Westfälische
Wilhelms-Universität Münster

Ausarbeitung des Vortrags

$PSL_2(q)$

Lena Frenken
2-Fach-Bachelor
Mathematik und Musik, Musikpraxis und neue Medien

Fachbereich Mathematik und Informatik
Mathematisches Institut
Prof. Dr. Kramer und Dr. Varghese

Inhaltsverzeichnis

1 Einleitung

In dieser Arbeit befasse ich mich mit dem Kapitel $PSL_2(q)$ aus dem Buch **Elementary Number Theory, Group Theory, and Ramanujan Graphs** [DSV10]. Dazu werden zunächst einmal die allgemeine lineare Gruppe, die spezielle lineare Gruppe und ihre Projektionen betrachtet. Im Anschluss daran werden die Eigenschaften Endlichkeit und Einfachheit betrachtet, wobei der Beweis der Einfachheit in meiner Bachelorarbeit erfolgt. Das letzte Kapitel befasst sich mit der Feststellung des amerikanischen Mathematikers Leonard Eugene Dickson, welcher vom 22.Januar 1874 bis zum 17. Januar 1954 gelebt hat und an der University of Chicago lehrte.Dieser publizierte im Jahr 1901, dass alle Untergruppen von $PSL_2(q)$ metabelsch sind, wenn q eine Primzahlpotenz ist, außer die Symmetrische Gruppe über $\mathbb{F}_4$ und die Alternierende Gruppe über $\mathbb{F}_5$[Hup79]. Diese Eigenschaft wird vor allem für die Konstruktion der Ramanujan-Graphen benötigt.

2 Einige endliche Gruppen

Definition 2.1. *Sei K ein Körper. Dann ist*
$GL_2(K) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} ; a_{ij} \in K, det(A) \neq 0 \right\}$ *und*
$SL_2(K) = \left\{ B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} ; b_{ij} \in K, det(B) = 1 \right\}$.
*Dabei nennt man $GL_n(K)$ die **allgemeine lineare Gruppe** n-ten Grades über K, welche die invertierbaren $n \times n$-Matrizen enthält. $SL_n(K)$ wird auch als **spezielle lineare Gruppe** n-ten Grades über K bezeichnet, welche die $n \times n$-Matrizen mit Determinante gleich eins enthält.*

Satz 2.2. *Sei K ein Körper und $det : GL_2(K) \to K^*$ die Abbildung einer invertierbaren 2×2-Matrix auf ihre Determinante. Dann ist $SL_2(K)$ der Kern der Abbildung.*

Beweis. Sei $B \in SL_2(K)$ beliebig. Dann gilt $det(B) = 1$. Sei nun $A \in GL_2(K) - SL_2(K)$. Dann ist $det(A) \neq 1$, also ist der Kern der Determinantenabbildung ganz $SL_2(K)$. □

Definition 2.3. *Sei K ein Körper. Die Quotientengruppe*
$PGL_2(K) = GL_2(K)/ \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} ; \lambda \in K^* \right\}$ *heißt **projektive lineare Gruppe** und*
$PSL_2(K) = SL_2(K)/ \left\{ \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix} ; \epsilon = \pm 1 \right\}$ *heißt **projektive spezielle lineare Gruppe**.*

Bemerkung 2.4. *Für das Verständnis betrachten wir zunächst einmal die **projektive Gerade**, wobei K ein Körper und $V = K^2$ ein zweidimensionaler K-Vektorraum ist.*

Die Menge der eindimensionalen Untervektorräume wird durch die projektive Gerade dargestellt, welche die Äquivalenzrelation
$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow$ *(es existiert ein* $\lambda \in K^*$*, sodass gilt*
$(x_1, y_1) = (\lambda x_2, \lambda y_2)$*)*
beinhaltet.
Das heißt, dass wir jeden Punkt der projektiven Gerade mit homogenen Koordinaten $[x : y]$ *mit* $x, y \in K$ *und* $(x, y) \neq (0, 0)$ *angeben können, wobei gilt* $[x : y] = [\lambda x : \lambda y]$ *für alle* $\lambda \in K$*.*
Die projektive Gerade P^1K *kann durch die Vereinigung der Mengen* $\{[x : 1] \in P^1(K); x \in K\}$ *und* $\{[1 : 0]\}$ *mit* $K \cup \infty$ *identifiziert werden, wobei* $[1 : 0] = \infty$*.*
Zwei Punkte werden also mit einander identifiziert, wenn sie auf einer Geraden liegen.

