu betrachten. Zunächst einmal gilt für Galois-Erweiterungen $L, L' \geq K$

$$|LL'/K| = \frac{|L/K| \cdot |L'/K|}{|L \cap L'/K|}.$$

Außerdem ist $\varphi(m)\varphi(n) = \varphi((m,n))\varphi([m,n])$ und es gelten

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)}) \quad \text{und} \quad \mathbb{Q}(\eta_m) \cap \mathbb{Q}(\eta_n) = \mathbb{Q}(\eta_{(m,n)})$$

und

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{[m,n]}).$$

Daraus lässt sich mit einer Fallunterscheidung der Grad der Erweiterung berechnen:

Lemma 1.3.13 ([F], 4.1)**.** *Seien m_0, m_1, m_∞ natürliche Zahlen > 2. Dann ist*

$$n = |F/\mathbb{Q}| = \frac{\varphi([m_0, m_1, m_\infty])}{l}$$

mit

$$l = \begin{cases} 8, & \text{wenn alle } (m_i, m_j) \leq 2,\ i \neq j, \\ 4, & \text{wenn genau ein Paar } (i,j),\ i \neq j \text{ existiert, mit } (m_i, m_j) > 2, \\ 2, & \text{sonst.} \end{cases}$$

Ist $m_0 = 2$ und $m_1, m_\infty > 2$, dann hat man

$$n = |F/\mathbb{Q}| = \frac{\varphi([m_1, m_\infty])}{l}$$

mit

$$l = \begin{cases} 4, & \text{wenn } (m_1, m_\infty) \leq 2, \\ 2, & \text{wenn } (m_1, m_\infty) > 2. \end{cases}$$

Den Grad für $E/\mathbb{Q}$ erhält man, indem man m_i durch $2m_i$ ersetzt.

Sei R_E bzw. R_F der Ring der ganzen Zahlen in E bzw. F. Dann gilt

Satz 1.3.14. *Sei $\mathfrak{p}$ ein Primideal in R_E bzw. R_F über p und $\mathbb{F}_q$ sei der Körper aus 1.2.7. Für $p \neq 2$ ist $\mathbb{F}_q \cong R_E/\mathfrak{p}$, für $p = 2$ ist $\mathbb{F}_q \cong R_F/\mathfrak{p}$.*

Beweis. Für $(m_0 m_1 m_\infty, p) = 1$ folgt das mit 1.3.12. Ist $m_i = p$, dann ist p vollverzweigt in $\mathbb{Q}(\zeta_{2m_i} + \zeta_{2m_i}^{-1})$, d.h. p hat hier Trägheitsgrad 1. □

1.4 Kerne zählen

Wir wollen nun abzählen, wie viele Epimorphismen von $\Delta(m_0, m_1, m_\infty)$ nach $\mathrm{PSL}_2(\mathbb{F}_q)$ mit unterschiedlichen Kernen für ein reguläres p-zulässiges Ordnungstripel existieren. Wir folgen hier weitestgehend der Darstellung in [F].

Definition 1.4.1. Seien $g_0, g_1 \in \mathrm{PSL}_2(\overline{\mathbb{F}}_p)$, wobei $\overline{\mathbb{F}}_p$ der algebraische Abschluss von $\mathbb{F}_p$ sei. Dann nennen wir (g_0, g_1) eine (m_0, m_1, m_∞)-*Präsentation* von $\mathrm{PSL}_2(\mathbb{F}_q)$, wenn $\langle g_0, g_1 \rangle \cong \mathrm{PSL}_2(\mathbb{F}_q)$ und m_0, m_1, m_∞ die Ordnungen von $g_0, g_1, g_0 g_1$ sind.

Zwei solche (m_0, m_1, m_∞)-Präsentationen heißen *wesentlich verschieden*, wenn es keinen Automorphismus von $\mathrm{PSL}_2(\mathbb{F}_q)$ gibt, der die Erzeugenden aufeinander abbildet und *simultan konjugiert*, falls doch.

Bemerkung. Sei $A := \mathrm{Aut}\mathrm{PSL}_2(\mathbb{F}_q)$. Dann gilt [Su] (8.8)

$$\mathrm{PGL}_2(\mathbb{F}_q) \lhd A \quad \text{und} \quad A/\mathrm{PGL}_2(\mathbb{F}_q) \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p).$$

Dabei lässt sich jedes Element von A als Hintereinanderausführung einer Konjugation in $\mathrm{PGL}_2(\mathbb{F}_q)$ und der Anwendung eines Galoisautomorphismus von $\mathbb{F}_q$ auf die Einträge der Matrix schreiben.

Die wesentlich verschiedenen (m_0, m_1, m_∞)-Präsentationen entsprechen den torsionsfreien Normalteilern N in einer Dreiecksgruppe $\Delta(m_0, m_1, m_\infty)$ mit $\mathrm{PSL}_2(\mathbb{F}_q)$ als Quotienten, denn es gilt

Lemma 1.4.2 ([F], 3.1)**.** *Seien* $\varphi, \psi : \Delta(m_0, m_1, m_\infty) \to \mathrm{PSL}_2(\mathbb{F}_q)$ *Epimorphismen, die die Ordnungen auf den* γ_i *erhalten, d.h.* $(\varphi(\gamma_0), \varphi(\gamma_1))$ *und* $(\psi(\gamma_0), \psi(\gamma_1))$ *sind* (m_0, m_1, m_∞)*-Präsentationen. Dann ist* $\ker\varphi = \ker\psi$ *genau dann, wenn* $\varphi(\gamma_0) \mapsto \psi(\gamma_0)$, $\varphi(\gamma_1) \mapsto \psi(\gamma_1)$ *einen Automorphismus von* $\mathrm{PSL}_2(\mathbb{F}_q)$ *induziert.*

Wir wollen nun über die (m_0, m_1, m_∞)-Präsentationen die verschiedenen torsionsfreien Normalteiler in $\Delta(m_0, m_1, m_\infty)$ mit Faktorgruppe $\mathrm{PSL}_2(\mathbb{F}_q)$ zählen. Dabei hilft einem das folgende

Lemma 1.4.3 ([F], 3.4)**.** $(\tilde{g}_0, \tilde{g}_1, \tilde{g}_\infty)$ *und* $(\tilde{h}_0, \tilde{h}_1, \tilde{h}_\infty)$ *seien nichtsinguläre* $\mathrm{SL}_2(\mathbb{F}_q)$*-Tripel,* g_i, h_i *bezeichne die zu* $\tilde{g}_i, \tilde{h}_i$ *gehörigen Elemente in* $\mathrm{PSL}_2(\mathbb{F}_q)$ *und* (g_0, g_1) *und* (h_0, h_1) *seien* (m_0, m_1, m_∞)*-Präsentationen von* $\mathrm{PSL}_2(\mathbb{F}_q)$*. Dann gibt es ein* $x \in \mathrm{PSL}_2\overline{\mathbb{F}}_p$ *mit*

$$xg_0x^{-1} = h_0 \quad \text{und} \quad xg_1x^{-1} = h_1$$

genau dann, wenn die Spurtripel identisch sind oder sich genau zwei Spuren um den Faktor -1 *unterscheiden.*

Bemerkung. Eine Konjugation mit einem Element $x \in \mathrm{PSL}_2(\overline{\mathbb{F}}_p)$ wie im Lemma beschrieben induziert einen Automorphismus von $\mathrm{PSL}_2(\mathbb{F}_q)$. Da es sich dabei um einen Automorphismus handelt, der die Spuren erhält, muss es sogar eine Konjugation in $\mathrm{PGL}_2(\mathbb{F}_q) \leq \mathrm{PSL}_2(\mathbb{F}_{q^2})$ gewesen sein.

In $\mathbb{F}_q$ treffe man eine Auswahl $\mathbb{F}_q^{\mathrm{pos}}$ von Repräsentanten für $\pm a$, $a \in \mathbb{F}_q$, so dass für alle $a \in \mathbb{F}_q$ genau ein Element $a' \in \mathbb{F}_q^{\mathrm{pos}}$ existiert, das $a' = a$ oder $a' = -a$ erfüllt. Für ein beliebiges $a \in \mathbb{F}_q$ bezeichne a^{pos} den Repräsentanten aus $\mathbb{F}_q^{\mathrm{pos}}$. Einer (m_0, m_1, m_∞)-Präsentation (g_0, g_1) mit Spurtripel $(\tau_0, \tau_1, \tau_\infty)$ können wir nun den Wert

$$\left(\tau_0^{\mathrm{pos}}, \tau_1^{\mathrm{pos}}, \tau_\infty^{\mathrm{pos}}, \frac{\tau_0^{\mathrm{pos}}}{\tau_0}\frac{\tau_1^{\mathrm{pos}}}{\tau_1}\frac{\tau_\infty^{\mathrm{pos}}}{\tau_\infty}\right) \in (\mathbb{F}_q^{\mathrm{pos}})^3 \times \mathbb{F}_3$$

zuordnen, wobei wir hier für $\tau_i = 0$ den Wert $\frac{\tau_i^{\mathrm{pos}}}{\tau_i}$ durch 0 ersetzen.

Ist $m_i = 2$ für ein i, dann ist der 4. Eintrag gleich 0 für alle (m_0, m_1, m_∞)-Präsentationen und es genügt das Spurtripel in $(\mathbb{F}_q^{\mathrm{pos}})^3$ zu betrachten. Ist hingegen $m_i \neq 2$ für alle i, dann nimmt der 4. Eintrag für unterschiedliche (m_0, m_1, m_∞)-Präsentationen Werte aus ± 1 an.

Wir führen eine Äquivalenzrelation auf $(\mathbb{F}_q^{\mathrm{pos}})^3 \times \mathbb{F}_3$ ein, und zwar

$$\begin{aligned}&(\tau_0, \tau_1, \tau_\infty, \varepsilon) \sim (\hat{\tau}_0, \hat{\tau}_1, \hat{\tau}_\infty, \hat{\varepsilon})\\ &\quad :\Leftrightarrow \quad \exists\, \sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \text{ mit } \sigma(\tau_i)^{\mathrm{pos}} = \hat{\tau}_i \text{ und } \frac{\sigma(\tau_0)^{\mathrm{pos}}\sigma(\tau_1)^{\mathrm{pos}}\sigma(\tau_\infty)^{\mathrm{pos}}}{\sigma(\tau_0\tau_1\tau_\infty)} = \hat{\varepsilon}.\end{aligned}$$

Da sich jeder Automorphismus von $\mathrm{PSL}_2(\mathbb{F}_q)$ als Komposition einer Konjugation mit einem Element aus $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ beschreiben lässt, folgt

Korollar 1.4.4. *Zwei (m_0, m_1, m_∞)-Präsentationen von $\mathrm{PSL}_2(\mathbb{F}_q)$ sind genau dann simultan konjugiert, wenn ihre Tupel in $(\mathbb{F}_q^{\mathrm{pos}})^3 \times \mathbb{F}_3$ äquivalent sind.*

Wir wollen nun untersuchen, was für Tupel zu gegebenem Ordnungstripel (m_0, m_1, m_∞) überhaupt auftreten können: Ist $m_i = 2$, dann ist die Spur 0 und das liefert genau einen Wert in $\mathbb{F}_q^{\mathrm{pos}}$. Bei einem parabolischen Element ist die Spur ± 2, was ebenfalls einen Wert in $\mathbb{F}_q^{\mathrm{pos}}$ ergibt. Die Spur eines nicht-parabolischen Elements der Ordnung m_i ist $\pm(\zeta_i + \zeta_i^{-1})$, wobei ζ_i eine primitive $2m$-te oder, bei ungerader Ordnung möglicherweise, m-te Einheitswurzel ist. Daraus ergeben sich $\frac{\varphi(m_i)}{2}$ viele verschiedene Werte in $\mathbb{F}_q^{\mathrm{pos}}$. Setzt man $\varphi_p := \varphi$ für Ordnungen nicht-parabolischer Elemente und $\varphi_p(p) = 2$, so erhält man unter Berücksichtigung des Vorzeichens in der 4. Koordinate insgesamt

$$\frac{\varphi_p(m_0)\varphi_p(m_1)\varphi_p(m_\infty)}{4}$$

viele verschiedene Tupel zum Ordnungstripel (m_0, m_1, m_∞).

Wir müssen nun noch die äquivalenten Tupel miteinander identifizieren. Dazu betrachten wir zunächst die Frage, wann ein $\sigma \in \mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ das Tupel $(\tau_0, \tau_1, \tau_\infty, \varepsilon)$ in sich abbildet: Das ist genau dann der Fall, wenn σ die Bedingung

$$\begin{aligned} \text{(VZ)} \qquad & \tau_i^{\mathrm{pos}} = \sigma(\tau_i)^{\mathrm{pos}} \text{ bzw. } \tau_i^2 = \sigma(\tau_i^2) \\ \text{und} \quad & \tau_0\tau_1\tau_\infty = \sigma(\tau_0\tau_1\tau_\infty), \text{ falls } \tau_0\tau_1\tau_\infty \neq 0 \end{aligned}$$

erfüllt. Die erste Bedingung sagt nichts anderes, als dass $\sigma(\tau_i) = \pm\tau_i$, und die zweite Bedingung, dass die Anzahl der Vorzeichenwechsel gerade ist. Insbesondere ist σ eine Involution.

Ein Element gerader Ordnung in $\mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ existiert nur, wenn f gerade ist. Dann ist das Element mit Ordnung 2 von der Form

$$\sigma(x) = x^{p^{f/2}}.$$

und $\mathbb{F}_{p^{f/2}}$ ist der Fixkörper von σ.

Sei $\tau_i = \zeta_i + \zeta_i^{-1}$. Setzt man σ auf $\mathbb{F}_p(\zeta_0, \zeta_1, \zeta_\infty)$ fort, dann muss $\sigma(\zeta_i) = \pm\zeta_i^{\pm 1}$ gelten, und ein Vorzeichenwechsel kann nur stattfinden, wenn m_i gerade ist. Sei ξ_i eine andere primitive Einheitswurzel gleicher Ordnung. Dann gibt es ein k mit $(k, m_i) = 1$ und $\xi_i = \zeta_i^k$. Folglich ist

$$\sigma(\xi_i) = \sigma(\zeta_i)^k = (\pm\zeta_i^{\pm 1})^k = (\pm 1)^k \xi_i^{\pm 1} = \begin{cases} \xi_i^{\pm 1}, & \text{wenn } \sigma(\zeta_i) = \zeta_i^{\pm 1} \\ -\xi_i^{\pm 1}, & \text{wenn } \sigma(\zeta_i) = -\zeta_i^{\pm 1} \end{cases}$$

und somit $\sigma(\xi_i + \xi_i^{-1}) = \pm(\xi_i + \xi_i^{-1})$ und ein Vorzeichenwechsel findet genau dann statt, wenn σ das Vorzeichen bei τ_i wechselt, m.a.W. die Bedingung (VZ) ist für alle in Frage kommenden Spuren simultan erfüllt oder für keine.

