Über die Anzahl der Bahnen in endlichen Gruppen unter der Operation ihrer Automorphismengruppe - Suzuki-Gruppen vs. lineare Gruppen

Stefan Kohl

Diplomarbeit im Fach
Mathematik
an der
Universität Stuttgart

Betreuer : Priv.-Doz. Dr. Markus Stroppel

Januar 2000

Mein Dank gilt Herrn PD Dr. Markus Stroppel für die vorzügliche Betreuung dieser Arbeit während des gesamten Bearbeitungszeitraums, sowie den Entwicklern des Computeralgebrasystems GAP (siehe [GAP99]), welches sich hier ein weiteres Mal als sehr nützlich erwiesen hat; dies betrifft nicht nur die Berechnung der Tabellen in Anhang A, sondern auch das Finden der Resultate und der zugehörigen Beweise selbst, zumal es mitunter eine nicht zu unterschätzende Hilfe war, die Struktur der behandelten Gruppen anhand von Beispielen rechnerisch untersuchen zu können.

Inhaltsverzeichnis

Vorwort

Die vorliegende Arbeit beschäftigt sich mit der Anzahl $\omega(G)$ der Bahnen, in die eine (endliche) Gruppe G unter der Operation ihrer Automorphismengruppe zerfällt.

In diesem Zusammenhang interessiert unter anderem die Fragestellung, was sich über G aussagen läßt, wenn man Eigenschaften von $\omega(G)$ vorgibt, es also zum Beispiel nach oben hin beschränkt. So folgt etwa aus $\omega(G) \leq 2$, daß G isomorph zur additiven Gruppe eines Vektorraums ist. Die entsprechende Fragestellung für $\omega(G) \leq 3$ wurde von Helmut Mäurer und Markus Stroppel in [MS97] -auch für unendliche Gruppen- untersucht und teilweise geklärt. Es ist hier natürlich naheliegend, allgemeiner zu fragen, was sich aus $\omega(G) \leq n$ folgern läßt, aber für $n > 3$ wird die Situation recht schnell sehr unübersichtlich und man wird wohl keine 'schönen' Ergebnisse mehr erwarten können. Eine Möglichkeit, dennoch zu Resultaten zu kommen, ist, daß man zusätzliche Forderungen an G stellt, also beispielsweise verlangt, daß G einfach ist (diese Frage wurde von Markus Stroppel in [Str99] für $n = 5$ beantwortet).

Möchte man bei der Behandlung der genannten Problemstellungen weiterkommen, wird es sicherlich von Nutzen sein, für gewisse 'interessante' Typen von Gruppen G den Wert von $\omega(G)$ zu bestimmen. Hierzu einen Beitrag zu leisten ist die Zielsetzung dieser Arbeit.

Zunächst geht es dabei um die linearen Gruppen vom Grad 2, genauer um $G = \mathrm{PSL}(2,q)$, $\mathrm{SL}(2,q)$, $\mathrm{PGL}(2,q)$ oder $\mathrm{GL}(2,p)$, wo geschlossene Formelausdrücke zur Berechnung von $\omega(G)$ hergeleitet werden, sowie um den 'Einzelfall' $G = \mathrm{PSL}(3,3)$, der von Interesse ist, um (zusammen mit den Suzuki-Gruppen, s.u.) alle minimalen einfachen Gruppen zu erfassen (vgl. Satz 1.9). Eine wesentliche Hilfe hierbei ist die explizite Kenntnis der Automorphismengruppen in diesen Fällen. Die Vorgehensweise ist im großen und ganzen die, daß man sich zunächst durch Übergang von beliebigen Elementen von G zu deren rationaler Normalform ein Repräsentantensystem für die Konjugiertenklassen von G verschafft und anschließend untersucht, welche dieser Repräsentanten sich durch äußere Automorphismen von G ineinander überführen lassen, also welche Konjugiertenklassen von G unter der Operation von $\mathrm{Out}(G)$ fusionieren. Die Komplexität des anschließenden Zählvorganges und der resultierenden -z.T. rekursiven- Formelausdrücke bereits für die linearen Gruppen vom Grad 2 läßt es wohl wenig plausibel erscheinen, daß sich für höhere Grade noch einigermaßen übersichtliche Ergebnisse erzielen lassen - selbst der Fall $G = \mathrm{GL}(2,q)$ für eine beliebige Primzahlpotenz q ist schon so unübersichtlich, daß ich hier keine allgemeine Formel mehr gefunden habe (eine GAP-Routine zum Abzählen der Bahnen in diesem Fall findet sich, nebst Funktionen zur Auswertung der oben erwähnten Formelausdrücke für die übrigen betrachteten Gruppen, in Anhang B).