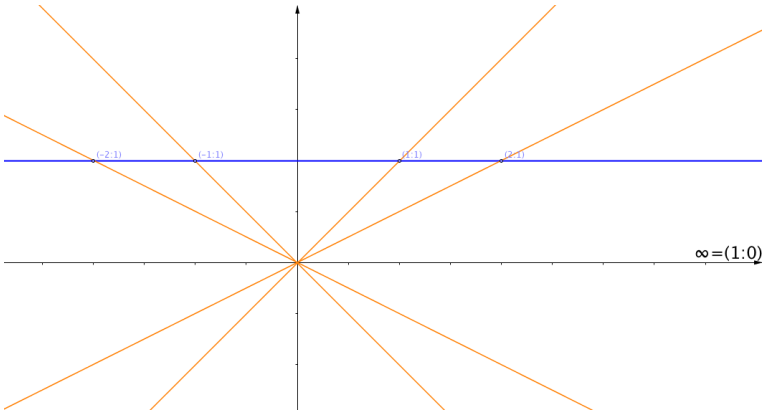

Abbildung 2.1: Die Projektive Gerade

Durch diese Projektion können wir uns $PGL_2(K)$ *und* $PSL_2(K)$ *vorstellen. Dazu benötigen wir allerdings die* ***Möbius-Transformation****:*

Definition 2.5. *Sei* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$*. Die gebrochen lineare Transformation* $\phi_A : P^1(K) \to P^1(K)$ *wird definiert durch* $\phi_A(z) = \frac{az+b}{cz+d}$*.*
Setze $\phi_A(\infty) = \begin{cases} \frac{a}{c} & \text{falls } c \neq 0 \\ \infty & \text{falls } c = 0 \end{cases}$ *und* $\phi_A(\frac{-a}{c}) = \infty$*.*

Satz 2.6. *Die Abbildung* $\phi : GL_2(K) \to Sym(P^1(K))$ *mit* $\phi(A) = \phi_A$ *ist ein Gruppenhomomorphismus. Dabei identifiziert man dann* $PGL_2(K)$ *mit* $\phi(GL_2(K))$ *und* $PSL_2(K)$ *mit* $\phi(SL_2(K))$*.*

Beweis. Seien $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ und $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in GL_2(K)$. Dann erhält man folgende Termumformungen:

$$
\begin{aligned}
\phi_{AB}(z) &= \phi(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix})(z) \\
&= \phi(\begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + c_2d_1 & c_1b_2 + d_1d_2 \end{pmatrix})(z) \\
&= \frac{(a_1a_2 + b_1c_2)z + a_1b_2 + b_1d_2}{(a_2c_1 + c_2d_1)z + c_1b_2 + d_1d_2} \\
&= \frac{a_1a_2z + a_1b_2 + b_1c_1z + b_1a_2}{a_2c_1z + b_2c_1 + c_2d_1z + d_1d_2} \\
&= \frac{\frac{a_1a_2z + a_1b_2}{c_2z + d_2} + b_1}{\frac{a_2c_1z + c_1b_2}{c_2z + d_2} + d_1} \\
&= \frac{a_1(\frac{a_2z + b_2}{c_2z + d_2}) + b_1}{c_1(\frac{a_2z + b_2}{c_2z + d_2}) + d_1} \\
&= \phi_A(z) \circ \phi_B(z).
\end{aligned}
$$

Der zweite Teil folgt aus den Überlegungen zur projektiven Gerade. □

Konvention: Für $K = \mathbb{F}_q$ schreibe $GL_2(q), SL_2(q), PGL_2(q)$ und $PSL_2(q)$.

Proposition 2.7. *Es gelten*

1. $|GL_2(q)| = q \cdot (q-1) \cdot (q^2-1)$
2. $|SL_2(q)| = |PGL_2(q)| = q \cdot (q^2-1)$
3. $|PSL_2(q)| = \begin{cases} q \cdot (q^2-1) & \textit{falls } q \textit{ gerade} \\ \frac{q \cdot (q^2-1)}{2} & \textit{falls } q \textit{ ungerade} \end{cases}$.