Fazit: Ist (VZ) nicht erfüllt, so operiert $\mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ fixpunktfrei auf den in Frage kommenden Spur-Tupeln und wir erhalten

$$\frac{\varphi_p(m_0)\varphi_p(m_1)\varphi_p(m_\infty)}{4f}$$

Äquivalenzklassen.

Ist (VZ) erfüllt, dann fixiert genau obiges σ alle auftretenden Spur-Tupel und $\mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)/\langle\sigma\rangle$ operiert fixpunktfrei, d.h. wir erhalten

$$\frac{\varphi_p(m_0)\varphi_p(m_1)\varphi_p(m_\infty)}{2f}$$

Äquivalenzklassen. Wir haben somit gezeigt

Satz 1.4.5 ([F], 3.5'). *Ist (m_0, m_1, m_∞) ein reguläres p-zulässiges Ordnungstripel, dann gibt es*

$$\frac{\varphi_p(m_0)\varphi_p(m_1)\varphi_p(m_\infty)}{4f^*}$$

wesentlich verschiedene (m_0, m_1, m_∞)-Präsentationen von $\mathrm{PSL}_2(\mathbb{F}_q)$, wobei

$$f^* = \begin{cases} f, & \text{falls (VZ) nicht erfüllt ist,} \\ \frac{f}{2}, & \text{falls (VZ) erfüllt ist.} \end{cases}$$

Ist $p = 2$, dann spielt das Vorzeichen und somit auch die Bedingung (VZ) keine Rolle mehr. Wir erhalten also

Satz 1.4.6. *Es sei (m_0, m_1, m_∞) ein 2-zulässiges reguläres Ordnungstripel. Dann gibt es*

$$\frac{\varphi_2(m_0)\varphi_2(m_1)\varphi_2(m_\infty)}{8f}$$

wesentlich verschiedene (m_0, m_1, m_∞)-Präsentationen von $\mathrm{PSL}_2(\mathbb{F}_q)$.

Bemerkung. Ist (m_0, m_1, m_∞) singulär, dann wird nicht bei allen Spurtripeln ganz $\mathrm{PSL}_2(\mathbb{F}_q)$ erzeugt, d.h. man bekommt hier nur eine obere Schranke.

Für irreguläre Ordnungstripel erhält man

$$\frac{\varphi_p(m_0)\varphi_p(m_1)\varphi_p(m_\infty)}{2f}$$

wesentlich verschiedene (m_0, m_1, m_∞)-Präsentationen von $\mathrm{PGL}_2(\mathbb{F}_q)$ (siehe [F] 3.5').

1.5 Verschiedene Kerne und die zugehörigen Kurven

Im folgenden bezeichne $\mathfrak{U}$ die obere Halbebene der komplexen Zahlen bzw. die hyperbolische Ebene. Aus den verschiedenen torsionsfreien Kernen $K \lhd \Delta$, die man über die Projektionen auf $\mathrm{PSL}_2(\mathbb{F}_q)$ gewinnt, erhält man quasiplatonische Riemannsche Flächen $K\backslash\mathfrak{U}$. Diese Flächen müssen im allgemeinen nicht verschieden sein. Gegeben zwei torsionsfreie Normalteiler in einer Fuchsschen Gruppe $K_1, K_2 \lhd \Gamma$, so sind die Riemannschen Flächen $K_i\backslash\mathfrak{U}$ genau dann isomorph, wenn es ein $\alpha \in \mathrm{PSL}_2(\mathbb{R})$ gibt, mit $K_1 = \alpha K_2 \alpha^{-1}$ (siehe z.B. [JS] 5.9.3).

Handelt es sich bei Γ jedoch um eine maximale Fuchssche Gruppe, dann gilt für den Normalisator in $\mathrm{PSL}_2(\mathbb{R})$: $N(\Gamma) = \Gamma$. Für Normalteiler K_i in Γ gilt $\Gamma \leq N(K_i)$ und wegen der Maximalität folgt sogar $\Gamma = N(K_i)$. Angenommen die K_i sind über α konjugiert in $\mathrm{PSL}_2(\mathbb{R})$, dann gilt $N(K_1) = \alpha N(K_2)\alpha^{-1}$, m.a.W. $\alpha \in N(\Gamma) = \Gamma$, folglich $K_1 = K_2$.

Satz 1.5.1 (vgl. [F] 6.1)**.** *Sei (m_0, m_1, m_∞) p-zulässig, regulär und die Dreiecksgruppe $\Delta = \Delta(m_0, m_1, m_\infty)$ sei maximal. K_i seien die verschiedenen torsionsfreien Kerne mit Quotienten $\mathrm{PSL}_2(\mathbb{F}_q)$. Dann sind die Riemannschen Flächen $K_i\backslash\mathfrak{U}$ alle paarweise nicht-isomorph und es besteht somit eine 1–1-Zuordnung zwischen diesen Riemannschen Flächen und den Spur-Tupeln $(\tau_0, \tau_1, \tau_\infty, \epsilon)$.*

Wir können obigen Satz noch auf eine gewisse Klasse nicht-maximaler Dreiecksgruppen erweitern. Dabei helfen einem die Resultate aus [GW]. Eine wichtige Rolle bei den Untersuchungen in dieser Arbeit spielte der Konjugator einer Untergruppe in einer größeren Gruppe.

Definition 1.5.2. Seien $K \leq \Gamma$ Fuchssche Gruppen. Dann bezeichne

$$C(\Gamma, K) := \left\{ \alpha \in \mathrm{PSL}_2(\mathbb{R}) \mid \alpha K \alpha^{-1} \leq \Gamma \right\} = \left\{ \alpha \in \mathrm{PSL}_2(\mathbb{R}) \mid K \leq \alpha^{-1}\Gamma\alpha \right\}$$

den *Konjugator von K in Γ*.

Gegeben $K \leq \Gamma$, so lässt Konjugation mit $N(K)$ die Untergruppe K fest und anschließende Konjugation mit $N(\Gamma)$ bewegt K nur innerhalb Γs, d.h. wir haben eine Inklusion

$$N(\Gamma) \cdot N(K) \subset C(\Gamma, K).$$

In der Regel ist $C(\Gamma, K)$ keine Gruppe, aber sind Γ, K beides Dreiecksgruppen, so gilt:

Satz 1.5.3 ([GW], Theorem 7)**.** *Seien $\Delta \leq \tilde{\Delta}$ zwei Fuchssche Dreiecksgruppen. Dann ist*

$$C(\tilde{\Delta}, \Delta) = N(\tilde{\Delta})N(\Delta).$$

Sei nun Δ eine Dreiecksgruppe mit torsionsfreiem Normalteiler K und $\alpha \in \mathrm{PSL}_2\mathbb{R}$ so, dass auch $\alpha K \alpha^{-1} \lhd \Delta$, was gleichbedeutend ist mit $K \lhd \alpha^{-1}\Delta\alpha$. Setzt man $\tilde{\Delta} = N(K)$, dann gilt $\Delta, \alpha^{-1}\Delta\alpha \leq \tilde{\Delta}$, also $\Delta \leq \alpha\tilde{\Delta}\alpha^{-1}$, m.a.W.

$$\alpha^{-1} \in C(\tilde{\Delta}, \Delta).$$

Ist Δ maximal, so ist $\tilde{\Delta} = N(K) = N(\Delta) = \Delta$, also $C(\tilde{\Delta}, \Delta) = \Delta$, und man erhält das Resultat aus Satz 1.5.1.

Die Enthaltensrelationen für Dreiecksgruppen wurden in [Si] bestimmt und sind allesamt Zusammensetzungen aus den Relationen in folgender Liste:

$$\begin{array}{rlll}
(i) & \Delta(n,n,n) & \lhd_3 & \Delta(3,3,n) \\
(ii) & \Delta(n,n,m) & \lhd_2 & \Delta(2,n,2m) \\
(iii) & \Delta(2,n,2n) & \leq_3 & \Delta(2,3,2n) \\
(iv) & \Delta(3,n,3n) & \leq_4 & \Delta(2,3,3n) \\
(v) & \Delta(2,7,7) & \leq_9 & \Delta(2,3,7) \\
(vi) & \Delta(3,8,8) & \leq_{10} & \Delta(2,3,8) \\
(vii) & \Delta(4,4,5) & \leq_6 & \Delta(2,4,5) \\
(viii) & \Delta(3,3,7) & \leq_8 & \Delta(2,3,7)
\end{array}$$

Dabei geben die Indizes den Index der Untergruppe in der größeren Gruppe an. Ist Δ nicht-maximal, handelt es sich also um eine Dreiecksgruppe vom Typ derer, die in obiger Liste auf der linken Seite stehen. Wir betrachten zunächst die Fälle (iii) und (iv), also $K \lhd \Delta(2,n,2n)$ oder $\Delta(3,n,3n)$: Angenommen K ist auch Normalteiler in $\Delta(2,3,2n)$ bzw. $\Delta(2,3,3n)$, dann ist $\tilde{\Delta} = N(K) = \Delta(2,3,2n)$ bzw. $\Delta(2,3,3n)$, d.h.

$$C(\tilde{\Delta}, \Delta) = N(\tilde{\Delta})N(\Delta) = \tilde{\Delta}\Delta = \tilde{\Delta}.$$

Folglich kann es keine zu K konjugierten Kerne in Δ geben.

Ist andererseits K kein Normalteiler in $\Delta(2,3,2n)$ bzw. $\Delta(2,3,3n)$, dann ist $\tilde{\Delta} = N(K) = \Delta$ und wir haben $C(\tilde{\Delta}, \Delta) = \Delta$ und ebenfalls keine zu K konjugierten Kerne in Δ. Somit gilt:

Lemma 1.5.4. *Sei Δ eine Dreiecksgruppe vom Typ $(2,n,2n)$ oder vom Typ $(3,n,3n)$, $n \neq 2,3$, und K_1, K_2 verschiedene torsionsfreie Normalteiler in Δ. Dann sind $K_1\backslash\mathfrak{U}$ und $K_2\backslash\mathfrak{U}$ nicht-isomorphe Riemannsche Flächen.*

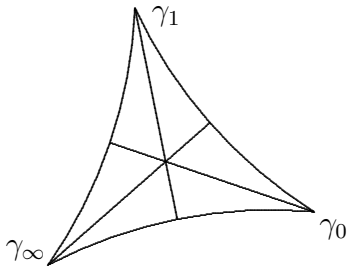
Ist der Quotient Δ/K eine einfache Gruppe, dann muss sogar $N(K) = \Delta$ gelten: Dazu betrachten wir zunächst $\Delta = \Delta(2, n, 2n) \leq \Delta(2, 3, 2n)$. Aus Theorem 6 [GW] entnehmen wir, dass es drei verschiedene konjugierte Untergruppen $\Delta_1 = \Delta$, Δ_2, Δ_3 vom Typ $(2, n, 2n)$ in $\Delta(2, 3, 2n)$ gibt, deren Schnitt $\Delta_1 \cap \Delta_2 \cap \Delta_3 = \Delta(n, n, n) \lhd \Delta(2, n, 2n)$ ist. Konjugation in $\Delta(2, 3, 2n)$ permutiert die Δ_i, d.h. angenommen $K \lhd \Delta(2, 3, 2n)$, dann ist K auch Normalteiler in $\Delta(n, n, n)$ und wir erhalten den Widerspruch

$$\Delta(n, n, n)/K \lhd \Delta/K.$$

Die Situation mit $\Delta = \Delta(3, n, 3n) \leq \Delta(2, 3, 3n)$ ist ähnlich. Hier hat man vier verschiedene konjugierte Untergruppen $\Delta_1 = \Delta$, Δ_2, Δ_3, Δ_4 vom Typ $(3, n, 3n)$ in $\Delta(2, 3, 3n)$ und Konjugation in der großen Gruppe permutiert die Δ_i, d.h. $\bigcap \Delta_i$ ist ein Normalteiler in $\Delta(2, 3, 3n)$, also auch in Δ. Nimmt man an, dass $K \lhd \Delta(2, 3, 3n)$ ist, folgt wie oben, dass $K \lhd \bigcap \Delta_i$ und die Einfachheit von Δ/K impliziert $K = \Delta_1 \cap \Delta_2 \cap \Delta_3 \cap \Delta_4$. Die Konjugationsoperation von $\Delta(2, 3, 3n)$ auf den Δ_i liefert einen Homomorphismus $\Delta(2, 3, 3n) \to S_4$, dessen Kern gerade $\bigcap \Delta_i$ ist. Da $\Delta(2, 3, 3n)$ Elemente von Ordnung $3n \geq 9$ enthält, ist der Kern aber nicht torsionsfrei, also $\neq K$. Wir fassen zusammen

Lemma 1.5.5. *Ist Δ vom Typ $(2, n, 2n)$ oder $(3, n, 3n)$, $n \neq 2, 3$, $K \lhd \Delta$ torsionsfrei und Δ/K einfach, dann ist Δ/K somit bereits die volle Automorphismengruppe der Fläche $K\backslash\mathfrak{U}$.*

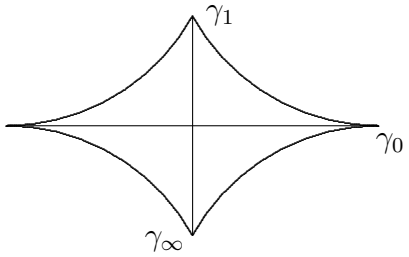
Alle anderen Dreiecksgruppen auf der linken Seite unserer Liste sind von der Form (n, n, n) oder (n, n, m). Hier kann man nicht mehr sicherstellen, dass unterschiedliche Kerne zu unterschiedlichen Riemannschen Flächen führen. Man betrachte z.B. den Fall $\Delta = \Delta(n, n, n)$ mit Kern K und Quotient $\Delta/K \cong G = \mathrm{PSL}_2(\mathbb{F}_p)$: Ist $K \lhd \tilde{\Delta} = N(K) = \Delta(2, 3, 2n)$, dann ist $C(\tilde{\Delta}, \Delta) = \Delta(2, 3, 2n)$ und somit gibt es keine anderen zu K konjugierten Kerne. Die Elemente von $\tilde{\Delta}$ induzieren durch Konjugation Elemente in der Automorphismengruppe von Δ/K. Betrachtet man die Fundamentalbereiche, sieht man, dass es ein $\delta \in \tilde{\Delta}$ gibt, das $\gamma_0, \gamma_1, \gamma_\infty \in \Delta$ zyklisch permutiert.