Anschließend werden die Suzuki-Gruppen $\mathrm{Sz}(q)$ untersucht. Obwohl sich diese Gruppen erheblich von den zuvor betrachteten linearen Gruppen unterscheiden, ergeben sich doch - zunächst einmal überraschende - Parallelen zu den Gruppen $\mathrm{PSL}(2,q)$, die sich auch im Ergebnis niederschlagen :

$$\omega(\mathrm{Sz}(q)) = \omega(\mathrm{PSL}(2,q)) + 2$$

Diesen Umstand kann man auch auffassen als eine Ähnlichkeit der einfachen Zassenhaus-Gruppen untereinander. (Zassenhaus-Gruppen sind zweifach transitive Permutationsgruppen endlicher Mengen, deren einziges Element, das mehr als zwei Punkte fixiert, das Neutralelement ist, und die keinen regulären Normalteiler haben. Einfache Zassenhaus-Gruppen sind $\mathrm{PSL}(2,q)$ für $q > 3$ und die Suzuki-Gruppen. Eine ausführliche Diskussion dieser Gruppen findet sich in [HB82], Kap. XI; hier sei nur noch erwähnt, daß die einfachen Zassenhaus-Gruppen die einzigen einfachen Gruppen mit einer nichttrivialen Partition, also einer Zerlegung in paarweise bis auf das Neutralelement disjunkte echte Untergruppen, sind (siehe [Hup67], S. 194, Bem. 8.6)). Die genannte Ähnlichkeit der Strukturen dieser Gruppen im Hinblick auf die Thematik dieser Arbeit manifestiert sich etwa darin, daß in beiden Fällen die äußere Automorphismengruppe halbregulär auf der Menge der Konjugiertenklassen operiert, die kein Element einer Untergruppe $\mathrm{PSL}(2,\tilde{q}) \lneq \mathrm{PSL}(2,q)$ bzw. $\mathrm{Sz}(\tilde{q}) \lneq \mathrm{Sz}(q)$ über einem echten Teilkörper $\mathrm{GF}(\tilde{q})$ von $\mathrm{GF}(q)$ enthalten, und daß das Ergebnis dann für beide Serien von Gruppen in praktisch derselben Art und Weise per geschickter 'Summation über den Teilkörperverband' des Grundkörpers gewonnen werden kann. Was die erwähnte Halbregularitätsaussage anbelangt, so ergibt sich diese einerseits für die speziellen linearen Gruppen ganz nebenbei und ohne jede Schwierigkeit, erfordert jedoch andererseits bei den Suzuki-Gruppen einen Großteil des Beweises des diesbezüglichen Satzes. Betreffs des Summanden '2' im oben genannten Hauptresultat beachte man, daß sich dieser letztlich aus der Gültigkeit der Gleichung für $q = 2$ ergibt, wenn man die Definition der Suzuki-Gruppen auf $\mathrm{Sz}(2) \cong \langle (2\ 4\ 3\ 5), (1\ 2)(3\ 4) \rangle \cong \mathrm{AGL}(1,5) \cong \mathrm{C}_5 \rtimes \mathrm{C}_4$ ausdehnt, zumal sich die Bahnenzerlegungen der Mengen der zu keinem Element dieser Untergruppen konjugierten Gruppenelemente von $\mathrm{Sz}(q)$ und $\mathrm{PSL}(2,q)$ in zählungsrelevanter Hinsicht völlig gleichen. Der Wunsch, neben den minimalen einfachen Gruppen auch die einfachen Zassenhaus-Gruppen im Sinne der Zielsetzung dieser Arbeit abschließend zu behandeln, kann als wesentliche Motivation dafür angesehen werden, sich nicht auf lineare Gruppen über Primkörpern und Suzuki-Gruppen $\mathrm{Sz}(2^p)$ für ungerade Primzahlen p zu beschränken, sondern die genannten Gruppen über sämtlichen zulässigen (endlichen) Grundkörpern zu betrachten, obwohl dies die Argumentation nicht unerheblich verkompliziert.

Die Frage nach einem Resümee dieser Arbeit läßt sich wohl dahingehend beantworten, daß die linearen Gruppen, so weit wie interessante, einem Leser vom Umfang her zuträgliche Ergebnisse zu erwarten sind, und die Suzuki-Gruppen vollständig in der bekannten Weise behandelt werden, und daß ferner quasi *en passant* eine weitere Ähnlichkeit der Suzuki-Gruppen zu linearen Gruppen aufgedeckt wird. Weitere Untersuchungen könnten in die Richtung gehen, sich zu überlegen, ob bzw. inwieweit sich die Resultate für die minimalen einfachen Gruppen in dem Sinne auf die übrigen einfachen Gruppen übertragen lassen, als daß sich die Bahnenanzahl durch Übergang zu einer größeren einfachen Gruppe zumindest nicht verringert - für allgemeine Gruppen ist dies nicht der Fall, wie das Beispiel $\omega(\mathrm{C}_2 \times \mathrm{C}_4) = 4$ und $\omega(\mathrm{C}_4^2) = 3$ zeigt.