Beweis. Man erhält drei kleine Beweise:

Zu (1) Eine 2×2-Matrix in $GL_2(q)$ wird zunächst durch die Wahl eines Vektors in der ersten Spalte, welcher ungleich 0 ist, bestimmt. Also gibt es im Körper $\mathbb{F}_q^2$ dafür $q^2 - 1$ Möglichkeiten. Für die zweite Spalte gilt dann, dass ein Vektor gewählt werden muss, der in $\mathbb{F}_q^2$ linear unabhängig vom ersten ist, da ansonsten die Determinante der Matrix gleich null wäre. Also kommen der erste Vektor und seine Vielfachen nicht in Frage. Somit ergeben sich noch $q^2 - q = q(q-1)$ Möglichkeiten.

Zu (2) Mit dem Homomorphiesatz folgt, dass $GL_2(q)/\ SL_2(q)$ isomorph zu $\mathbb{F}_q^*$ ist.

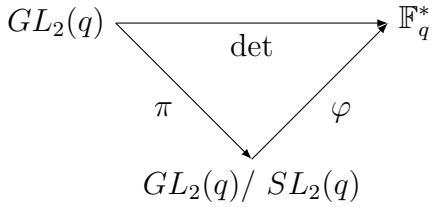

Abbildung 2.2: Homomorphiesatz

Es folgt, dass

$$|GL_2(q)/\ SL_2(q)| = |\mathbb{F}_q^*| = q - 1$$

gilt. Durch Umformen erhält man

$$|GL_2(q)|/\ |SL_2(q)| = q - 1$$

und weiter mit (1)

$$|SL_2(q)| = \frac{q(q-1)(q^2-1)}{q-1} = q(q^2-1).$$

Weiterhin gilt

$$\begin{aligned}
|PGL_2(q)| &= |GL_2(q)/\ \{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}; \lambda \in \mathbb{F}_q^*\}| \\
&= |GL_2(q)|/\ |\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}; \lambda \in \mathbb{F}_q^*\}| \\
&= \frac{q(q-1)(q^2-1)}{q-1} \\
&= q(q^2-1) \\
&= |SL_2(q)|.
\end{aligned}$$

Zu (3) Ähnlich wie im Beweis zu Teil (2) erhält man folgende Umformungen:

$$\begin{aligned}
|PSL_2(q)| &= |SL_2(q)/\ \{\begin{pmatrix}\epsilon & 0\\ 0 & \epsilon\end{pmatrix}; \epsilon = \pm 1\}| \\
&= |SL_2(q)|/\ |\{\begin{pmatrix}\epsilon & 0\\ 0 & \epsilon\end{pmatrix}; \epsilon = \pm 1\}| \\
&= q(q^2-1)/\ |\{\begin{pmatrix}\epsilon & 0\\ 0 & \epsilon\end{pmatrix}; \epsilon = \pm 1\}| = \begin{cases} q(q^2-1) & \text{falls } q \text{ gerade} \\ \frac{q(q^2-1)}{2} & \text{falls } q \text{ ungerade.} \end{cases}
\end{aligned}$$

□

3 Endlichkeit und Einfachheit

Dieses Kapitel wird in der Bachelorarbeit vor allem durch den Beweis der Einfachheit von $PSL_2(q)$ näher beleuchtet.

Lemma 3.1. *Sei K ein Körper. Die Gruppe $SL_2(K)$ wird durch die Vereinigung der zwei Untergruppen $\left\{\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}; \lambda \in K\right\}$ und $\left\{\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix}; \mu \in K\right\}$ erzeugt.*
Jede Matrix aus $SL_2(K)$ ist also durch ein endliches Produkt aus oberen und unteren Dreiecksmatrizen mit Einsen auf den Diagonalen darstellbar. Wenn K endlich ist, dann gilt dies also ebenfalls für $SL_2(q)$ und demnach auch für $PSL_2(q)$.