D.h. es gibt ein Element $d \in \mathrm{Aut}\,(G) = \mathrm{PGL}_2(\mathbb{F}_p)$, das g_0, g_1, g_∞ zyklisch permutiert; die g_i haben also alle die gleiche Spur.

Betrachtet man einen Kern $K \lhd \Delta$, bei dem die γ_i auf Elemente unterschiedlicher Spur in Δ/K abgebildet werden, dann ist folglich $K \not\lhd \tilde{\Delta}$. In diesem Fall ist $N(K) = \Delta$ oder $\Delta(3,3,n)$ und $C(N(K),\Delta) = \tilde{\Delta} = \Delta(2,3,2n)$. Der Konjugator lässt K somit nicht fest, sondern konjugiert über verschiedene $K' \neq K$. Andererseits ist $\Delta \lhd \tilde{\Delta}$, d.h. auch K' ist ein Normalteiler in Δ. Es gibt somit verschiedene zueinander konjugierte Kerne in Δ.

Für $\Delta = \Delta(n,n,m)$, $n \neq m$, kann man ähnlich argumentieren mit $\tilde{\Delta} = \Delta(2,n,2m)$. Hier ist die Inklusion der Fundamentalbereiche wie folgt:



$K \lhd \tilde{\Delta}$ impliziert dann $\operatorname{tr} g_1 = \operatorname{tr} g_\infty$. Für Tupel mit paarweise verschiedenen Spuren muss also $K \not\lhd \tilde{\Delta}$ gelten und wir erhalten wieder zueinander konjugierte Kerne.

1.6 Multiplikatoren

Um die Galois-Operation auf einer Familie kompakter Riemannscher Flächen X_i zu verstehen, haben sich spezielle Multiplikatoren der Automorphismengruppe der X_i als nützliches Hilfsmittel erwiesen (siehe z.B. [St00], [StWo]): Kann man die X_i anhand ihrer Multiplikatoren innerhalb ihrer Familie beschreiben, so lässt sich die Galois-Operation auf den X_i an dem Verhalten der Multiplikatoren unter der Galois-Gruppe nachvollziehen.

Definition 1.6.1. Sei X eine Riemannsche Fläche, $\alpha \in \operatorname{Aut}(X)$ mit Fixpunkt $x \in X$ und h sei eine Karte um x mit $h(x) = c \in \mathbb{C}$. Dann nennen wir

$$m_\alpha = m_{\alpha,x} := (h\alpha h^{-1})'(c) \neq 0$$

den *Multiplikator von α im Punkt x*.

Lemma 1.6.2. *Mit obigen Bezeichnungen gilt:*

(i) *$m_{\alpha,x}$ ist unhabhängig von der Wahl der Karte.*

(ii) *Der Multiplikator ist invariant unter Konjugation, d.h. für $\varphi \in \operatorname{Aut}(X)$ gilt*

$$m_{\varphi\alpha\varphi^{-1},\varphi(x)} = m_{\alpha,x}.$$

Beweis. Ein Kartenwechsel, der c in den Nullpunkt verschiebt, ändert nichts an der Ableitung, d.h. wir können o.B.d.A. Karten mit $x \mapsto 0$ betrachten. Seien h, k also zwei beliebige Karten um x mit $h(x) = 0 = k(x)$. Dann gilt

$$(k\alpha k^{-1})'(0) = ((kh^{-1})(h\alpha h^{-1})(hk^{-1}))'(0) = (h\alpha h^{-1})'(0).$$

Das zeigt (i). (ii) folgt ebenfalls durch Anwendung der Kettenregel. □

Sind α, β aus der Fixgruppe $\mathrm{Aut}(X)_x$ von x in $\mathrm{Aut}(X)$ und h eine Karte mit $h(x) = 0$, dann ist

$$(h\alpha\beta h^{-1})'(0) = ((h\alpha h^{-1})(h\beta h^{-1}))'(0) = m_\alpha m_\beta,$$

d.h. $m_{\alpha\beta} = m_\alpha m_\beta$, m.a.W. $\mathrm{Fix}_x(\mathrm{Aut}(X)) \to \mathbb{C}^*$, $\alpha \mapsto m_\alpha$ ist ein Homomorphismus. Ist $\operatorname{ord}\alpha = m < \infty$, dann ist der Multiplikator von α somit eine m-te Einheitswurzel.

Wir wollen nun die Fixpunkte eines Automorphismus einer quasiplatonischen Riemannschen Fläche genauer betrachten: Sei also $\Delta = \Delta(m_0, m_1, m_\infty)$ eine Dreiecksgruppe, $\Gamma \lhd \Delta$ ein torsionsfreier Normalteiler von endlichem Index und $X = \Gamma\backslash\mathfrak{U}$ die Riemannsche Fläche. $G := \Delta/\Gamma$ ist dann in der Automorphismengruppe von X enthalten. Da der Normalisator von Γ eine Dreiecksgruppe ist, ist auch die volle Automorphismengruppe von X vom Typ Dreiecksgruppe/Γ.

Sei $z \in \mathfrak{U}$ und $x := \Gamma z \in X$. Ist $\delta \in \mathrm{Stab}_\Delta(z)$, dann ist $\delta\Gamma z = \Gamma\delta z = \Gamma z$, d.h. $\delta\Gamma \in \mathrm{Stab}_G(x)$. Ist andererseits $1 \neq \delta\Gamma \in \mathrm{Stab}_G(x)$, also $\Gamma z = \delta\Gamma \cdot \Gamma z = \Gamma\delta z$, dann gibt es genau ein $\gamma \in \Gamma$ mit $\gamma z = \delta z$, m.a.W. $\delta^{-1}\gamma \in \mathrm{Stab}_\Delta(z)$. Somit ist gezeigt:

Lemma 1.6.3. *Unter der Projektion $\Delta \twoheadrightarrow G = \Delta/\Gamma$ werden die Stabilisatoren von $z \in \mathfrak{U}$ in Δ isomorph auf die Stabilisatoren von $x = \Gamma z \in X$ in G abgebildet.*

Sind z_i die Fixpunkte von γ_i, dann sind die Punkte mit nicht-trivialem Stabilisator in $\mathfrak{U}$

$$\Delta z_0 \cup \Delta z_1 \cup \Delta z_\infty$$

und $\mathrm{Stab}_\Delta(\delta z_i) = \delta\mathrm{Stab}_\Delta(z_i)\delta^{-1}$. Folglich liegen die Punkte in X mit nicht-trivialem Stabilisator in der Menge

$$Gx_0 \cup Gx_1 \cup Gx_\infty$$

mit $x_i := \Gamma z_i$ und

$$\mathrm{Stab}_G(gx_i) = g\mathrm{Stab}_G(x_i)g^{-1} = g\langle g_i\rangle g^{-1} \cong \mathbb{Z}/m_i\mathbb{Z},$$

mit $g_i := \gamma_i \Gamma$.

Wir bestimmen nun die Anzahl der Fixpunkte für ein $g \in G$: Hat g einen Fixpunkt in hx_i, mit $h \in G$, so ist das gleichbedeutend mit

$$\langle g \rangle \leq \mathrm{Stab}_G(hx_i) \quad \text{bzw.} \quad \langle g \rangle \leq h \langle g_i \rangle h^{-1}.$$

Ist $d = \operatorname{ord} g$, dann ist d ein Teiler von m_i und $\langle g \rangle$ ist konjugiert zu der Untergruppe mit Ordnung d von $\langle g_i \rangle$. Setze

$$\varepsilon_i(g) := \begin{cases} 1, & \langle g \rangle \text{ ist konjugiert zu der UG mit Ordnung } d \text{ in } \langle g_i \rangle, \\ 0, & \text{sonst.} \end{cases}$$

Angenommen $\varepsilon_i(g) = 1$. Die Anzahl der Fixpunkte konjugierter Elemente ist gleich, wir können also o.B.d.A. $g = g_i^{m_i/d}$ annehmen. Dann gilt:

$$\begin{aligned} g \text{ fixiert } hx_i &\Leftrightarrow \langle {g_i}^{m_i/d} \rangle = h \langle {g_i}^{m_i/d} \rangle h^{-1} \\ &\Leftrightarrow h \in \mathrm{N}_G(\langle g \rangle). \end{aligned}$$

Da außerdem $\mathrm{Stab}_{\mathrm{N}_G(\langle g_i^{m_i/d} \rangle)}(x_i) = \langle g_i \rangle$, haben wir

$$|\mathrm{N}_G(\langle g \rangle) \cdot x_i| = \left|\mathrm{N}_G(\langle g \rangle) : \mathrm{Stab}_{\mathrm{N}_G(\langle g \rangle)}(x_i)\right| = \frac{|\mathrm{N}_G(\langle g \rangle)|}{m_i}$$

verschiedene Fixpunkte von g in der G-Bahn von x_i; insgesamt hat g demnach

$$|\mathrm{N}_G(\langle g \rangle)| \sum_i \varepsilon_i(g)/m_i$$

viele Fixpunkte.

Auf die gleiche Weise lässt sich die Anzahl der Fixpunkte einer Automorphismengruppe einer Riemannschen Fläche berechnen, wenn wir statt einer Dreiecksgruppe Δ eine Fuchssche Gruppe mit Signatur $(g; m_1, \ldots, m_r; -)$ vorliegen haben. Die Formel bleibt die gleiche, nur dass der Index i dann über die Werte $1, \ldots, r$ läuft und wurde bewiesen in [M73]. Der Beweis wurde hier noch einmal wiedergegeben, da wir aus ihm im Fall $G = \Delta/\Gamma \cong \mathrm{PSL}_2(\mathbb{F}_q)$ weitere Informationen über die Multiplikatoren erhalten:

Ist $\operatorname{ord} g = d$ und $d \mid m_i$, dann ist aufgrund der Eigenschaften von $\mathrm{PSL}_2(\mathbb{F}_q)$ bzgl. Konjugation (je zwei nicht-parabolische Elemente gleicher Spur sind konjugiert und jedes parabolische Element ist konjugiert zu einer oberen Dreiecksmatrix) $\langle g \rangle$ konjugiert zu der Untergruppe von $\langle g_i \rangle$ mit Ordnung d, d.h. g hat Fixpunkte in Gx_i.

Ist g nicht-parabolisch und hx_i, $h \in G$, ein Fixpunkt von g, dann ist g zu genau zwei Elementen in $\langle g_i \rangle$ konjugiert, nämlich $(g_i^{m_i/d})^{\pm k}$, wobei k so

gewählt ist, dass die Spur mit der von g übereinstimmt. Ist $g = h(g_i^{m_i/d})^k h^{-1}$, so gilt

$$m_{g,hx_i} = m_{(g_i^{m_i/d})^k, x_i}.$$

Für den Multiplikator von g_i in x_i gilt

$$m_{g_i,x_i} = \zeta_{m_i} := \exp(2\pi i/m_i).$$

In allen Fixpunkten von g, die in der G-Bahn von x_i liegen, kommen als Multiplikatoren somit nur die Werte $\zeta_{m_i}^{\pm km_i/d}$ in Frage. Da g und g^{-1} zueinander konjugiert sind, treten $\zeta_{m_i}^{\pm km_i/d}$ außerdem gleich häufig als Multiplikatoren auf.

Wir fassen zusammen:

Lemma 1.6.4. *Sei Γ ein torsionsfreier Normalteiler in der Dreiecksgruppe $\Delta = \Delta(m_0, m_1, m_\infty)$ und $G = \Delta/\Gamma \cong \mathrm{PSL}_2(\mathbb{F}_q)$ die Automorphismengruppe der Riemannschen Fläche $X = \Gamma\backslash\mathfrak{U}$. Dann gelten für $g \in G$ mit $\operatorname{ord} g = d$:*

(i) $\varepsilon_i(g) = 1 \Leftrightarrow d \mid m_i$. g hat dann $\frac{|\mathrm{N}_G(\langle g\rangle)|}{m_i}$ viele Fixpunkte in Gx_i.

(ii) Ist g nicht-parabolisch und $\varepsilon_i(g) = 1$, dann hat g insgesamt $\frac{|\mathrm{N}_G(\langle g\rangle)|}{2m_i}$ viele Fixpunkte in Gx_i mit Multiplikator $\zeta_{m_i}^{km_i/d}$ und ebenso viele mit Multiplikator $\zeta_{m_i}^{-km_i/d}$, wobei k nur von der Spur von g abhängt.

Bemerkung. Für $\Delta = \Delta(2,3,7)$ bzw. $\Delta(2,3,n)$, $n > 6$, erhält man zusammen mit Korollar 1.1.8 die Aussage von Lemma 1 bzw. Lemma 1' aus [St00], ohne dabei die Eichlersche Spurformel zu benutzen.