Kapitel 1

Grundlagen

Dieses Kapitel dient der Darlegung der in dieser Arbeit verwendeten mathematischen Grundlagen. Die Ausführungen können und sollen selbstverständlich kein Lehrbuch ersetzen. Auf Beweise wird weitgehend verzichtet und stattdessen auf die gängige Literatur verwiesen - für 'Standardwissen' sind dies bevorzugt Lehrbücher, ansonsten Originalliteratur; wo immer es in den referenzierten Quellen mehr oder weniger direkte Entsprechungen zu den genannten Sätzen gibt, wird darauf hingewiesen. Auf die meisten der hier aufgeführten Aussagen wird später Bezug genommen; wo immer es angebracht erscheint, werden jedoch zur besseren Illustration auch weitere Zusatzinformationen gegeben - dies ist beispielsweise der Fall bei den linearen Gruppen (siehe Lemma 1.5) sowie den Suzuki-Gruppen (siehe Lemma 1.8). Vorausgesetzt wird lediglich eine gewisse Vertrautheit mit den Grundzügen der Gruppentheorie, der linearen Algebra, der Kombinatorik sowie der elementaren Zahlentheorie. Betreffs der Erläuterung der verwendeten Schreibweisen sei der Leser auf das Symbolverzeichnis in Anhang C verwiesen.

1.1 Lemma *Es sei M eine nichtleere endliche Menge. Dann gilt :*

$$\sum_{\varnothing \neq \tilde{M} \subseteq M} (-1)^{|\tilde{M}|+1} \;=\; 1 + \sum_{\tilde{M} \subseteq M} (-1)^{|\tilde{M}|} \;=\; 1 + 0 \;=\; 1$$

Beweis : Diese Aussage ist eine direkte Konsequenz daraus, daß M genauso viele Teilmengen gerader wie ungerader Kardinalität besitzt. Das wiederum zeigt man via Induktion über die Kardinalität von M : im Falle $|M| = 1$ ist die Aussage offensichtlich richtig, und da sich aus jeder Teilmenge einer Menge $\tilde{M} \subsetneq M$ der Kardinalität $|M|-1$ durch Hinzunahme bzw. Nichthinzunahme des Elementes von $M \backslash \tilde{M}$ jeweils genau eine Teilmenge gerader wie auch ungerader Kardinalität bilden läßt, ergibt sich die Behauptung. □

1.2 Lemma *Es seien M_i, $i \in I$ endlich viele endliche Mengen, und es sei $M = \bigcup_{i\in I} M_i$. Dann gilt :*

$$|M| = \sum_{\varnothing \neq J \subseteq I} (-1)^{|J|+1} \left| \bigcap_{i\in J} M_i \right|$$

Zum Beweis überlege man sich, daß jedes Element der Vereinigung genau einmal gezählt wird : liegt $m \in M$ in genau n Teilmengen M_i, so liegt m für jedes k in genau $\binom{n}{k}$ Schnitten von je k dieser Teilmengen, und die Behauptung ergibt sich aus $\sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k} = 1$. □

1.3 Lemma *Es sei $n \in \mathbb{N}$ und $t|n$. Dann hat die zyklische Gruppe C_n der Ordnung n genau eine Untergruppe der Ordnung t. Die Automorphismen von C_n sind gegeben durch $\sigma_l : \mathrm{C}_n \to \mathrm{C}_n : g \mapsto g^l$ für $1 \leq l \leq n-1$, $\mathrm{ggT}(l,n) = 1$. Die Menge der Bahnen von C_n unter $\mathrm{Aut}(\mathrm{C}_n)$ steht in natürlicher Bijektion zur Menge der Teiler von n : für jeden Teiler t von n bildet die Menge der Elemente der Ordnung t eine Bahn unter der Operation der Automorphismengruppe. Insbesondere gilt $|\mathrm{Aut}(\mathrm{C}_n)| = \varphi(n)$ und $\omega(\mathrm{C}_n) = \tau(n)$.*

(Siehe z.B. [Hup67], S. 11, Satz 2.20 sowie S. 20/21, Satz 4.6)

1.4 Lemma *Es sei p prim, $k \in \mathbb{N}$ und $\mathrm{GF}(p^k)$ der (bis auf Isomorphie eindeutig bestimmte) Körper mit p^k Elementen. Dann gilt :*