Beweis. Sei $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(q)$. Betrachte folgende Fallunterscheidung:

1. Sei $c \neq 0$. Dann erhält man diese Gleichungskette:

$$\begin{pmatrix}1 & \frac{a-1}{c}\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}\begin{pmatrix}1 & \frac{d-1}{c}\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \frac{a-1}{c}\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & \frac{d-1}{c}\\ c & d\end{pmatrix}$$
$$= \begin{pmatrix}a & \frac{d-1}{c} + d\frac{a-1}{c}\\ c & d\end{pmatrix},$$

   wobei $\frac{d-1}{c} + \frac{d(a-1)}{c} = \frac{d-1+da-d}{c} = \frac{ad-(ad-bc)}{c} = b$.

2. Sei nun also $c = 0$. Dann folgt direkt, dass $d \neq 0$, da ansonsten die Determinante gleich null wäre. Somit gilt für die Matrix $\begin{pmatrix}a+b & b\\ d & d\end{pmatrix} \in SL_2(K)$ mit (1) das Lemma und es folgt aus

$$\begin{pmatrix}a+b & b\\ d & d\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix} = \begin{pmatrix}a & b\\ 0 & d\end{pmatrix}$$

   die Behauptung.

□

Definition 3.2. *Eine Gruppe G heißt einfach, wenn die einzigen normalen Untergruppen $\{1\}$ und G selbst sind. Äquivalent zu dieser Defioniton ist, dass jeder Gruppenhomomorphismus $\Pi : G \to H$ konstant oder injektiv ist.*

Theorem 3.3. *Sei K ein Körper mit $|K| = q \geq 4$. Dann ist $PSL_2(q)$ einfach.*

Beweis. Der Beweis erfolgt in meiner Bachelorarbeit. □

4 Einschub: Allgemeine Aussagen der Gruppentheorie

Konvention: Für eine Permutation σ auf einer Menge X und für ein $x \in X$ ist der Orbit von x unter σ

$$\Omega_x = \{\sigma^k(x); k \in \mathbb{Z}\}.$$

Lemma 4.1. *Sei σ eine Permutation einer Menge X. Wenn die Ordnung p von σ prim ist, dann hat jeder Orbit von σ auf X entweder 1 oder p Elemente.*

Beweis. Sei $H \subseteq Sym(X)$ eine Untergruppe erzeugt durch σ. Für $x \in X$ gilt $|\Omega_x| = \frac{|H|}{|H_x|}$, wobei $H_x = \{\alpha \in H; \alpha(x) = x\}$ der Stabilisator von x in H ist. Aus der Voraussetzung, dass die Ordnung von H gleich p ist, folgt entweder, dass die Ordnung vom Stabilisator gleich eins und die Ordnung vom Orbit gleich p ist oder umgekehrt, da p prim ist. □

Bemerkung 4.2. *Wenn die Ordnung des Orbits gleich eins ist, dann ist x ein Fixpunkt von σ.*

Theorem 4.3 (Cauchys Theorem über die Existenz von Elementen mit Primzahlordnung in endlichen Gruppen)**.** *Sei G eine endliche Gruppe und p eine Primzahl. Wenn p die Ordnung von G teilt, dann enthält G ein Element mit Ordnung p.*

Beweis. Betrachte zunächst das Produkt $G^p = G \times G \times \cdots \times G$ und die zyklische Permutation σ mit $\sigma(g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$ für alle g_i in G mit $i = 1, \ldots, p$.
Dann ist σ eine Permutation von G^p mit Ordnung p.
Sei nun $H \subseteq G^p$ definiert durch $H = \{(g_1, \ldots, g_p); g_1 \cdot g_2 \ldots g_p = 1\}$. H hat die Ordnung $|G|^{p-1}$, da wir die ersten $p-1$ Koordinaten frei wählen können und g_p dann als Inverses vom Produkt $g_1 \ldots g_{p-1}$ bestimmen, damit die Gleichung erfüllt ist. Es gilt

$$g_p = (g_1 \ldots g_{p-1})^{-1} \in G,$$

da G eine Gruppe ist. Außerdem gilt

$$\begin{aligned} & g_1 \cdot g_2 \ldots g_p = 1 \\ \Leftrightarrow\ & 1 \cdot g_2 \ldots g_p = g_1^{-1} \\ \Leftrightarrow\ & g_2 \ldots g_p g_1 = 1 \end{aligned}$$

Durch Konjugation mit g_1^{-1} folgt also, dass H invariant unter σ ist. Betrachte nun σ als Permutation von H.
Da die Orbiten von σ H unterteilen und die Ordnung von H eine p-Potenz ist, folgt mit der Bahnengleichung, dass die Summe der Ordnungen der Orbiten gleich 0 modulo p ist [vgl. Bos13, S. 241].