Damit ergibt sich folgender Zusammenhang zwischen Spurtripeln und Multiplikatoren: Wir identifizieren $G = \mathrm{PSL}_2(\mathbb{F}_q)$ mit Δ/Γ, wobei γ_i auf g_i abgebildet wird. Für ein nicht-parabolisches g_i sei $\operatorname{tr} g_i = \pm(\xi_i + \xi_i^{-1})$ mit einer $2m_i$-ten primitiven Einheitswurzel $\xi_i \in \mathbb{F}_{q^2}$. Die Multiplikatoren von g_i in Fixpunkten in $G\cdot\Gamma z_i$ sind ζ_i und ζ_i^{-1} für $\zeta_i = \exp(2\pi i/m_i)$. Wir betrachten nun eine andere Abbildung von Δ auf G, indem wir die γ_i auf ein anderes G-Tripel g_i' abbilden und erhalten somit einen anderen Kern $\Delta/\Gamma' \cong G$. Dann ist $\operatorname{tr} g_i' = \pm(\xi_i^r + \xi_i^{-r})$ für ein r mit $(2m_i, r) = 1$ und die Multiplikatoren der g_i' in $G \cdot \Gamma' z_i$ sind ζ_i und ζ_i^{-1}. g_i und $g_i'^s$ mit $rs \equiv 1 \bmod 2m_i$ haben die gleiche Spur, sind also konjugiert, d.h. g_i hat die Multiplikatoren ζ_i^s, ζ_i^{-s} in $G \cdot \Gamma' z_i$. In 1.4.4 haben wir die verschiedenen Γ mit $\Delta/\Gamma \cong G$ über die Spurtripel der verschiedenen Bilder der γ_i beschrieben. Spielt das Vorzeichen der Spuren keine Rolle, so können wir die Kerne also genauso gut über die Multiplikatoren eines fest gewählten Tripels (g_0, g_1, g_∞) in G beschreiben.

1.7 Galois-Operation

Wir betrachten nun den Effekt der Galois-Operation auf den Multiplikatoren wie in [St95] bzw. [St00] beschrieben: X sei eine kompakte Riemannsche Fläche und $\Omega(X)$ der $\mathbb{C}$-Vektorraum der holomorphen Differentialformen auf X. Es ist $\dim_{\mathbb{C}} \Omega(X) = g$, wobei g das Geschlecht von X ist. $\omega_1, \ldots, \omega_g$ sei eine Basis und bzgl. einer Karte z um $x \in X$ sei $\omega_i = f_i dz$ die lokale Darstellung. Ist w eine andere Karte um x, so gilt $\omega_i = f_i \frac{\partial z}{\partial w} dw$, d.h. man erhält eine wohldefinierte Abbildung

$$\theta : X \to \mathbb{P}^{g-1}(\mathbb{C}) \quad \text{mit} \quad x \mapsto (f_1(x) : \cdots : f_g(x))$$

von X in den projektiven Raum. Ist X nicht hyperelliptisch, dann ist θ sogar eine Einbettung ([FK], III.10.2), die sogenannte *kanonische Einbettung*. $\theta(X)$ nennen wir auch das *kanonische Modell* von X.

Des weiteren kann man eine (Rechts-)Operation von $\mathrm{Aut}(X)$ auf $\Omega(X)$ definieren, und zwar lokal durch

$$\omega^\alpha = f \circ \alpha d(z \circ \alpha)$$

für $\alpha \in \mathrm{Aut}(X)$ und $\omega = f dz \in \Omega(X)$. Daraus erhalten wir eine treue Darstellung $\rho : \mathrm{Aut}(X) \to \mathrm{GL}_g(\mathbb{C})$ ([FK], V.2.1 Proposition). Aus ρ erhält man einen Homomorphismus $\hat{\rho} : \mathrm{Aut}(X) \to \mathrm{PGL}_g(\mathbb{C})$, so dass das Diagramm

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & X \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ \theta(X) & \xrightarrow{\hat{\rho}(\alpha)} & \theta(X) \end{array}$$

kommutiert, d.h. die Automorphismengruppe operiert als projektive Gruppe auf dem kanonischen Modell.

Ist $x \in X$ ein Fixpunkt von α, dann ist entsprechend $(\omega_1(x) : \cdots : \omega_g(x))$ ein Fixpunkt von $\hat{\rho}(\alpha)$, d.h. $(\omega_1(x), \ldots, \omega_g(x)) \in \mathbb{C}^g$ ist ein Eigenvektor von $\rho(\alpha)$. Wegen

$$\omega_i^\alpha(x) = f_i(\alpha(x)) d(z\alpha) = \frac{\partial \alpha}{\partial z}(x) f_i(x) dz = m_{\alpha,x} \cdot \omega_i(x),$$

ist der zugehörige Eigenwert gleich dem Multiplikator $m_{\alpha,x}$.

Sei $I = I(X)$ das Ideal der Kurve X, d.h. X ist die Nullstellenmenge aller Polynome in I. Da X arithmetisch ist, können wir uns I als

$$I = \langle p_1(x_1, \ldots, x_g), \ldots, p_r(x_1, \ldots, x_g) \rangle, p_i \in \overline{\mathbb{Q}}[x_1, \ldots, x_g]$$

denken. Wendet man $\sigma \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ koeffizientenweise auf die p_i an, so erhält man ein Ideal

$$I^\sigma = \langle p_1^\sigma, \ldots, p_r^\sigma \rangle\,,$$

das uns eine Kurve X^σ definiert.

Beschreibt man die $\omega_i = f_i dz$ auf dem kanonischen Modell durch rationale Funktionen, so erhält man, wieder durch Anwenden von σ auf die Koeffizienten, Differentiale $\omega_i^\sigma = f_i^\sigma dz$ auf X^σ und $\alpha \in \mathrm{Aut}(X)$ operiert auf $\Omega(X^\sigma)$ durch $\rho(\alpha)^\sigma$, wobei σ auf alle Einträge der Matrix $\rho(\alpha)$ angewandt wird. Entsprechend operiert α durch $\hat{\rho}(\alpha)^\sigma$ auf X^σ und wir haben:

Fazit 1.7.1 (siehe [St00], Lemma 2)**.** *Ist $\alpha \in \mathrm{Aut}(X)_x$ mit Multiplikator $m_{\alpha,x}$, dann ist $(\omega_1(x), \ldots, \omega_g(x))$ ein Eigenvektor von $\rho(\alpha)$ mit Eigenwert $m_{\alpha,x}$.*

Auf der konjugierten Kurve X^σ ist der Punkt $x^\sigma := (\omega_1^\sigma(x) : \cdots : \omega_g^\sigma(x))$ ein Fixpunkt von α und $(\omega_1^\sigma(x), \ldots, \omega_g^\sigma(x))$ ist Eigenvektor von $\rho(\alpha)^\sigma$ mit Eigenwert $\sigma(m_{\alpha,x})$, d.h. α hat in x^σ den Multiplikator $\sigma(m_{\alpha,x})$.

Die Kurven, die wir betrachten wollen, haben eine einfache Automorphismengruppe. Auf einer hyperelliptischen Fläche von Geschlecht $g \geq 2$ gibt es die hyperelliptische Involution, die mit allen Elementen der Automorphismengruppe kommutiert ([FK] III.7.9, Corollary 3), d.h. es gibt einen nicht-trivialen Normalteiler in der Automorphismengruppe einer hyperelliptischen Kurve. Wir können also das kanonische Modell und die Folgerungen für die Multiplikatoren verwenden.

Nach Lemma 1.6.4 und Korollar 1.4.4 können wir die torsionsfreien Kerne $\Delta(m_0, m_1, m_\infty) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{F}_q)$ über das Spurtripel in $\mathbb{F}_q$ und im Fall $m_0 = 2$ oder $p = 2$ sogar durch das Tripel der Multiplikatoren von g_0, g_1, g_∞ beschreiben. Daraus ergibt sich für die Galois-Konjugation der zugehörigen Kurven:

Satz 1.7.2. *Sei $p \neq 2$, $\Delta = \Delta(2, m_1, m_\infty)$ ein p-zulässiges nicht irreguläres Ordnungstripel zu einer maximalen Fuchsschen Gruppe oder einer Gruppe vom Typ $(2, m, 2m)$ und $\mathbb{F}_q$ sei der zugehörige Spurkörper aus Satz 1.2.7. K_i seien die torsionsfreien Normalteiler in Δ mit $\Delta/K_i \cong \mathrm{PSL}_2(\mathbb{F}_q)$ und $X_i := K_i \backslash \mathfrak{U}$ seien die Riemannschen Flächen.*

Dann lässt sich die Operation von $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ auf den X_i über die Operation von $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ auf den Multiplikatoren von g_1 und g_∞ beschreiben.

Wir wollen jetzt noch den Definitionskörper der Kurven bestimmen. Da wir es mit quasiplatonischen Flächen zu tun haben, stimmt der Definitionskörper mit dem Modulkörper überein (siehe [Wo], Thm. 5). Der Modulkörper einer kompakten Riemannschen Fläche ist der Fixkörper von:

$$U(X) := \{\, \sigma \in \mathrm{Aut}\,(\mathbb{C}) \mid X^\sigma \cong X \}\,.$$

Das ist der kleinste Körper K mit der Eigenschaft, dass für alle $\sigma \in \mathrm{Aut}(\mathbb{C})$ mit $\sigma|_K = \mathrm{id}_K$ folgt, dass $X \cong X^\sigma$ (vgl. [Wo], 4.3).

Um die Situation im Detail zu beschreiben führen wir außerdem die folgende Notation ein:

Definition 1.7.3. Sei F/K eine Galois-Erweiterung mit der Galoisgruppe $\mathfrak{G}$. $\mathfrak{p}$ sei ein Primideal im Ring der ganzen Zahlen von F. Dann heißt

$$\mathfrak{G}_\mathfrak{p} := \{\sigma \in \mathfrak{G} \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

die *Zerlegungsgruppe* von $\mathfrak{p}$ über K. Der Fixkörper

$$Z_\mathfrak{p} := \{x \in F \mid \sigma x = x \text{ für alle } \sigma \in \mathfrak{G}_\mathfrak{p}\}$$

heißt *Zerlegungskörper* von $\mathfrak{p}$ über K.

Außerdem induziert jedes $\sigma \in \mathfrak{G}_\mathfrak{p}$ einen Automorphismus

$$\overline{\sigma}: R_F/\mathfrak{p} \to R_F/\mathfrak{p}, \quad a \bmod \mathfrak{p} \mapsto \sigma a \bmod \mathfrak{p}$$

auf dem Restklassenkörper. Man erhält sogar alle Elemente der Galoisgruppe der Restklassenkörper-Erweiterung als Bilder von Elementen aus $\mathfrak{G}_\mathfrak{p}$ (siehe [N], Satz (9.4)).

In unserem Fall sei E der Spurkörper von Δ und F der invariante Spurkörper, also der Spurkörper der Untergruppe der Quadrate von Δ. Dann sind sowohl $\mathfrak{G}' = \mathrm{Gal}(E/\mathbb{Q})$ als auch $\mathfrak{G} = \mathrm{Gal}(F/\mathbb{Q})$ Abelsche Gruppen. Die verschiedenen Primideale $\mathfrak{p}$ über p sind alle konjugiert zueinander, ebenso wie die Gruppen $\mathfrak{G}_\mathfrak{p}$. Für verschiedene $\mathfrak{p}$ über p erhalten wir also die gleiche Zerlegungsgruppe und wir können somit $\mathfrak{G}_p := \mathfrak{G}_\mathfrak{p}$ für ein $\mathfrak{p} \mid p$ setzen. Analog definieren wir $Z_p := Z_\mathfrak{p}$ und entsprechendes für $\mathfrak{G}'$.

Für die Trägheitsgrade der beiden Erweiterungen gilt folgendes

Lemma 1.7.4. *Der Trägheitsgrad von E stimmt mit dem Index f der Erweiterung $\mathbb{F}_q/\mathbb{F}_p$ überein. Ist $(2, m_1, m_\infty)$ ein Ordnungstripel wie in Satz 1.7.2, dann gilt für den Trägheitsgrad f_i der Erweiterung $F/\mathbb{Q}$, dass $f_i = f^*$, wobei f^* definiert ist wie in Satz 1.4.5.*

Beweis. Die erste Aussage ist Inhalt von 1.3.14. Wir betrachten jetzt die Trägheitsgrade: Sind m_1, m_∞ beide ungerade, dann ist $E = F$ und die Bedingung (VZ) ist nicht erfüllt, also $f = f_i = f^*$.

Wir nehmen nun an, m_1 wäre gerade und m_∞ ungerade. Für die Körpergrade folgt dann mit Satz 1.3.13, dass $|E/F|$=2. Es ist also $f_i = f$ oder $f_i = \frac{f}{2}$. σ_1 sei das durch $\zeta_{2m_1} \mapsto -\zeta_{2m_1}$ induzierte Element aus $\mathfrak{G}'$, also $F = \mathrm{Fix}(\sigma_1)$.

Wird der Trägheitsgrad echt kleiner, also $f_i = \frac{f}{2}$, dann war σ_1 in der Zerlegungsgruppe $\mathfrak{G}'_p$, m.a.W. σ_1 induziert ein Element $\overline{\sigma}_1 \in \mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ mit $\overline{\sigma}_1(\tau_1) = -\tau_1$ und $\overline{\sigma}_1(\tau_\infty) = \tau_\infty$. Außerdem hat $\overline{\sigma}_1$ die Ordnung 2, d.h. $\overline{\sigma}_1 = x \mapsto x^{p^{f/2}}$. Daraus folgt $\tau_1 \in \mathbb{F}_q \setminus \mathbb{F}_{p^{f/2}}$ und $\tau_\infty \in \mathbb{F}_{p^{f/2}}$. Nach Satz 1.2.9 ist das Tupel $(2, m_1, m_\infty)$ irregulär, im Widerspruch zur Voraussetzung, d.h. $f_i = f$. Insbesondere kann die Bedingung (VZ) nicht erfüllt werden.

Es seien nun m_1 und m_∞ gerade. σ_1, σ_∞ seien wie oben definiert. Wir betrachten zunächst die Situation, dass $\sigma_1, \sigma_\infty \in \mathfrak{G}'_p$: Dann ist $\overline{\sigma}_1 = x \mapsto x^{p^{f/2}} = \overline{\sigma}_\infty$ und die Bedingung (VZ) ist erfüllt. Weiter sind $\tau_1, \tau_\infty \in \mathbb{F}_q \setminus \mathbb{F}_{p^{f/2}}$, wir haben also ein nicht irreguläres Tripel. Mit $(\zeta_{m_i} + \zeta_{m_i}^{-1})^{p^{f/2}} = \zeta_{m_i} + \zeta_{m_i}^{-1}$ folgt $f_i \leq \frac{f}{2}$. Da $F = \mathrm{Fix}\,(\langle \sigma_1, \sigma_\infty \rangle)$, aber σ_1 und σ_∞ das gleiche Bild in $\mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ haben, gilt sogar $f_i = \frac{f}{2} = f^*$.