1. *Der Körper $\mathrm{GF}(p^k)$ entsteht aus dem Primkörper $\mathrm{GF}(p)$ durch Adjunktion eines beliebigen Elements mit Minimalpolynom vom Grad k.*
2. *Die Teilkörper von $\mathrm{GF}(p^k)$ sind genau die $\mathrm{GF}(p^t)$ mit $t|k$.*
3. *Für $k_1, k_2 \in \mathbb{N}$ ist $\mathrm{GF}(p^{k_1}) \cap \mathrm{GF}(p^{k_2}) = \mathrm{GF}(p^{\mathrm{ggT}(k_1,k_2)})$.*
4. *Es sei $\sigma : \mathrm{GF}(p^k) \to \mathrm{GF}(p^k)$, $x \mapsto x^p$ der* Frobenius - Automorphismus *von $\mathrm{GF}(p^k)$. Dann ist $\mathrm{Aut}(\mathrm{GF}(p^k)) = \langle\sigma\rangle \cong \mathrm{C}_k$.*
5. *Es ist $\mathrm{GF}(p^k)^* \cong \mathrm{C}_{p^k-1}$.*
6. *In $\mathrm{GF}(p^k)\backslash\{0\}$ $(p \neq 2)$ gibt es $\frac{1}{2}(p^k-1)$ Quadrate und ebensoviele Nichtquadrate.*

(Siehe z.B. [Jun93], S. 15, Satz 1.2.2)

1.5 Definition und Lemma *Es sei $n \in \mathbb{N}$ und $q = p^k$ Primzahlpotenz.*

1. *Die* allgemeine lineare Gruppe $\mathrm{GL}(n,q)$ *vom Grad n über $\mathrm{GF}(q)$ besteht aus allen invertierbaren $n \times n$ - Matrizen über $\mathrm{GF}(q)$. Es gilt*

$$|\mathrm{GL}(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

Dies macht man sich am besten folgendermaßen klar :

- Für die erste Spalte gibt es $q^n - 1$ Belegungsmöglichkeiten (alle außer der Nullspalte).

- Für die folgenden Spalten können noch alle von den bereits gewählten Spaltenvektoren linear unabhängigen Werte eingesetzt werden; da es zu i Spalten q^i mögliche Linearkombinationen gibt, ergibt dies für die $i+1$. Spalte $q^n - q^i$ Möglichkeiten. Aufmultiplizieren liefert die angegebene Formel. □

2. *Die* allgemeine semilineare Gruppe $\Gamma\mathrm{L}(n,q)$ *vom Grad* n *über* $\mathrm{GF}(q)$ *ist die Gruppe der semilinearen Abbildungen des Vektorraums* $\mathrm{GF}(q)^n$*, also der Abbildungen von* $\mathrm{GF}(q)^n$*, die sich als Kompositum einer linearen Abbildung und einer durch einen Automorphismus von* $\mathrm{GF}(q)$ *induzierten Abbildung schreiben lassen. Da der Körper* $\mathrm{GF}(q)$ *nach Lemma 1.4 genau* k *Automorphismen besitzt, ist*

$$|\Gamma\mathrm{L}(n,q)| = k \cdot |\mathrm{GL}(n,q)|.$$

3. *Die* projektive allgemeine lineare Gruppe $\mathrm{PGL}(n,q)$ *vom Grad* n *über* $\mathrm{GF}(q)$ *entsteht aus* $\mathrm{GL}(n,q)$ *durch Herausfaktorisieren des Zentrums. Wegen* $|\mathrm{Z}(\mathrm{GL}(n,q))| = q-1$ *gilt*

$$|\mathrm{PGL}(n,q)| = \frac{|\mathrm{GL}(n,q)|}{q-1}.$$

4. *Die* projektive semilineare Gruppe $\mathrm{P}\Gamma\mathrm{L}(n,q)$ *vom Grad* n *über* $\mathrm{GF}(q)$ *entsteht aus der Gruppe* $\Gamma\mathrm{L}(n,q)$ *durch Herausfaktorisieren des Zentrums. Wegen* $|\mathrm{Z}(\Gamma\mathrm{L}(n,q))| = q-1$ *gilt*

$$|\mathrm{P}\Gamma\mathrm{L}(n,q)| = \frac{|\Gamma\mathrm{L}(n,q)|}{q-1}.$$

5. *Die* spezielle lineare Gruppe $\mathrm{SL}(n,q)$ *vom Grad* n *über* $\mathrm{GF}(q)$ *besteht aus allen Elementen von* $\mathrm{GL}(n,q)$ *mit Determinante 1. Da die Abbildung* $\det : \mathrm{GL}(n,q) \to \mathrm{GF}(q)^*,\ A \mapsto \det(A)$ *ein Homomorphismus und* $\mathrm{SL}(n,q)$ *dessen Kern ist, gilt*