Mit Lemma 1 folgt nun, dass die Orbiten entweder Fixpunkte sind oder p Elemente haben. Da σ mindestens einen Fixpunkt, nämlich das p-Tupel $(1, 1, \ldots, 1)$ hat, muss es mindestens $p-1$ weitere Fixpunkte geben. Dieser Fixpunkt hat die Form $(a, a, \ldots, a)$ wobei $a \neq 1$ gilt. Da dieses Tupel ein Element aus H ist, gilt $a^p = 1$, also hat a die Ordnung p in G. Damit folgt die Behauptung. □

Lemma 4.4. *Sei q eine Primzahl. Für eine Matrix $A \in SL_2(q)$ sind äuqivalent*

1. *ϕ_A hat die Ordnung q.*
2. *Es existiert eine bestimmte eindimensionale Teilmenge D in $\mathbb{F}_q^2$, sodass D entweder unter A oder $-A$ punktweise fixiert wird.*
3. *ϕ_A ist in $PGL_2(q)$ zu einem ϕ_{Cb} mit $b \in \mathbb{F}_q^\times$ konjugiert.*

Beweis. Der Beweis erfolgt per Ringschluss.

$(i) \Rightarrow (ii)$ Sei A eine Matrix in $SL_2(q)$ und ϕ_A die gebrochenrationale lineare Transformation auf die projektive Gerade. ϕ_A habe Ordnung q. Da die Ordnung der projektiven Gerade über den Körper $\mathbb{F}_q$ gleich der Ordnung der Vereinugung von der Menge $\{[x : 1]; x \in \mathbb{F}_q\}$ und ∞ ist, hat die projektive Gerade also Ordnung $q + 1$. Es gilt also

$$\begin{aligned} |P^1(\mathbb{F}_q)| &= |\,\{[x : 1]; x \in \mathbb{F}_q\} \cup \infty| \\ &= |\,\{[x : 1]; x \in \mathbb{F}_q\}\,| + |\infty| \\ &= q + 1. \end{aligned}$$

Somit folgt aus Bemerkung 4.2, dass ϕ_A einen Fixpunkt auf $P^1(\mathbb{F}_q)$ hat. Dieser Fixpunkt ist also eine eindimensionale Teilmenge von $\mathbb{F}_q^2$, die invariant unter A ist. Wenn ϕ_A die Ordnung q hat, kann A entweder Ordnung q oder $2q$ in $SL_2(q)$ haben. Betrachten wir also beide Fälle:

(a) A hat die Ordnung q. Da A auf D mit mindestens einem Fixpunkt wirkt, nämlich $(0, 0)$ und mit dem Satz von Lagrange folgt, dass D ORdnung q hat, folgt mit Lemma 4.1, dass A D punktweise fixiert.

(b) A hat Ordnung $2q$. Dann gilt das obige Argument für A^2, also fixiert A^2 D punktweise. Daraus folgt, dass A auf D durch die Zuordnungsvorschrift $x \mapsto -x$ wirkt, sodass $-A$ D punktweise fixiert.

$(ii) \Rightarrow (iii)$ Wähle die Basis e_1, e_2 von $\mathbb{F}_q^2$, wobei $e_1 \in D$ gelte. Die Matrix A hat unter der gewählten Basis die Form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ mit $a = d = \pm 1$ und $b \neq 0$. Das bedeutet, dass die Transformation ϕ_a in $PGL_2(q)$ zu ϕ_{C_b} konjugiert ist.