Ist $\sigma_1 \in \mathfrak{G}'_p$ und $\sigma_\infty \notin \mathfrak{G}'_p$, dann bildet $x \mapsto x^{p^{f/2}}$ die Spur τ_∞ nicht auf $-\tau_\infty$, also auf τ_∞ ab. Es folgt, dass das Tripel irregulär war, Widerspruch.

Seien schließlich $\sigma_1, \sigma_\infty \notin \mathfrak{G}'_p$. Wäre f gerade, dann würde $x \mapsto x^{p^{f/2}}$ die Spuren τ_1, τ_∞ fest lassen, also $\tau_1, \tau_\infty \in \mathbb{F}_{p^{f/2}}$, Widerspruch. f ist somit ungerade, (VZ) nicht erfüllt und $f = f_i = f^*$. □

Satz 1.7.5. *Mit den Bezeichnungen aus Satz 1.7.2 und F, Z_p wie oben gilt:*

Der Definitionskörper der Kurven X_i ist der Zerlegungskörper Z_p von F. Des weiteren gilt:

(i) Ist $m_\infty = p$, dann bilden die Kurven X_i einen Galois-Orbit.

(ii) Sind $m_1, m_\infty \neq p$ und $(m_1, m_\infty) \leq 2$, dann bilden die X_i ebenfalls eine Bahn unter der Galois-Operation.

(iii) Sind $m_1, m_\infty \neq p$ und $(m_1, m_\infty) > 2$, dann hat man $\frac{\varphi((m_1, m_\infty))}{2}$ verschiedene Bahnen der X_i.

Beweis. Die Kurven X_i können durch die Multiplikator-Paare von g_1 (Fall (i)) bzw. g_1, g_∞ (Fall (ii), (iii)) beschrieben werden. Der Definitionskörper ist somit in F enthalten. Ist $(m_1, m_\infty) \leq 2$, dann sind die Erweiterungen $\mathbb{Q}(\cos\frac{2\pi}{m_1})$ und $\mathbb{Q}(\cos\frac{2\pi}{m_\infty})$ linear disjunkt. Man kann also die Multiplikatoren unabhängig voneinander verändern. Bei (i) und (ii) operiert $\mathrm{Gal}\,(F/\mathbb{Q})$ also transitiv auf den X_i.

Elemente $\sigma \in \mathfrak{G}_p$ induzieren Elemente $\overline{\sigma} \in \mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$, d.h. die Spur-Tupel

$$(\zeta_{2m_i} + \zeta_{2m_i}^{-1}) \quad \text{und} \quad (\sigma(\zeta_{2m_i} + \zeta_{2m_i}^{-1}))$$

sind äquivalent. Alle anderen $\sigma \in \mathfrak{G} \setminus \mathfrak{G}_p$ ändern die Spuren so, dass sich die Abbildung nicht zu einem Element aus $\mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ fortsetzen lässt, d.h. man erhält nicht-äquivalente Spurtupel. Somit ist $\mathfrak{G}_p = U(X)$.

Sei $k = (m_1, m_\infty) > 2$. Wir bestimmen zunächst die Länge einer Galois-Bahn. Als Multiplikatoren von g_1 kommen $\frac{\varphi(m_1)}{2}$ viele Paare in Frage, für die von g_∞ hat man $\frac{\varphi(m_\infty)}{2}$ viele Paare. Lässt man die Multiplikatoren von g_1 unverändert, d.h. $\zeta_{m_1} \mapsto \zeta_{m_1}^{\pm 1}$, dann muss auch $\zeta_k \mapsto \zeta_k^{\pm 1}$ gelten. Durchläuft man alle Multiplikatoren von g_∞, dann wird das Paar $\{\zeta_k, \zeta_k^{-1}\}$ dabei auf $\frac{\varphi(k)}{2}$ viele andere Paare abgebildet. Möchte man die Multiplikatoren von g_1 unverändert lassen, dann hat man also nur $\frac{\varphi(m_\infty)}{\varphi(k)}$ viele Möglichkeiten die Multiplikatoren von g_∞ zu verändern. Die Länge einer Bahn ist somit:

$$\frac{\varphi(m_1)\varphi(m_\infty)}{2\varphi(k)} = \frac{\varphi(k)\varphi([m_1, m_\infty])}{2\varphi(k)} = \frac{\varphi([m_1, m_\infty])}{2}$$

auf allen Tupeln. Wir müssen noch äquivalente Tupel über die Operation von $\mathfrak{G}_p$ miteinander identifizieren. Nach Lemma 1.7.4 hat $\mathfrak{G}_p$ die Größe f^*, die Länge einer Bahn auf den Kurven ist somit $\frac{\varphi([m_1,m_\infty])}{2f^*}$ und es gibt $\frac{\varphi(k)}{2}$ viele Bahnen.

Nach Lemma 1.7.4 stimmt (Bahnenlänge) $\cdot$ (Anzahl Bahnen) mit der Anzahl der Kurven überein und der Satz ist bewiesen. □

Bemerkung. Ist $p = 2$, dann spielt das Vorzeichen und somit auch die Bedingung (VZ) keine Rolle mehr. Außerdem können wir die verschiedenen Kurven über das Tripel der Multiplikator-Paare eines fest gewählten $\mathrm{PSL}_2(\mathbb{F}_q)$-Tripels g_0, g_1, g_∞ beschreiben. Damit liegt der Definitionskörper in F. Wie für $p \neq 2$ ist $U(X) = \mathfrak{G}_2$, d.h. der Definitionskörper ist der Zerlegungskörper.

Sind alle Ordnungen $m_i \neq 2$ und $p \neq 2$, dann hat man ein 2–1-Beziehung zwischen Spurtupeln und Multiplikatortupeln. Ändert man ein Vorzeichen bei den Spuren, so erhält man eine andere Kurve, aber das Multiplikatortupel bleibt gleich. Die Information aus den Multiplikatoren der g_i ist hier also nicht ausreichend um die Kurven bzw. die Galois-Operation auf den Kurven zu beschreiben.

Kapitel 2

Kerne und Quaternionenalgebren

Wir wollen zu Beginn die für uns wichtigsten Fakten über Ordnungen in Quaternionenalgebren bzw. zentralen einfachen Algebren zusammenstellen. Für eine ausführliche Behandlung siehe z.B. [MR], [R], [V].

2.1 Quaternionenalgebren

Eine Quaternionenalgebra A über K ist ein K-Vektorraum mit Basis $1, i, j, k$, der bei Multiplikation die Relationen

$$i^2 = a,\ j^2 = b,\ ij = -ji = k, \quad a, b \in K^*$$

erfüllt, wobei 1 die Rolle des multiplikativen Neutralelements übernimmt. Durch Angabe der Daten a, b, K ist A somit bestimmt, und kann durch das Hilbertsymbol angegeben werden

$$A = \left(\frac{a, b}{K}\right).$$

Setzt man $i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ und $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so erhält man z.B. die Quaternionenalgebra

$$\mathrm{M}_2(K) \cong \left(\frac{1, 1}{K}\right).$$

Es gelten:

(1) $A' = \left(\frac{x^2 a, y^2 b}{K}\right) \cong \left(\frac{a,b}{K}\right) = A.$

(Denn über

$$1' \mapsto 1,\ i' \mapsto xi,\ j' \mapsto yj,\ k' \mapsto xyk$$

wird ein Isomorphismus definiert.)

(2) Das Zentrum von $A = \left(\frac{a,b}{K}\right)$ ist K.

(Sei $\overline{K}$ der algebraische Abschluss von K. Dann gilt

$$\overline{K} \otimes_K A = \left(\frac{a,b}{\overline{K}}\right) \cong \left(\frac{1,1}{\overline{K}}\right) \cong \mathrm{M}_2(\overline{K}).$$

Das Zentrum von $\mathrm{M}_2(\overline{K})$ ist $\overline{K}$ und daher hat A das Zentrum K.)

(3) A ist eine einfache Algebra.

(Sei I ein nichttriviales Ideal in A. Dann ist $\overline{K} \otimes_K I$ ein nichttriviales Ideal in $\mathrm{M}_2(\overline{K})$, also gleich $\mathrm{M}_2(\overline{K})$. I ist also ein 4-dimensionaler K-Untervektorraum von A.)

(4) (2)+(3) besagt also, dass jede Quaternionenalgebra eine zentrale einfache Algebra der Dimension 4 ist. Es gilt auch die Umkehrung, denn mit dem Satz von Skolem-Noether folgt: Ist die Charakteristik von K ungleich 2, dann ist jede 4-dimensionale zentrale einfache K-Algebra eine Quaternionenalgebra.

(5) *Struktursatz von Wedderburn:* Jede einfache Algebra A endlicher Dimension über K ist von der Form $A \cong \mathrm{M}_n(D)$, wobei D eine Divisionsalgebra über K ist. n und D sind dabei eindeutig durch A bestimmt.

Für eine Quaternionenalgebra hat man also die Möglichkeiten:

$$A \cong \mathrm{M}_2(K) \quad \text{oder} \quad A \cong D.$$

(6) Ist a oder b ein Quadrat in K, so ist $\left(\frac{a,b}{K}\right) \cong \mathrm{M}_2(K)$.

(O.b.d.A. ist $\left(\frac{a,b}{K}\right) \cong \left(\frac{1,b}{K}\right)$, also $i^2 = 1$ und wegen $(i-1)(i+1) = i^2 - 1 = 0$ hat man Nullteiler.)

Mit (1)+(5) folgt jetzt für $K = \mathbb{R}$, dass man sogar insgesamt nur zwei Quaternionenalgebren über $\mathbb{R}$ hat, nämlich

$$\mathrm{M}_2(\mathbb{R}) \cong \left(\frac{1,1}{\mathbb{R}}\right) \quad \text{und} \quad \mathbb{H} \cong \left(\frac{-1,-1}{\mathbb{R}}\right),$$

wobei $\mathbb{H}$ die Hamiltonschen Quaternionen bezeichnet.

Entsprechendes gilt über den vollständigen p-adischen Körpern: Es gibt genau eine Divisions-Quaternionenalgebra.

(7) Jede Quaternionenalgebra über K lässt sich in $\mathrm{M}_2(L)$ einbetten, mit $|L : K| = 1, 2$.
(Setze $L := K(\sqrt{a})$. Dann ist $L \otimes_K A \cong \mathrm{M}_2(L)$.)

(8) Als *reine* Quaternionen bezeichnet man die Elemente des von i, j, k aufgespannten Untervektorraums A_0. Diese Definition ist unabhängig von der Wahl der Basis. Man hat für $x \in A$ also eine eindeutige Zerlegung

$$x = \xi_0 + \xi_1 \qquad \text{mit} \quad \xi_0 \in K \text{ und } \xi_1 \in A_0.$$

Das *Konjugierte* zu x ist $\overline{x} = \xi_0 - \xi_1$ und die *(reduzierte) Norm* und *Spur* sind definiert als

$$\mathrm{n}(x) = x \cdot \overline{x} = \overline{x} \cdot x \in K \quad \text{und} \quad \mathrm{tr}(x) = x + \overline{x} \in K.$$

In $\mathrm{M}_2(L)$ entspricht die Norm der Determinante und die Spur der gewöhnlichen Spur einer Matrix.

(9) Jedes $x \in A$ erfüllt die Polynomgleichung

$$x^2 - \mathrm{tr}(x)x + \mathrm{n}(x) = 0.$$

(10) Durch $T(x, y) := \mathrm{tr}(xy)$ ist eine nicht-ausgeartete symmetrische Bilinearform auf A definiert.

(11) Oft ist es hilfreich von einer (Quaternionen-)Algebra A über K zu ihrer $\mathfrak{p}$-adischen Komplettierung überzugehen: Ist $\widehat{K}_\mathfrak{p}$ die Komplettierung von K an der Stelle $\mathfrak{p}$, so setzen wir $\widehat{A}_\mathfrak{p} := \widehat{K}_\mathfrak{p} \otimes_K A$. $\widehat{A}_\mathfrak{p}$ ist dann entweder isomorph zu der Divisionsalgebra über $\widehat{K}_\mathfrak{p}$; in diesem Fall nennen wir A *verzweigt* an der Stelle $\mathfrak{p}$. Oder es ist $\widehat{A}_\mathfrak{p} \cong \mathrm{M}_2(\widehat{K}_\mathfrak{p})$, und man sagt A *zerfällt* in $\mathfrak{p}$.

(12) Die bis auf Isomorphie eindeutige Divisions(quaternionen)algebra $\widehat{A}$ über einem vollständigen bewerteten Körper $\widehat{K}$ mit Bewertungsring $\widehat{R}$ lässt sich genauer angeben:

Zu $\widehat{K}$ gibt es eine eindeutig bestimmte unverzweigte quadratische Erweiterung $\widehat{L}$, wobei $\widehat{L} = \widehat{K}(\sqrt{u})$ für ein $u \in \widehat{R}$ ([MR], 0.7.13). Da es sich um eine Erweiterung vollständiger bewerteter Körper handelt, ist der Trägheitsgrad hier gleich 2. Die Divisionsalgebra ist dann isomorph zu

$$\left(\frac{u, \pi}{\widehat{K}}\right),$$

wobei π die Uniformisierende in $\widehat{R}$ ist ([MR], 2.6.3). Außerdem gilt $\widehat{L} \otimes_{\widehat{K}} \widehat{A} \cong \mathrm{M}_2(\widehat{L})$.

2.2 Ordnungen

Sei R ein Integritätsbereich mit Quotientenkörper K und A eine endlichdimensionale K-Algebra. Dann gilt

$$\begin{aligned} x \in A \text{ ist ganz} \quad &:\Leftrightarrow \quad f(x) = 0 \text{ für ein normiertes Polynom } f \in R[X] \\ &\Leftrightarrow \quad R[x] \text{ ist ein endlich erzeugter } R\text{-Modul.} \end{aligned}$$

Ist R ein Dedekindring, d.h. ein ganzabgeschlossener Noetherscher Ring, in dem jedes nichttriviale Primideal maximal ist, und A eine Quaternionenalgebra, so gilt sogar

$$x \in A \text{ ist ganz} \quad \Leftrightarrow \quad \mathrm{tr}(x), \mathrm{n}(x) \in R.$$

Ist K ein algebraischer Zahlkörper, so bilden die (über $\mathbb{Z}$) ganzen Elemente einen Ring R_K. So ist z.B. $R_K = \mathbb{Z}[\zeta]$ für einen Kreisteilungskörper $K = \mathbb{Q}(\zeta)$, mit n-ter Einheitswurzel ζ und $R_K = \mathbb{Z}[2\cos\frac{2\pi}{n}]$ für $K = \mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{n})$.