$$|\mathrm{SL}(n,q)| = \frac{|\mathrm{GL}(n,q)|}{q-1}.$$

6. *Die* projektive spezielle lineare Gruppe $\mathrm{PSL}(n,q)$ *vom Grad* n *über* $\mathrm{GF}(q)$ *entsteht aus der Gruppe* $\mathrm{SL}(n,q)$ *durch Herausfaktorisieren des Zentrums. Wegen* $|\mathrm{Z}(\mathrm{SL}(n,q))| = \mathrm{ggT}(n,q-1)$ *gilt*

$$|\mathrm{PSL}(n,q)| = \frac{|\mathrm{SL}(n,q)|}{\mathrm{ggT}(n,q-1)},$$

und im Falle $\mathrm{ggT}(n,q-1) = 1$ *ist* $\mathrm{PSL}(n,q) \cong \mathrm{SL}(n,q)$*. Es gibt die folgenden* exzeptionellen Isomorphien *:* $\mathrm{PSL}(2,2) \cong \mathrm{S}_3$, $\mathrm{PSL}(2,3) \cong \mathrm{A}_4$, $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong \mathrm{A}_5$, $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$, $\mathrm{PSL}(2,9) \cong \mathrm{A}_6$ *sowie* $\mathrm{PSL}(4,2) \cong \mathrm{A}_8$*. Für* $n \geq 2$ *und* $(n,q) \notin \{(2,2),(2,3)\}$ *ist* $\mathrm{PSL}(n,q)$ *einfach.*

(Siehe z.B. [Hup67], S. 178, Hilfssatz 6.2 sowie S. 182f, Sätze 6.13 und 6.14)

1.6 Lemma (Rationale Normalform von Matrizen) *Es sei K ein Körper, $n \in \mathbb{N}$ und $A \in \mathrm{GL}(n,K)$. Dann gibt es eindeutig bestimmte $d_1,\ldots,d_r \in \mathbb{N}$ und eindeutig bestimmte Matrizen $A_i \in \mathrm{GL}(d_i,K)$, $i=1,\ldots,r$ der Form*

$$A_i = \begin{pmatrix} 0 & \cdots & 0 & -a_{i,0} \\ 1 & & 0 & -a_{i,1} \\ & \ddots & & \vdots \\ 0 & & 1 & -a_{i,d_i-1} \end{pmatrix}$$

so, daß gilt :

1. *Es gibt ein $S \in \mathrm{GL}(n,K)$ mit*

$$S^{-1}AS = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$$

2. *$\chi(A_1)|\chi(A_2)|\ldots|\chi(A_r)$*
($\chi(A_i) = x^{d_i} + \sum_{j=0}^{d_i-1} a_{i,j}x^j \in K[x]$ bezeichne das charakteristische Polynom von A_i, es gilt $\chi(A_i) = \mu(A_i)$ (Minimalpolynom von A_i))

(Vgl. hierzu etwa [Lün87], die angegebene ist nicht die allgemeinste mögliche Form dieser Aussage, genügt im folgenden jedoch vollkommen)

1.7 Lemma *Es sei $n \in \mathbb{N}$ und q Primzahlpotenz.*

1. *Es sei $G \in \{\mathrm{SL}(n,q), \mathrm{GL}(n,q)\}$ und $\phi : G \to G,\ x \mapsto (x^{-1})^t$. Für $l \in \mathbb{N}$ sei $\psi_l : G \to G,\ x \mapsto \det(x)^l x$, und setze*

$$\Psi := \{\psi_l \mid 1 \le l < q-1,\ \mathrm{ggT}(ln+1, q-1) = 1\}.$$

Dann gilt

$$\mathrm{Aut}(G) = \langle \mathrm{P\Gamma L}(n,q), \Psi, \phi \rangle .$$

Ist $G = \mathrm{SL}(n,q)$, so gilt natürlich $\Psi = \{id\}$. Im Falle $G = \mathrm{SL}(2,q)$ ist $\phi \in \mathrm{PGL}(2,q)$, und ist $G = \mathrm{GL}(2,q)$, so ist $\phi \in \langle \mathrm{PGL}(2,q), \Psi \rangle$, genauer gilt für alle $x \in \mathrm{GL}(2,q)$: $\phi(x) = \det(x)^{-1}\, x^{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)}$.