$(iii) \Rightarrow (i)$ ϕ_{C_b} hat Ordnung q, da auf der Diagonalen Einsen stehen und das Element $b \in \mathbb{F}_q^*$ die Ordnung q hat. Da ϕ_A zu ϕ_{C_b} konjugiert ist, gilt

$$\begin{aligned} |\phi_a| &= |\phi_{C_b}| \\ &= q. \end{aligned}$$

Somit folgt die Behauptung.

□

Korrolar 4.5. *Aus Lemma 4 lässt sich folgende Eigenschaft herleiten: Seien A und B in $SL_2(q)$, sodass ϕ_A und ϕ_B die Ordnung q haben. Wenn A und B die gleiche Gerade D in $\mathbb{F}_q^2$ fixieren, dann erzeugen ϕ_A und ϕ_B die gleiche Untergruppe mit Ordnung q.*

5 Struktur der Untergruppen von $PSL_2(q)$

Definition 5.1. *Sei G eine Gruppe. Dann heißt G* ***metabelsch****, wenn G eine normale Untergruppe $N \trianglelefteq G$ besitzt, sodas N und G/N abelsch sind.*

Beispiel 5.2.

- *Alle abelschen Gruppen sind metabelsch.*
- *Die* ***Heisenberggruppe*** $H_3(K) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} ; x, y, z \in K \right\}$ *ist metabelsch.*

  Beweis. Betrachte zunächst den Kommutator von $H_3(K)$.

$$\begin{aligned} &\left[\begin{pmatrix} 1 & x_1 & z_1 \\ 0 & 1 & y_1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & x_2 & z_2 \\ 0 & 1 & y_2 \\ 0 & 0 & 1 \end{pmatrix} \right] \\ &= \begin{pmatrix} 1 & x_1 & z_1 \\ 0 & 1 & y_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 & z_2 \\ 0 & 1 & y_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_1 & z_1 \\ 0 & 1 & y_1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x_2 & z_2 \\ 0 & 1 & y_2 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & x_2 + x_1 & z_2 + x_1 z_2 + z_1 z_2 \\ 0 & 1 & y_2 + y_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x_1 & -z_1 + x_1 y_1 \\ 0 & 1 & -y_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x_2 & -z_2 + x_2 y_2 \\ 0 & 1 & -y_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & x_2 + x_1 & z_2 + x_1 z_2 + z_1 z_2 \\ 0 & 1 & y_2 + y_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x_2 - x_1 & -z_2 + x_2 y_2 + x_1 y_2 - z_1 + x_1 y_1 \\ 0 & 1 & -y_2 - y_1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

wobei

$$\begin{aligned} a &= -z_2 + x_2y_2 + x_1y_2 - z_1 + x_1y_1 - x_2y_2 - x_2y_1 - x_1y_2 - x_1y_1 + z_2 + x_1z_2 + z_1z_2 \\ &= -z_1 - x_2y_1 + x_1z_2 + z_1z_2 \in K. \end{aligned}$$

Also ist $N := [H_3(K), H_3(K)] = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ; a \in K \right\}$ die Kommutatorengruppe von $H_3(K)$. Diese ist immer Normalteiler und weiterhin gilt, dass $H_3(K)/\ N$ abelsch ist [vgl. Bos13, S. 255]. Es bleibt also zu prüfen, dass N abelsch ist. Betrachte dazu die Kommutatorengruppe von N.
Seien a und b aus K. Dann erhält man:

$$\begin{aligned} [N, N] &= \left[\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \\ &= \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 0 & b+a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & b+a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -b-a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Daraus, folgt, dass N abelsch ist. Somit haben wir eine normale Untergruppe N gefunden, für die gilt, dass N und $G/\ N$ abelsch sind. Also ist die Heisenberggruppe metabelsch.

□

Lemma 5.3. *Sei G eine Gruppe. G ist metabelsch genau dann, wenn $[[g_1, g_2], [g_3, g_4]] = 1$ für alle g_i in G, wobei $i = 1, \ldots 4$.*

Beweis. $\Rightarrow$ Sei $N := [g_1, g_2] = [g_3, g_4]$ die Kommutatorgruppe von G. Dann folgt aus $[N, N] = 1$ schon, dass N abelsch ist. Außerdem gilt für die Kommutatorgruppe, dass sie der kleinste Normalteiler ist, sodass $G/\ N$ abelsch ist. Damit ist G metabelsch.