Im Fall einer Quaternionenalgebra ist das i.d.R. nicht so: Z.B. sind

$$x = \begin{pmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{pmatrix}$$

ganz in $A = \mathrm{M}_2(\mathbb{Q})$, aber $x + y$ nicht. Die Rolle des Rings ganzer Zahlen R_K in einem algebraischen Zahlkörper übernehmen hier die Ordnungen.

Definition 2.2.1. Sei R ein Dedekindring mit Quotiontenkörper K und sei A eine Quaternionenalgebra über K.

- Ein *R-Gitter* L in einem K-Vektorraum V ist ein endlich erzeugter R-Modul.
- $L \leq V$ ist ein *volles R-Gitter*, falls zusätzlich $K \otimes_R L \cong V$ gilt.
- Ein *Ideal* in A ist ein volles R-Gitter.
- Eine *Ordnung* $\mathcal{O}$ in A ist ein Ideal, das gleichzeitig ein Ring mit 1 ist. Oder äquivalent dazu: $\mathcal{O}$ ist ein Ring ganzer Zahlen in A mit $R \subset \mathcal{O}$ und $K \cdot \mathcal{O} = A$.
- Eine *maximale Ordnung* in A ist eine Ordnung, die maximal bzgl. Inklusion ist.

Beispiel 2.2.2. Ist I ein Ideal in A, dann kann man I seine *Linksordnung*

$$\mathcal{O}_l(I) := \{\alpha \in A \mid \alpha I \subset I\}$$

und seine *Rechtsordnung*

$$\mathcal{O}_r(I) := \{\alpha \in A \mid I\alpha \subset I\}$$

zuordnen.

Definition 2.2.3. Sei I ein Ideal in A. Wir nennen I

- *beidseitig*, falls $\mathcal{O}_l(I) = \mathcal{O}_r(I)$,
- *normal*, falls $\mathcal{O}_l(I)$ und $\mathcal{O}_r(I)$ maximale Ordnungen sind und
- *ganz*, falls $I \subset \mathcal{O}_l(I), \mathcal{O}_r(I)$.

Beobachtung 2.2.4. *Sei $\mathcal{O}$ eine maximale Ordnung. Ist I ein beidseitiges Ideal in $\mathcal{O}$ im herkömmlichen Sinn (d.h. ein beidseitiges Ideal in dem Ring $\mathcal{O}$) mit $K \cdot I = A$, dann ist I beidseitig, normal und ganz als Ideal in A.*

Ist R ein Dedekindring, so lässt sich die Idealtheorie auf die Ideale in A fortsetzen: Jedes beidseitige Ideal in einer maximalen Ordnung lässt sich eindeutig bis auf Reihenfolge in ein Produkt von Primidealen zerlegen ([R], (23.6)) und wie in Dedekindringen sind die Primideale maximale Ideale ([R], (22.3)). Ist K ein algebraischer Zahlkörper, so gibt es außerdem eine 1-1-Beziehung zwischen den Primidealen in einer maximalen Ordnung und den Primidealen in R, genauer:

Satz 2.2.5 ([R], (32.1))**.** *Sei R ein Dedekindring, dessen Quotientenkörper $K \neq R$ ein globaler Körper ist. $\mathcal{O}$ sei eine maximale Ordnung in der zentralen einfachen K-Algebra A. Die Primideale $\mathfrak{p}$ von R und die Primideale $\mathfrak{P}$ von $\mathcal{O}$ lassen sich einander ein-eindeutig zuordnen durch:*

$$\mathfrak{p} = R \cap \mathfrak{P} \quad \text{und} \quad \mathfrak{P} \mid \mathfrak{p}\mathcal{O}.$$

Im Spezialfall, dass A eine Quaternionenalgebra ist, lässt sich $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}$ präzisieren zu: $\mathfrak{P} = \mathfrak{p}\mathcal{O}$, falls A in $\mathfrak{p}$ zerfällt und $\mathfrak{P}^2 = \mathfrak{p}\mathcal{O}$, falls A in $\mathfrak{p}$ verzweigt.

Über lokalen Körpern ist die Situation wie folgt: Es sei $\widehat{R}$ ein vollständiger diskreter Bewertungsring mit Quotientenkörper $\widehat{K}$ und Bewertung

$$v = v_{\mathfrak{p}} : \widehat{K}^* \to \mathbb{Z},$$

Uniformisierender π, maximalem Ideal $\widehat{\mathfrak{p}} = \pi\widehat{R}$ und Restklassenkörper $\kappa = \widehat{R}/\widehat{\mathfrak{p}} \cong \mathbb{F}_q$, wobei $q = p^f$, und $\widehat{A} = \mathrm{M}_r(D)$ sei eine zentrale einfache $\widehat{K}$-Algebra, wobei D eine Divisionsalgebra über $\widehat{K}$ ist. Die Bewertung auf $\widehat{K}$ lässt sich durch Vorschalten der Norm von D über $\widehat{K}$ zu einer Bewertung auf D fortsetzen (vgl. [R] Kap. 12). $\mathcal{D}$ sei der zugehörige Bewertungsring mit Uniformisierender π_D. Es gilt

Satz 2.2.6 ([R] (17.3),(17.5))**.** *Mit den Bezeichnungen aus dem obigen Absatz gilt:*

(i) Sei $\widehat{\mathcal{O}} = \mathrm{M}_r(\mathcal{D})$. Dann ist $\widehat{\mathcal{O}}$ eine maximale $\widehat{R}$-Ordnung in $\widehat{A}$ und hat ein eindeutig bestimmtes maximales beidseitiges Ideal $\widehat{\mathfrak{P}} = \pi_D\widehat{\mathcal{O}}$. Die Potenzen

$$\widehat{\mathfrak{P}}^m = \pi_D^m\widehat{\mathcal{O}}, \quad m = 0, 1, 2, \ldots,$$

bilden alle nichttrivialen beidseitigen Ideale von $\widehat{\mathcal{O}}$.

(ii) Jede maximale $\widehat{R}$-Ordnung in $\widehat{A}$ ist von der Form $u\widehat{\mathcal{O}}u^{-1}$ für ein $u \in \widehat{A}^*$, und jeder solche Ring ist eine maximale Ordnung.

(iii) Für jede maximale $\widehat{R}$-Ordnung $\widehat{\mathcal{O}}$ in $\widehat{A}$ gilt

$$\operatorname{rad}\widehat{\mathcal{O}} = \widehat{\mathfrak{P}} \quad \text{und} \quad \widehat{\mathcal{O}}/\operatorname{rad}\widehat{\mathcal{O}} \cong \mathrm{M}_r(\mathcal{D}/\operatorname{rad}\mathcal{D}),$$

wobei rad *das Jacobson-Radikal bezeichnet.*

Was bedeutet das für den konkreten Fall, dass $\widehat{A}$ eine Quaternionenalgebra über der Komplettierung $\widehat{K}$ eines algebraischen Zahlkörpers K ist?

$\widehat{A}$ ist dann entweder von der Form

$$\widehat{A} = \mathrm{M}_2(\widehat{K}) \quad \text{oder} \quad \widehat{A} = D,$$

wobei D eine Divisionsalgebra vom Grad 4 über $\widehat{K}$ ist.

Ist $\widehat{A} = D$, so erhält man die Bewertung auf D über die reduzierte Norm der Quaternionenalgebra, nämlich durch

$$w : D^* \to \mathbb{Z} \quad \text{mit } w(x) := v(\mathrm{n}(x)).$$

Der Bewertungsring ist dann

$$\mathcal{D} := \{\, x \in D \mid w(x) \geq 0 \}\,.$$

Das sind bereits alle ganzen Elemente in D, d.h. $\mathcal{D}$ ist *die* maximale Ordung in D und das maximale Ideal in $\mathcal{D}$ ist

$$\widehat{\mathfrak{P}} = \{\, x \in D \mid w(x) > 0 \}\,.$$

Außerdem sind Verzweigungs- und Trägheitsindex der Erweiterung $D/\widehat{K}$ jeweils gleich 2 (siehe [R] (14.3)), d.h. $|\mathcal{D}/\widehat{\mathfrak{P}} : \kappa| = 2$ und $\widehat{\mathfrak{P}}^2 = \pi\mathcal{D}$.

Ist $\widehat{A} = \mathrm{M}_2(\widehat{K})$, dann ist jede maximale Ordnung konjugiert zu $\mathrm{M}_2(\widehat{R})$ und die beidseitigen Ideale in $\mathrm{M}_2(\widehat{R})$ sind Potenzen des maximalen Ideals $\pi\mathrm{M}_2(\widehat{R})$.

Wir wollen nun die Quotienten $\widehat{\mathcal{O}}/\widehat{\mathfrak{P}}$ aus Satz 2.2.6 im Falle von Quaternionenalgebren näher bestimmen.

Ist $\widehat{A} = \mathrm{M}_2(\widehat{K})$, dann ist $\mathcal{D} = \widehat{R}$. Das Radikal eines Rings lässt sich berechnen als der Schnitt über alle maximalen Linksideale (siehe [R] (6.3)). In $\widehat{R}$ gibt es aber nur ein maximales Ideal, nämlich $\pi\widehat{R}$, d.h. $\operatorname{rad}\widehat{R} = \widehat{\mathfrak{p}}$.

Sei nun $\widehat{A} = D$, $\mathcal{D}$ der Bewertungsring von D. Dann ist $\widehat{\mathcal{O}} = \mathcal{D}$ und nach Satz 2.2.6 ist $\operatorname{rad}\mathcal{D} = \widehat{\mathfrak{P}} = \pi_D\mathcal{D}$.

Lemma 2.2.7. *Mit diesen Bezeichnungen gilt:*

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{P}} = \begin{cases} \mathrm{M}_2(\widehat{R}/\pi\widehat{R}) \cong \mathrm{M}_2(\mathbb{F}_q), & \text{wenn } \widehat{A} = \mathrm{M}_2(\widehat{K}), \\ \mathcal{D}/\pi_D\mathcal{D} \cong \mathbb{F}_{q^2}, & \text{wenn } \widehat{A} = D. \end{cases}$$

Korollar 2.2.8. *Sei* $\widehat{\mathcal{O}} \cong \mathrm{M}_2(\widehat{R})$ *und* $\widehat{I} := \ker\left(\mathrm{M}_2(\widehat{R}) \to \mathrm{M}_2(\widehat{R}/\widehat{\mathfrak{p}})\right)$. *Dann ist* $\widehat{I} = \widehat{\mathfrak{P}}$.

Beweis. Es ist $\widehat{\mathcal{O}}/\widehat{I} \cong \mathrm{M}_2(\mathbb{F}_q) \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{P}}$. Nach Satz 2.2.6 ist $\widehat{\mathfrak{P}} = \pi\widehat{\mathcal{O}}$, also $\widehat{\mathfrak{P}} \subset \widehat{I}$. Außerdem ist $\widehat{I}$ ein beidseitiges Ideal in $\widehat{\mathcal{O}}$, also enthalten in $\widehat{\mathfrak{P}}$. Es folgt $\widehat{I} = \widehat{\mathfrak{P}}$. □

2.3 Die Quaternionenalgebra zu einer Fuchsschen Gruppe

Wir wollen nun einer Fuchsschen Gruppe Γ eine Quaternionenalgebra zuordnen, die Γ in ihrer Norm-1-Untergruppe enhält. Diese Konstuktion wird ausführlich in [MR] duchgeführt.

Sei $\Gamma \leq \mathrm{PSL}_2(\mathbb{C})$. Γ heißt *reduzibel*, falls alle Elemente einen gemeisamen Fixpunkt bzgl. der Operation auf $\mathbb{C}_\infty$ besitzen, andernfalls *irreduzibel*.

Lemma 2.3.1 ([MR], 1.2.3)**.** *Seien* $\gamma_0, \gamma_1 \in \mathrm{PSL}_2(\mathbb{C})$. $\langle\gamma_0, \gamma_1\rangle$ *ist reduzibel* $\Leftrightarrow \operatorname{tr}[\gamma_0, \gamma_1] = 2$.

Beweis. Die Gruppe sei reduzibel und der gemeinsame Fixpunkt sei o.B.d.A. ∞, d.h. alle Matrizen sind trigonalisiert. Aus

$$\begin{pmatrix} \lambda & * \\ 0 & \lambda^{-1} \end{pmatrix} \cdot \begin{pmatrix} \mu & * \\ 0 & \mu^{-1} \end{pmatrix} = \begin{pmatrix} \lambda\mu & * \\ 0 & \lambda^{-1}\mu^{-1} \end{pmatrix}$$

ersieht man, dass

$$[\gamma_0, \gamma_1] = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Sei nun die Spur des Kommutators 2. Wir nehmen zunächst an γ_0 habe genau einen Fixpunkt und zwar o.B.d.A. ∞.

$$\begin{aligned} [\gamma_0, \gamma_1] &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \begin{pmatrix} 1 + ac + c^2 & * \\ * & 1 - ac \end{pmatrix}, \end{aligned}$$

d.h. $2 = \mathrm{tr}[\gamma_0, \gamma_1] = 2 + c^2$, also $c = 0$ und ∞ ist ein gemeinsamer Fixpunkt.

Nun habe γ_0 zwei verschiedene Fixpunkte und zwar 0 und ∞.

$$\begin{aligned} [\gamma_0, \gamma_1] &= \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \begin{pmatrix} ad - \lambda^2 bc & * \\ * & ad - \lambda^{-2} bc \end{pmatrix}, \end{aligned}$$

also $2 = 2ad - bc(\lambda^2 + \lambda^{-2}) = 2 - bc(\lambda - \lambda^{-1})^2$. Es folgt $bc = 0$ und 0 oder ∞ ist ein gemeinsamer Fixpunkt, oder $\lambda = \lambda^{-1}$ und γ_0 ist die Identität. □

Schreibt man die Einträge von 1, γ_0, γ_1, $\gamma_0\gamma_1$ in die Spalten einer 4×4-Matrix $M(\gamma_0, \gamma_1)$, so erhält man

$$\det M(\gamma_0, \gamma_1) = 2 - \mathrm{tr}[\gamma_0, \gamma_1],$$

m.a.W., $\langle \gamma_0, \gamma_1 \rangle$ ist genau dann irreduzibel, wenn 1, γ_0, γ_1, $\gamma_0\gamma_1$ über $\mathbb{C}$ linear unabhängig sind.