2. *Die Automorphismen von $\mathrm{SL}(n,q)$ und $\mathrm{PSL}(n,q)$ stehen in natürlicher Bijektion zueinander, d.h., jeder Automorphismus von $\mathrm{PSL}(n,q)$ läßt sich als Wirkung eines eindeutig bestimmten Automorphismus von $\mathrm{SL}(n,q)$ auf der Menge der Nebenklassen $x\,\mathrm{Z}(\mathrm{SL}(n,q)) \in \mathrm{PSL}(n,q)$ beschreiben. Insbesondere bilden diese Nebenklassen ein Blocksystem bezüglich der Operation von $\mathrm{Aut}(\mathrm{SL}(n,q))$ auf $\mathrm{SL}(n,q)$.*

3. *Die Automorphismen von $\mathrm{PGL}(n,q) = \mathrm{GL}(n,q)/Z(\mathrm{GL}(n,q))$ sind gegeben als Wirkung der Automorphismen von $\mathrm{GL}(n,q)$ auf der Menge der Nebenklassen $x\,\mathrm{Z}(\mathrm{GL}(n,q)) \in \mathrm{PGL}(n,q)$. Diese Nebenklassen bilden ein Blocksystem bezüglich der Operation von $\mathrm{Aut}(\mathrm{GL}(n,q))$ auf $\mathrm{GL}(n,q)$.*

(Zum Beweis vgl. [Die51], siehe auch [Die63])

1.8 Definition und Lemma *Sei $m \in \mathbb{N}$. Setze $q := 2^{2m+1}$, $r := 2^{m+1}$ und $K := \mathrm{GF}(q)$ (Dann ist $\theta : a \mapsto a^r$ ein Automorphismus des Körpers K so, daß $\theta^2 = \sigma_{frob}(K)$, die Umkehrung von θ ist $\theta^{-1} : a \mapsto a^{2^m}$). Für $a, b \in K$ sei*

$$M(a,b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & a^r & 1 & 0 \\ a^{r+2} + ab + b^r & a^{r+1} + b & a & 1 \end{pmatrix}$$

und $S(q)$ bezeichne die von allen $M(a,b)$ gebildete Gruppe. Matrixmultiplikation liefert $M(a,b) \cdot M(c,d) = M(a+c, a^r c + b + d)$. Jedem $\kappa \in K \backslash \{0\}$ werde die Diagonalmatrix

$$\begin{pmatrix} \kappa^{1+2^m} & 0 & 0 & 0 \\ 0 & \kappa^{2^m} & 0 & 0 \\ 0 & 0 & \kappa^{-2^m} & 0 \\ 0 & 0 & 0 & \kappa^{-1-2^m} \end{pmatrix}$$

zugeordnet und gleichfalls mit κ bezeichnet. Die Menge $K(q)$ der $\kappa's$ bildet eine zyklische Gruppe der Ordnung $q-1$, es gilt also $K(q) \cong K^*$. Matrixmultiplikation liefert $\kappa^{-1} M(a,b) \kappa = M(a\kappa, b\kappa^{r+1})$, die von $S(q)$ und $K(q)$ erzeugte Gruppe $H(q)$ hat also die Ordnung $q^2(q-1)$. Ist nun

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

so ist die Suzuki-Gruppe $\mathrm{Sz}(q)$ *definiert als das Erzeugnis von $H(q)$ und T. Es gilt für $G := \mathrm{Sz}(q)$:*

1. *G ist eine einfache Gruppe der Ordnung $q^2(q-1)(q^2+1)$. Die Ordnung von G ist nicht durch 3, aber durch 5 teilbar.*

2. *Sind t_1 und t_2 Teiler von $2m+1$, so sind $\mathrm{Sz}(2^{t_1})$ und $\mathrm{Sz}(2^{t_2})$ Untergruppen von G, und es gilt $\mathrm{Sz}(2^{t_1}) \cap \mathrm{Sz}(2^{t_2}) = \mathrm{Sz}(2^{\mathrm{ggT}(t_1,t_2)})$.*

3. *Liegt b in keinem echten Teilkörper von K, so ist $G = < M(1,b),\ T >$.*

4. *G ist eine* CN - Gruppe, *d.h., jedes vom Neutralelement verschiedene Element von G hat nilpotenten Zentralisator in G.*

5. *Die 2 - Sylowgruppen von G sind konjugiert zu $S(q)$. Der Exponent von $S(q)$ ist 4, der Normalisator von $S(q)$ in G ist $H(q)$.*

6. *Die p - Sylowgruppen von G für $p \neq 2$ sind zyklisch.*

7. *G hat zyklische Untergruppen $U_i(q)$, $i = 1, 2$ der Ordnungen $q + r + 1$ bzw. $q - r + 1$. Diese sind Hall-Untergruppen. Die Konjugierten von $S(q)$, $K(q)$, $U_1(q)$ und $U_2(q)$ bilden eine Partition von G in Untergruppen, und sind daher insbesondere auch TI-Untergruppen von G. (Eine Untergruppe heißt* TI-Untergruppe, *wenn sie mit allen von ihr verschiedenen Konjugierten einen trivialen Schnitt hat).*

8. *Es gilt* $|\mathrm{N}_G(K(q)) : K(q)| = 2$, *und für* $i = 1, 2$ *ist* $|\mathrm{N}_G(U_i) : U_i| = 4$.