$\Leftarrow$ Sei G metabelsch. Dann existiert ein $H \trianglelefteq G$, sodass H und $G/\ H$ abelsch sind. Aus H abelsch folgt, dass der Kommutator, also $[H, H] = 1$. Weiterhin ist $N = [g_1, g_2]$ der kleinste Normalteiler,

sodass $G/\ N$ abelsch ist. Damit folgt, dass N eine Teilmenge von H sein muss. Da gilt

$$\begin{aligned} 1 &= [[g_1, g_2], [g_3, g_4]] \\ &= [N, N] \\ &\subseteq [H, H] \\ &= 1 \end{aligned}$$

folgt, dass $N = H$ ist. Damit folgt die Behauptung.

□

Lemma 5.4. *Sei G eine Gruppe. Wenn G eine abelsche Untergruppe H mit Index 2 hat, dann ist G metabelsch.*

Beweis. Sei G eine Gruppe und $H \subseteq G$ eine abelsche Gruppe mit $(G : H) = 2$. Dann gibt es neben H noch genau eine weitere Nebenklasse aH, wboei $a \notin H$. Da die Nebenklassen eine Zerlegung von G bilden, jedoch $Ha \neq H$ gilt, da a nicht in H und H eine Gruppe, muss $aH = Ha$ gelten. Somit ist H Normalteiler. Außerdem ist H abelsch.
Insgesamt folgt also, dass auch $G/\ H$ abelsch ist und somit G metabelsch ist. □

Bemerkung 5.5. *Metabelsche Gruppen sind auflösbar. Außerdem sind Untergruppen metabelscher Gruppen wieder metabelsch.*

Im Jahr 1901 hat Dickson eine Liste mit allen Untergruppen von $PSL_2(q)$ bis auf Isomorphie erstellt.
Dabei fiel ihm auf, dass alle Untergruppen von $PSL_2(q)$ metabelsch sind, wenn q eine Primzahlpotenz ist, außer

- $Sym(4)$ mit Ordnung 24, die nur auflösbar ist
- $Alt(5)$ mit Ordnung 60, die nicht abelsch ist.

Dies soll im Folgenden bewiesen werden.

Proposition 5.6. *Sei q eine Primzahl und H eine echte Untergruppe von $PSL_2(q)$. Wenn q die Ordnung von H teilt, dann ist H metabelsch.*

Beweis. Sei H eine Untergruppe von $PSL_2(q)$ und q teilt die Ordnung von H. Daraus folgt mit Theorem 3 aus Paragraph 3, dass H ein Element der Ordnung q enthält.

Behauptung: H enthält eine einzige Untergruppe der Ordnung q.

Beweis. Wir nehmen an, dass C_1 und C_2 disjunkte Untergruppen der Ordnung q in H sind. Dann folgt, dass die beiden projezierten Geraden D_1 und D_2 in $\mathbb{F}_q^2$ ebenfalls disjunkt sind. Man erhält also bezüglich der Basis $\{e_1, e_2\}$ die Abbildnungen $C_1 = \phi \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} ; \lambda \in \mathbb{F}_q \right\}$ und

$C_2 = \phi\left\{\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix}; \mu \in \mathbb{F}_q\right\}$.
Mit Lemma 1 aus Paragraph 2 folgt nun direkt, dass C_1 und C_2 ganz $PSL_2(q)$ erzeugen. Dies ist ein Widerspruch dazu, dass H eine geegnete Untergruppe von $PSL_2(q)$ ist. □

Sei also C die einzige Untergruppe mit Ordnung q in H. Dann ist $C \trianglelefteq H$ normal, denn gCg^{-1} ist eine Untergruppe und gleichmächtig zu C, also muss C schon gleich gCg^{-1} sein.
Durch eventuelle Konjugation können wir annehmen, dass
$C = \phi\left\{\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}; \lambda \in \mathbb{F}_q\right\}$. Also ist die Wirkung von C auf der projektiven Gerade $P^1(\mathbb{F}_q)$ Translation.
Da der einzige Fixpunkt von C in $P^1(\mathbb{F}_q)$ unendlich ist und $C \trianglelefteq H$ normal ist, gilt für jedes $\phi_A \in C$ und $\phi_B \in H$:

$$\begin{aligned}\phi_A(\phi_B(\infty)) &= \phi_B(\phi_{B^{-1}AB}(\infty))\\ &= \phi_B(\infty).\end{aligned}$$