Satz 2.3.2 ([MR], 3.2.1)**.** *Die Untergruppe $\Gamma \leq \mathrm{PSL}_2(\mathbb{C})$ enthalte zwei Elemente γ_0, γ_1, so dass $\langle \gamma_0, \gamma_1 \rangle$ irreduzibel ist. Dann definiert*

$$A_0\Gamma := \mathbb{Q}(\mathrm{tr}\Gamma)[\Gamma] = \left\{ \sum_{\text{endl.}} a\gamma \;\middle|\; a \in \mathbb{Q}(\mathrm{tr}\Gamma), \gamma \in \Gamma \right\}$$

eine Quaternionenalgebra über $\mathbb{Q}(\mathrm{tr}\Gamma)$.

Beweis. Nach dem Lemma ist $\mathbb{C} \cdot A_0\Gamma = \mathrm{M}_2(\mathbb{C})$. Liegt x im Zentrum von $A_0\Gamma$, dann auch im Zentrum von $\mathrm{M}_2(\mathbb{C})$, x ist also ein Vielfaches der Einheitsmatrix, m.a.W. $A_0\Gamma$ ist zentral.

Zu $v_j \in \{1, \gamma_0, \gamma_1, \gamma_0\gamma_1\}$ ist $T(-, v_j)$ eine Basis im Dualraum, wobei T die symmetrische Bilinearform aus 2.1 (10) auf $\mathrm{M}_2(\mathbb{C})$ ist. Sei v_i^* die dazu duale Basis, d.h. $T(v_i^*, v_j) = \delta_{ij}$. Sei $\gamma \in \Gamma$ beliebig und

$$\gamma = \sum \xi_i v_i^* \quad \text{mit } \xi_i \in \mathbb{C}.$$

Dann folgt $\xi_j = T(\gamma, v_j) \in \mathbb{Q}(\mathrm{tr}\Gamma)$. $A_0\Gamma$ ist also in einem $\mathbb{Q}(\mathrm{tr}\Gamma)$-Vektorraum der Dimension 4 enthalten, ist also selbst ein $\mathbb{Q}(\mathrm{tr}\Gamma)$-Vektorraum der Dimension 4.

Schließlich sei $I \neq 0$ ein beidseitiges Ideal in $A_0\Gamma$, d.h. $\mathbb{C} \cdot I$ ist ein beidseitiges Ideal in $\mathrm{M}_2(\mathbb{C})$, also $\mathbb{C} \cdot I = \mathrm{M}_2(\mathbb{C})$. I hat somit Dimension ≥ 4 über $\mathbb{Q}(\mathrm{tr}\Gamma)$. □

Satz 2.3.3. *Sind alle Spuren von* Γ *ganze algebraische Zahlen, so ist*

$$\mathcal{O}\Gamma := R_{\mathbb{Q}(\mathrm{tr}\Gamma)}[\Gamma] = \left\{ \sum_{\text{endl.}} a\gamma \;\middle|\; a \in R_{\mathbb{Q}(\mathrm{tr}\Gamma)}, \gamma \in \Gamma \right\}$$

eine Ordnung in A.

Beweis. Es genügt zu zeigen, dass $\mathcal{O}\Gamma$ ein Ring ganzer Zahlen ist, der $R_{\mathbb{Q}(\mathrm{tr}\,\Gamma)}$ enthält, mit $\mathbb{Q}(\mathrm{tr}\,\Gamma) \cdot \mathcal{O}\Gamma = A_0\Gamma$. Offensichtlich sind $\mathbb{Q}(\mathrm{tr}\,\Gamma) \cdot \mathcal{O}\Gamma = A_0\Gamma$ und $R_{\mathbb{Q}(\mathrm{tr}\,\Gamma)} \subset \mathcal{O}\Gamma$ erfüllt und $\mathcal{O}\Gamma$ ist ein Ring. Zu zeigen bleibt die Ganzheit.

Ein Element einer Quaternionenalgebra ist genau dann ganz, wenn seine Spur und Norm algebraische ganze Zahlen sind. Nach der Voraussetzung über die Spuren von Γ sind die Spuren aller Elemente aus $\mathcal{O}\Gamma$ ganz. Des weiteren ist $\mathrm{n}(a\gamma) = a^2 \in R_{\mathbb{Q}(\mathrm{tr}\,\Gamma)}$. Wir müssen also nur noch die Norm der Summe zweier Elemente betrachten.

Seien $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathcal{O}\Gamma$ mit ganzzahliger Determinante.

$$\det(x+y) = \underbrace{ad - bc + \alpha\delta - \beta\gamma}_{\in R} + a\delta + d\alpha - b\gamma - c\beta$$

Aus $a + d, \alpha + \delta \in R$ folgt $(a+d)(\alpha+\delta) = a\alpha + d\delta + a\delta + d\alpha \in R$ und aus $\mathrm{tr}\,(x \cdot y) \in R$ folgt $a\alpha + d\delta + b\gamma + c\beta \in R$ und schließlich

$$a\delta + d\alpha - b\gamma - c\beta = (a\alpha + d\delta + a\delta + d\alpha) - (a\alpha + d\delta + b\gamma + c\beta) \in R. \quad \square$$

Für den Fall einer Dreiecksgruppe Δ vom Typ (m_0, m_1, m_∞) ist

$$\mathrm{tr}(\Delta) \subset \mathbb{Z}[2\cos\tfrac{\pi}{m_0}, 2\cos\tfrac{\pi}{m_1}, 2\cos\tfrac{\pi}{m_\infty}],$$

und somit ist $\mathcal{O}\Delta$ eine Ordnung in $A_0\Delta$.

Bemerkung. Möchte man der Gruppe Γ eine Quaternionenalgebra als Invariante der Kommensurabilitätsklasse von Γ zuordnen, so muss man, wie beim Spurkörper, $A_0\Gamma^{(2)}$ statt $A_0\Gamma$ betrachten ([MR], 3.3.5).

2.4 Projektionen auf $\mathrm{PSL}_2\mathbb{F}_q$

Wir möchten nun die Projektionen einer Dreiecksgruppe $\Delta = \Delta(m_0, m_1, m_\infty)$ mit „schönem“ Ordnungstripel auf $\mathrm{PSL}_2(\mathbb{F}_q)$, $q = p^f$, aus Satz 1.4.5 über die Δ zugeordnete Quaternionenalgebra $A = A_0\Delta$ beschreiben. Dabei verstehen wir unter einem schönen Tripel ein p-zulässiges, nicht irreguläres Tripel, das zu einer maximalen Fuchsschen Gruppe oder einer Gruppe vom Typ $(2, m, 2m)$ oder $(3, m, 3m)$ gehört. E bezeichne wieder den Spurkörper von Δ. Wir betrachten zunächst den Übergang zu einer Komplettierung $\widehat{A}_\mathfrak{p} = \widehat{E}_\mathfrak{p} \otimes_E A$ an der Stelle $\mathfrak{p}$ über p. $\tilde{\Delta}$ sei das Urbild von Δ in $\mathrm{SL}_2(\mathbb{R})$, $\mathcal{O}$ sei eine maximale Ordnung in A, die $\mathcal{O}\Gamma$ enthält und $\widehat{\mathcal{O}}_E$ sei eine maximale Ordnung in $\widehat{A}_\mathfrak{p}$, die $\mathcal{O}$ enthält. Nach 2.2.7 haben wir folgende Situation:

$$\tilde{\Delta} \subset \mathcal{O} \hookrightarrow \widehat{\mathcal{O}}_E \twoheadrightarrow \widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}} \cong \begin{cases} \mathrm{M}_2(\mathbb{F}_q), & \mathfrak{p} \notin \mathrm{Ram}\,(A), \\ \mathbb{F}_{q^2}, & \mathfrak{p} \in \mathrm{Ram}\,(A). \end{cases}$$

Im verzweigten Fall können wir die Komplettierung mit der quadratischen Erweiterung $\widehat{L}/\widehat{E}_\mathfrak{p}$ vom Trägheitsgrad 2 aus 2.1(12) tensorieren und erhalten

$$\tilde{\Delta} \subset \mathcal{O} \hookrightarrow \widehat{\mathcal{O}}_E \hookrightarrow \widehat{\mathcal{O}}_L \twoheadrightarrow \widehat{\mathcal{O}}_L/\widehat{\mathfrak{P}}_L \cong \mathrm{M}_2(\mathbb{F}_{q^2}),$$

mit einer maximalen Ordnung $\widehat{\mathcal{O}}_L$ in $\widehat{L} \otimes_{\widehat{E}_\mathfrak{p}} \widehat{A}_\mathfrak{p} \cong \mathrm{M}_2(\widehat{L})$.

Lemma 2.4.1. *Beim Übergang von $\widehat{\mathcal{O}}_E$ zu $\widehat{\mathcal{O}}_L$ gilt $\widehat{\mathfrak{P}} = \widehat{\mathfrak{P}}_E \subset \widehat{\mathfrak{P}}_L$.*

Beweis. $\widehat{R}_L \otimes_{\widehat{R}_E} \widehat{\mathfrak{P}}_K$ ist ein Ideal in $\widehat{\mathcal{O}}_L$, d.h. $\widehat{\mathfrak{P}}_L \mid \widehat{R}_L \otimes_{\widehat{R}_E} \widehat{\mathfrak{P}}_E$. □

In $\widehat{\mathcal{O}}_L/\widehat{\mathfrak{P}}_L$ betrachten wir nun den Unterring $\widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_L$. Für diesen gilt:

Lemma 2.4.2. *In $\widehat{\mathcal{O}}_L/\widehat{\mathfrak{P}}_L$ ist $\widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_L \cong \widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_E$.*

Beweis. Zwei Elemente in $\widehat{\mathcal{O}}_E$ sind kongruent modulo $\widehat{\mathfrak{P}}_L$, falls ihre Differenz in $\widehat{\mathfrak{P}}_L \cap \widehat{\mathcal{O}}_E = \widehat{\mathfrak{P}}_E$ liegt. Also $\widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_L = \widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_L \cap \widehat{\mathcal{O}}_E = \widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_E$. □

Nach 2.2.8 ist $\widehat{\mathfrak{P}}_L = \ker(\mathrm{M}_2(\widehat{R}_L) \to \mathrm{M}_2(\widehat{R}_L/\widehat{\mathfrak{p}}_L))$, d.h. die Quotientenbildung nach $\widehat{\mathfrak{P}}_L$ ist nichts anderes, als wenn man die Einträge in den Matrizen modulo dem Primideal $\widehat{\mathfrak{p}}_L$ in $\widehat{R}_L$ betrachtet. Demnach ist $\mathrm{tr}\,(\gamma_i + \widehat{\mathfrak{P}}_L) = \mathrm{tr}\,\gamma_i \bmod \widehat{\mathfrak{p}}_L$. Ist m_i teilerfremd zu p, dann ist ζ_{2m_i} (bzw. ζ_{m_i}) auch im Restklassenkörper noch eine primitive Einheitswurzel, d.h. das Element im Quotienten hat die gleiche Ordnung wie γ_i. Ist eine Ordnung gleich p, o.B.d.A. $m_0 = p$, dann sind m_1, m_∞ verschieden, ungleich p und wegen der p-Zulässigkeit auch teilerfremd zu p. Die Ordnungen von γ_1, γ_∞ bleiben also im Quotienten erhalten. Daraus folgt

$$1 \neq \mathrm{ord}\,(\gamma_0 + \widehat{\mathfrak{P}}) \mid \mathrm{ord}\,\gamma_0 = p,$$

also bleibt auch die Ordnung von γ_0 erhalten.

Sei $\overline{\mathbb{F}}_p$ der algebraische Abschluss von $\mathbb{F}_p$. Nach Voraussetzung haben wir das Ordnungstripel so gewählt, dass die in $\mathrm{PSL}_2(\overline{\mathbb{F}}_p)$ erzeugte Gruppe isomorph zu $\mathrm{PSL}_2(\mathbb{F}_q)$ ist. Wäre A bei $\mathfrak{p}$ verzweigt, dann würden die γ_i also einerseits auf Elemente in $\mathrm{M}_2(\mathbb{F}_{q^2})$ abgebildet, die $\mathrm{PSL}_2(\mathbb{F}_q)$ erzeugen. Andererseits sind die γ_i in $\widehat{\mathcal{O}}_E$ enthalten, d.h. sie erzeugen in $\mathrm{M}_2(\mathbb{F}_{q^2})$ eine Untergruppe, die in $\widehat{\mathcal{O}}_E/\widehat{\mathfrak{P}}_L \cong \mathbb{F}_{q^2}$ enthalten ist und wir erhalten einen Widerspruch. Also gilt:

Lemma 2.4.3. *Sei (m_0, m_1, m_∞) ein p-„schönes“ Ordnungstripel. Dann ist A bei $\mathfrak{p} \mid p$ unverzweigt.*

Nach Voraussetzung ist also $\widehat{A}_\mathfrak{p} \cong \mathrm{M}_2(\widehat{E}_\mathfrak{p})$. In $\mathrm{M}_2(\widehat{E}_\mathfrak{p})$ ist jede maximale Ordnung konjugiert zu $\mathrm{M}_2(R_{\widehat{E}_\mathfrak{p}})$, d.h. wir bekommen eine Abbildung $\Delta \to \mathrm{PSL}_2(\mathbb{F}_q)$ über

$$\begin{array}{ccccccc} \Delta \twoheadleftarrow \tilde{\Delta} \subset & \mathcal{O} & \hookrightarrow & \widehat{\mathcal{O}}_\mathfrak{p} & \overset{\text{konj.}}{\to} & \mathrm{M}_2(R_{\widehat{E}_\mathfrak{p}}) & \to \mathrm{M}_2(R_{\widehat{E}_\mathfrak{p}}/\widehat{\mathfrak{p}}) \cong \mathrm{M}_2(\mathbb{F}_q) \\ & \cap & & \cap & & \cap & \\ & A & \hookrightarrow & \widehat{A}_\mathfrak{p} & \cong & \mathrm{M}_2(\widehat{E}_\mathfrak{p}) & \end{array}$$

wobei $\widehat{\mathcal{O}}_\mathfrak{p}$ eine maximale Ordnung in $\widehat{A}_\mathfrak{p}$ ist, die $\mathcal{O}$ enthält. Es wird ein Ringhomomorphismus $\tilde{\varphi} : \mathcal{O} \to \mathrm{M}_2(\mathbb{F}_q)$ induziert. $I := \ker\tilde{\varphi}$ ist also ein zweiseitiges Ideal in $\mathcal{O}$. Ist $\beta \in \mathfrak{p}\mathcal{O}$, d.h. in $\mathrm{M}_2(R_{\widehat{E}_\mathfrak{p}})$ enthält jeder Eintrag der zu β gehörigen Matrix einen Faktor $\rho \in \mathfrak{p} \subseteq \widehat{\mathfrak{p}}$, dann ist $\tilde{\varphi}(\beta) = 0$ bzw. $\mathfrak{p}\mathcal{O} \subseteq I$. Daraus folgt $K \cdot I = A$, d.h. I ist auch ein Ideal von A.