9. *Alle Involutionen von* G *sind zueinander konjugiert, es gibt zwei Konjugiertenklassen aus Elementen der Ordnung 4 (diese lassen sich nicht durch einen Automorphismus von* G *ineinander überführen), ferner gibt es* $\frac{|K(q)|-1}{2} = \frac{q-2}{2}$ *Konjugiertenklassen, die einen nichttrivialen Schnitt mit* $K(q)$ *haben, und für* $i \in \{1, 2\}$ *gibt es* $\frac{|U_i|-1}{4} = \frac{q \pm r}{4}$ *Konjugiertenklassen, die einen nichttrivialen Schnitt mit* $U_i(q)$ *haben. Zusammen mit der Konjugiertenklasse, die das Neutralelement enthält, hat* G *folglich insgesamt* $1 + 1 + 2 + \frac{q-2}{2} + \frac{q+r}{4} + \frac{q-r}{4} = q + 3$ *Konjugiertenklassen.*

10. $\mathrm{Out}(G) \cong \mathrm{Aut}(K) \cong \mathrm{C}_{2m+1}$, *genauer : jedes Element von* $\mathrm{Out}(G)$ *hat einen Repräsentanten, der in natürlicher Weise induziert wird durch einen Automorphismus von* K. *Es bezeichne* ς_q *den Automorphismus von* G, *der vom Frobenius - Automorphismus von* K *induziert wird.*

11. *Im projektiven Raum* $\mathbb{P}(3, q)$ *sei* $p_\infty := (1, 0, 0, 0)$, *und für* $x, y \in K$ *sei* $p(x, y) := (x^{r+2} + xy + y^r, y, x, 1)$. *Dann ist das* Tits'sche Ovoid $\mathcal{O}(q)$ *gegeben durch* $\mathcal{O}(q) := \{p_\infty\} \cup \{p(x, y) \mid x, y \in K\}$. *Es induziert* G *auf* $\mathbb{P}(3, q)$ *die Gruppe aller projektiven (d.h. linear induzierten) Kollineationen, die* $\mathcal{O}(q)$ *als Menge stabilisieren.* G *operiert zweifach transitiv und treu auf* $\mathcal{O}(q)$. *Es gilt* $G_{p_\infty} = H(q)$ *und* $G_{p(0,0)} = K(q)$, *nur das Neutralelement läßt mehr als zwei Punkte fest.*

(Siehe [Suz62], insbes. Abschnitte 13, 16 und 17, [HB82], Kapitel XI.3 und XI.5 sowie [Lün80], Abschnitte 21, 22 und 24)

1.9 Satz *Die minimalen einfachen Gruppen, also die nicht-abelschen einfachen Gruppen, deren sämtliche echten Untergruppen auflösbar sind, sind gegeben durch*

1. $\mathrm{PSL}(2, 2^p)$ *für eine Primzahl* p

2. $\mathrm{PSL}(2, 3^p)$ *für eine ungerade Primzahl* p

3. $\mathrm{PSL}(2, p)$ *für eine Primzahl* $p \neq 3$ *mit* $p^2 + 1 \equiv 0$ *(mod 5)*

4. $\mathrm{PSL}(3, 3)$

5. $\mathrm{Sz}(2^p)$ *für eine ungerade Primzahl* p

(Dies wird hergeleitet in [Tho68], vgl. Korollar 1 in Abschnitt 3 auf Seite 388).

1.10 Definition und Satz *Eine* Zassenhaus - Gruppe *ist eine endliche zweifach transitive Permutationsgruppe, deren einziges Element, das mehr als zwei Punkte fixiert, das Neutralelement ist und die keinen regulären Normalteiler hat. Die einfachen Zassenhaus-Gruppen sind gegeben durch*

1. $\mathrm{PSL}(2, q)$ *für Primzahlpotenzen* $q > 3$

2. *Die Suzuki-Gruppen* $\mathrm{Sz}(q)$

(Siehe [HB82], Kapitel XI, Definition 1.2 und Beispiele 1.3; dort findet sich auch eine Beschreibung der übrigen (nicht-einfachen) Zassenhaus-Gruppen).