Also ist $\phi_B(\infty)$ Fixpunkt unter C. Da außerdem gilt, dass

$$\phi_B(\infty) = \infty$$

für alle $\phi_B \in H$, ist H im Stabilisator von ∞ in $PSL_2(q)$ enthalten. Und dies ist nichts anderes als die folgende Untergruppe, welche auch Borelgruppe genannt wird:

$$B_0 := \phi\left\{\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix}; a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\right\}.$$

Es folgt damit:

$$\begin{aligned}H &\subseteq Stab(\infty)\\ &= B_0\\ &= \phi\left\{\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix}; a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\right\}\\ &\subseteq PSL_2(q).\end{aligned}$$

Durch Berechnung des Kommutators $[[B_0, B_0], [B_0, B_0]] = 1$ folgt mit Lemma 5.3, dass B_0 metabelsch ist. Berechne zunächst den Kommutator von $[B_0, B_0]$. Seien dazu $\begin{pmatrix}a_1 & b_1\\ 0 & a_1^{-1}\end{pmatrix}$ und $\begin{pmatrix}a_2 & b_2\\ 0 & a_2^{-1}\end{pmatrix}$ beliebige Elemente

aus B_0. Man erhält dann:

$$\begin{aligned}\left[\begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & a_2^{-1} \end{pmatrix}\right] &= \begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2^{-1} \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1^{-1} \end{pmatrix}^{-1} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2^{-1} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2^{-1} \\ 0 & a_1^{-1}a_2^{-1} \end{pmatrix} \begin{pmatrix} a_1^{-1} & -b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2^{-1} & -b_2 \\ 0 & a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2^{-1} \\ 0 & a_1^{-1}a_2^{-1} \end{pmatrix} \begin{pmatrix} a_1^{-1}a_2^{-1} & -a_1^{-1}b_2 - b_1a_2 \\ 0 & a_1a_2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -a_2b_2 - a_2^2a_1b_1 \\ 0 & 1 \end{pmatrix}\end{aligned}$$

Die Einträge innerhalb der Matrix sind kommutativ, da sie aus dem Körper $\mathbb{F}_q$ kommen. Der Übersicht halber, definiere nun

$$c := -a_2b_2 - a_2^2a_1b_1 \in \mathbb{F}_q$$

und berechne nun den Kommutator der zuvor erhaltenen Kommutatorgruppe:

$$\begin{aligned}\left[\begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c_2 \\ 0 & 1 \end{pmatrix}\right] &= \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & c_2 \\ 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & c_1 + c_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -c_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -c_2 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & c_1 + c_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -c_2 - c_1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -c_2 - c_1 + c_2 + c_1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

Also ist B_0 metabelsch. Da H eine Teilmenge von B_0 ist, ist also auch H metablesch. □

Proposition 5.7. *Sei q eine Primzahl und H eine Untergruppe von $PSL_2(q)$. Wenn die Ordnung von H größer 60 ist und q die Ordnung von H nicht teilt, dann hat H eine abelsche Untergruppe mit Index 2. H ist dann metabelsch.*

Aus der Proposition 7 in Paragraph 1 folgt, dass H eine echte Untergruppe von $PSL_2(q)$ ist, wenn q die Ordnung von H nicht teilt.

Theorem 5.8. *Sei q eine Primzahl und H eine echte Untergruppe von $PSL_2(q)$ mit $|H| > 60$. Dann ist H metabelsch.*

Beweis. Das Theorem folgt direkt aus den beiden Propositionen sechs und sieben. □

Literatur

[Bos13] Siegfried Bosch. *Algebra.* Springer Spektrum, Berlin Heidelberg, 2013.

[DSV10] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary Number Theory, Group Theory, and Ramanujan Graphs.* Cambridge University Press, London, 2010.

[Hup79] Bertram Huppert. *Endliche Gruppen I.* Number 134. Springer-Verlag, 1979.