A ist unverzweigt in $\mathfrak{p}$, d.h. $\mathfrak{p}\mathcal{O}$ ist ein Primideal in $\mathcal{O}$, also maximal. Demnach gilt sogar $I = \mathfrak{p}\mathcal{O}$.

$\mathcal{O}^1$ bezeichnet die Elemente mit Norm 1 in $\mathcal{O}$. Die Hauptkongruenzgruppe von $\mathcal{O}^1$ bzgl. I ist definiert als

$$\mathcal{O}^1(I) := \left\{ \alpha \in \mathcal{O}^1 \;\middle|\; \alpha - 1 \in I \right\},$$

also

$$\begin{aligned} \alpha \in \mathcal{O}^1(I) &\Leftrightarrow \alpha \in \mathcal{O}^1 \text{ und } 0 = \tilde{\varphi}(\alpha - 1) = \tilde{\varphi}(\alpha) - 1, \text{ bzw. } \tilde{\varphi}(\alpha) = 1 \\ &\Leftrightarrow \alpha \text{ ist im Kern von } \mathcal{O}^1 \to \mathrm{SL}_2\mathbb{F}_q. \end{aligned}$$

Über $\tilde{\varphi}$ bekommen wir schließlich einen Gruppenhomomorphismus $\varphi : \Delta \to \mathrm{PSL}_2(\mathbb{F}_q)$. Mit der gleichen Argumentation wie oben folgt, dass die Ordnungen von $g_i := \varphi(\gamma_i)$ mit denen der γ_i übereinstimmen. Es folgt:

Satz 2.4.4. *Sei (m_0, m_1, m_∞) ein p-„schönes“ Ordnungstripel. Dann lässt sich über die Quaternionenalgebra $A = A_0\Delta$ ein surjektiver Gruppenhomomorphismus $\varphi : \Delta \to \mathrm{PSL}_2(\mathbb{F}_q)$ definieren mit*

$$\ker\varphi = \Delta \cap \mathrm{P}\mathcal{O}^1(\mathfrak{p}\mathcal{O}).$$

2.5 Galois-Operation

Wir wollen nun betrachten, wie sich $\ker\varphi$ verändert, wenn wir von $\varphi = \varphi_{\mathfrak{p}}$ zu einer anderen Primstelle $\mathfrak{p}'$ über p wechseln und $\ker\varphi_{\mathfrak{p}'}$ betrachten.

Dazu wählen wir eine Primstelle $\mathfrak{p}$ fest und identifizieren $\mathbb{F}_q$ mit $R_E/\mathfrak{p} = R_{\widehat{E}_{\mathfrak{p}}}/\widehat{\mathfrak{p}}$. Da $\mathrm{Gal}\,(E/\mathbb{Q})$ transitiv auf den Primidealen über p operiert, gibt es $\sigma \in \mathrm{Gal}\,(E/\mathbb{Q})$ mit $\sigma : \mathfrak{p}' \mapsto \mathfrak{p}$. σ induziert einen Isomorphismus $R_E \to R_E$ und somit auch einen Isomorphismus $\mathbb{F}_q = R_E/\mathfrak{p} \cong R_E/\mathfrak{p}'$ via

$$a \bmod \mathfrak{p}' \;\mapsto\; \sigma(a) \bmod \mathfrak{p}.$$

Wir vergleichen die beiden Abbildungen $\varphi_{\mathfrak{p}}$ und $\varphi_{\mathfrak{p}'}$:

$$\begin{array}{ccccccc} & & \widehat{\mathcal{O}}_{\mathfrak{p}} & \overset{\text{konj.}}{=\!=} & \mathrm{M}_2(R_{\widehat{E}_{\mathfrak{p}}}) & \twoheadrightarrow & \mathrm{M}_2(R_{\widehat{E}_{\mathfrak{p}}}/\widehat{\mathfrak{p}}) \quad = \quad \mathrm{M}_2(\mathbb{F}_q) \;\ni g_i \\ \gamma_i \in \mathcal{O} & \nearrow & & & & & \\ & \searrow & & & & & \\ & & \widehat{\mathcal{O}}_{\mathfrak{p}'} & \overset{\text{konj.}}{=\!=} & \mathrm{M}_2(R_{\widehat{E}_{\mathfrak{p}'}}) & \twoheadrightarrow & \mathrm{M}_2(R_{\widehat{E}_{\mathfrak{p}'}}/\widehat{\mathfrak{p}'}) = \mathrm{M}_2(R_E/\mathfrak{p}') \ni g_i' \end{array}$$

Für $g_i = \varphi_{\mathfrak{p}}(\gamma_i)$ und $g_i' = \varphi_{\mathfrak{p}'}(\gamma_i)$ gilt dann

$$\mathrm{tr}\, g_i = \mathrm{tr}\,\gamma_i \bmod \mathfrak{p}$$

und

$$\mathrm{tr}\, g_i' = \mathrm{tr}\,\gamma_i \bmod \mathfrak{p}' = \sigma\mathrm{tr}\,\gamma_i \bmod \sigma(\mathfrak{p}') = \sigma\mathrm{tr}\,\gamma_i \bmod \mathfrak{p}.$$

Vertauscht man also gemäß $\sigma : \mathfrak{p}' \mapsto \mathfrak{p}$ die Primstellen $\mathfrak{p} \mid p$, so erhält man eine Operation auf den Spurtripeln in $\mathrm{SL}_2(\mathbb{F}_q)$:

$$(\mathrm{tr}\,\gamma_0, \mathrm{tr}\,\gamma_1, \mathrm{tr}\,\gamma_\infty) \bmod \mathfrak{p} \;\mapsto\; (\sigma\mathrm{tr}\,\gamma_0, \sigma\mathrm{tr}\,\gamma_1, \sigma\mathrm{tr}\,\gamma_\infty) \bmod \mathfrak{p}.$$

Für $\sigma \in \mathfrak{G}_p'$ induziert σ einen Automorphismus von $\mathbb{F}_q$, d.h. $(\mathrm{tr}\,\gamma_i)$ wird auf ein äquivalentes Tripel geschickt. Vergleicht man die Veränderung der Spurtripel hier mit der Galois-Operation auf den Multiplikatoren, so erhält man

Satz 2.5.1. *Die Voraussetzungen seien wie in Satz 1.7.2. Ist dann* $X := \ker\varphi_{\mathfrak{p}}\backslash\mathfrak{U}$*, dann ist*

$$X^{\sigma} \cong \ker\varphi_{\sigma(\mathfrak{p})}\backslash\mathfrak{U}.$$

Beweis. γ_i habe die Spur $\sqrt{\zeta_i} + \sqrt{\zeta_i}^{-1}$ und Multiplikator ζ_i. Die Multiplikatoren von $g_i = \varphi_{\mathfrak{p}}(\gamma_i)$ auf X sind dann $\zeta_i^{\pm 1}$, und auf X^σ hat g_i die Multiplikatoren $\sigma(\zeta_i) = \zeta_i^s$ und ζ_i^{-s}. Der durch γ_i induzierte Automorphismus g_i' auf X^σ hat auch Multiplikatoren $\zeta_i^{\pm 1}$, somit ist g_i' konjugiert zu g_i^r, wobei $\zeta_i^{s \cdot r} = \zeta_i$, bzw. $\sigma^{-1}(\zeta_i) = \zeta_i^r$. Für die Spuren gilt:

$$\operatorname{tr} g_i = \sqrt{\zeta_i} + \sqrt{\zeta_i}^{-1} \bmod \mathfrak{p}$$

und

$$\operatorname{tr} g_i' = \sqrt{\zeta_i}^{r} + \sqrt{\zeta_i}^{-r} \bmod \mathfrak{p} = \sigma^{-1}(\operatorname{tr} \gamma_i) \bmod \mathfrak{p}.$$

Andererseits gehört zu $\varphi_{\sigma(\mathfrak{p})}(\gamma_i)$ das Spurtripel

$$(\sigma^{-1}\operatorname{tr} \gamma_0, \sigma^{-1}\operatorname{tr} \gamma_1, \sigma^{-1}\operatorname{tr} \gamma_\infty) \bmod \mathfrak{p}.$$

Die Operation auf den Spurtripeln ist also jeweils die gleiche. □

Bemerkung.

- Da $F \leq E$ der Definitionskörper der Kurven X^σ ist, spielt eigentlich nur die Operation von σ auf Primidealen in F eine Rolle: Hat man zwei Primideale $\mathfrak{p} \neq \mathfrak{p}'$ mit $R_F \cap \mathfrak{p} = R_F \cap \mathfrak{p}'$, dann ist $\ker \varphi_{\mathfrak{p}} = \ker \varphi_{\mathfrak{p}'}$.
- Zerfallen die Kurven X_i aus 1.7.2 in mehrere Bahnen, wie in 1.7.5(iii), dann beschreiben die $\ker \varphi_{\mathfrak{p}}$ nur die Kerne in einer dieser Bahnen.

Literaturverzeichnis

[D] A. Džambić, 'Macbeaths infinite series of Hurwitz groups', in *Arithmetic and Geometry Around Hypergeometric Functions*, Progress in Mathematics **260**, R.-P. Holzapfel, A. M. Uludağ, M. Yoshida, Birkhäuser, Basel, 2007

[Di] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901

[FK] H. M. Farkas, I. Kra, *Riemann Surfaces*, Graduate Texts in Mathematics **71**, Springer-Verlag, New York, 1991

[F] H. W. Frye, *Arithmetische Charakterisierung von Normalteilern zu Dreiecksgruppen*, Dissertation, Johann Wolfgang Goethe-Universität, Frankfurt, 1985

[GW] E. Girondo, J. Wolfart, 'Conjugators of Fuchsian Groups and Quasiplatonic Surfaces', *Quart. J. Math.* **56** (2005) 525-540

[JS] G. A. Jones, D. Singerman, *Complex Functions*, Cambridge University Press, 1987

[L] U. Langer, *Erzeugende endlicher linearer Gruppen*, Dissertation, Universität Hamburg, 1977

[M69] A. M. Macbeath, 'Generators of the Linear Fractional Groups', in *Number Theory*, Proc. Sympos. Pure Math. **12**, W. J. Leveque, E. G. Straus, Amer. Math. Soc., Providence, 1969

[M73] A. M. Macbeath, 'Action of Automorphisms of a Compact Riemann Surface on the First Homology Group', *Bull. London Math. Soc.* **5** (1973) 103-108

[MR] C. Maclachlan, A. W. Reid, *The Arithmetic of Hyperbolic 3–Manifolds*, Graduate Texts in Mathmatics **219**, Springer-Verlag, New York, 2003

[N] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 2002

[R] I. Reiner, *Maximal Orders*, L.M.S. Monographs **5**, Academic Press, London, 1975

[S] C.-H. Sah 'Groups Related to Compact Riemann Surfaces', *Acta Math.* **123** (1969), 13-42

[Si] D. Singerman, 'Finitely Maximal Fuchsian Groups', *J. London Math. Soc.* (2), **6** (1972) 29-38

[SS] T. A. Schmidt, K. M. Smith, 'Galois Orbits of Principal Congruence Hecke Curves', *J. London Math. Soc.* (3) **67** (2003) 673-685

[St95] M. Streit, *Darstellungstheorie für Hypermaps und kanonisches Modell algebraischer Kurven*, Dissertation, Johann Wolfgang Goethe-Universität, Frankfurt, 1995

[St00] M. Streit, 'Field of definition and Galois orbits for the Macbeath-Hurwitz curves', *Arch. Math.* **74** (2000) 342-349

[StWo] M. Streit, J. Wolfart, 'Characters and Galois Invariants of Regular Dessins', *Revista Matemática Complutense* (2000) vol. XIII num. 1, 49-81

[Su] M. Suzuki, *Group theory II*, Grundlehren der Mathematischen Wissenschaften 247, Springer, Berlin, 1982

[V] M. F. Vignéras, *Arithmétique des Algèbre de Quaternions*, Lecture Notes in Mathematics **800**, Springer-Verlag, 1980

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1982

[Wo] J. Wolfart, 'ABC for polynomials, dessins d'enfants, and uniformization — a survey', *Elementare und Analytische Zahlentheorie*, Proceedings ELAZ-Conference, Steiner Verlag, Stuttgart, 2006

Lebenslauf

Frank Feierabend, geboren am 27.10.1975 in Bochum

1982-1986	Grundschule Kalbach, Frankfurt
1986-1995	Wöhlerschule, Frankfurt Abschluss: Abitur
1995-1996	Orthopädische Klinik Stiftung Friedrichsheim, Frankfurt Zivildienst in der Röntgenabteilung
1996-2005	Johann Wolfgang Goethe–Universität, Frankfurt Studium der Mathematik mit Nebenfach Informatik Vordiplom: 22.10.1998 Diplom: 1.3.2005 Besuch von Vorlesungen/Seminaren bei den Professoren: Baumeister, Bieri, Drobnik, Kersting, Kloeden, Schnittger, Wolfart Betreuer der Diplomarbeit: Prof. Dr. R. Bieri Titel der Diplomarbeit: S-arithmetische Gruppen in $\mathrm{SL}_2\mathbb{R}$ und kontrollierter Zusammenhang
2005-2008	Johann Wolfgang Goethe–Universität, Frankfurt Promotionsstudent der Mathematik und wissenschaftlicher Mitarbeiter bei Prof. Dr. J. Wolfart
ab 2008	Software-Entwickler bei der Firma ISD in Dortmund