Kapitel 2

Die linearen Gruppen

2.1 Lemma *Es sei q Primzahlpotenz und $G \in \{\mathrm{SL}(2,q), \mathrm{GL}(2,q)\}$.*

1. *Setze*

$$\mathfrak{K} := \mathrm{Z}(\mathrm{GL}(2,q)) \cup \left\{ \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} \;\middle|\; a,b \in \mathrm{GF}(q),\ b \neq 0 \right\}.$$

   Dann bildet $\mathfrak{K} \cap G$ ein Repräsentantensystem für die Menge der Konjugiertenklassen von G, es gibt also ein Repräsentantensystem $\mathfrak{R} \subseteq \mathfrak{K} \cap G$ für die Menge der Bahnen in G unter der Operation von $\mathrm{Aut}(G)$.

2. *Die Menge*

$$\mathfrak{K} := \left\{ \begin{array}{l} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \end{array} \right\}$$

   bildet ein Repräsentantensystem für die Menge der Konjugiertenklassen von $\mathrm{SL}(3,3)$.

Beweis :

1. Diese Aussage ist eine unmittelbare Konsequenz aus Lemma 1.6 (man mache sich klar, welche Blockstrukturen rationaler Normalformen von Elementen von $\mathrm{GL}(2,q)$ vorkommen; wegen $\mathrm{SL}(2,q) \trianglelefteq \mathrm{GL}(2,q)$ überträgt sich dies problemlos auf $\mathrm{SL}(2,q)$).

2. Hier gilt Entsprechendes; man beachte, daß es in GF(3) keine von 1 verschiedene 3. Einheitswurzel gibt, das Zentrum von $\mathrm{SL}(3,3)$ also trivial ist, und daß sich eine Matrix mit $1 \times 1 \ - \ 2 \times 2$ - Blockstruktur nur dann in rationaler Normalform befindet, wenn das Minimalpolynom des 2×2 - Blocks durch das des 1×1 - Blocks teilbar ist. □

2.2 Lemma *Es sei $n \in \mathbb{N}$, q Primzahlpotenz und $A \in \mathrm{GL}(n,q)$. Befindet sich die Matrix A in rationaler Normalform, so ändert sich an dieser Eigenschaft nichts, wenn man auf jeden Eintrag einen fest gewählten Automorphismus von $\mathrm{GF}(q)$ anwendet.*

Beweis : Nach Lemma 1.6 genügt es zu zeigen, daß die Teilbarkeitsrelationen der charakteristischen Polynome der Blöcke von A erhalten bleiben. Aufgrund der Gestalt der betrachteten Blöcke ist es hierzu hinreichend, daß die Teilbarkeitsbeziehung $P_2|P_1$ zweier Polynome $P_1, P_2 \in \mathrm{GF}(q)[x]$ erhalten bleibt, wenn man auf jeden Koeffizienten einen festen Körperautomorphismus α anwendet. Dies trifft jedoch zu, da es im Falle $P_2|P_1$ ein $P_3 \in \mathrm{GF}(q)[x]$ mit $P_1 = P_2 \cdot P_3$ gibt, und sich an der Gültigkeit dieser Gleichung durch Anwenden von α auf alle Koeffizienten nichts ändert, zumal die Koeffizienten von P_1 Summen von Produkten von Koeffizienten von P_2 und P_3 sind und sich die Reihenfolge von Addition bzw. Multiplikation und der Anwendung von Körperautomorphismen umkehren läßt. □

2.3 Lemma *Es sei p prim und $k \in \mathbb{N}$. Für einen endlichen Körper K bezeichnen wir mit $\omega(K)$ die Anzahl der Bahnen, in die K unter der Operation seiner Automorphismengruppe zerfällt, und für eine Menge M von Teilern von k sei - hier wie im ganzen Rest der Arbeit - $T_{k,M} := \mathrm{ggT}_{t \in M} \frac{k}{t}$. Dann gilt :*

$$\omega(\mathrm{GF}(p^k)) = \frac{p^k}{k} + \sum_{\varnothing \neq M \subseteq \pi(k)} (-1)^{|M|} \left(\frac{p^{T_{k,M}}}{k} - \omega(\mathrm{GF}(p^{T_{k,M}})) \right)$$

Beweis : Die Menge $\mathrm{GF}(p^k)_{\max}$ der in keinem echten Teilkörper von $\mathrm{GF}(p^k)$ liegenden Elemente von $\mathrm{GF}(p^k)$ zerfällt unter der Operation von $\mathrm{Aut}(\mathrm{GF}(p^k))$ in Bahnen der Länge $k = |\mathrm{Aut}(\mathrm{GF}(p^k))|$, da von diesen Elementen als Nullstellen irreduzibler Polynome vom Grad k über $\mathrm{GF}(p)$ jeweils k zueinander konjugiert sind. Aus Lemma 1.4, Teil 2 und 3 sowie Lemma 1.2 folgt :

$$\begin{aligned} \left|\mathrm{GF}(p^k)_{\max}\right| &= \left|\mathrm{GF}(p^k)\right| - \left| \bigcup_{t|k, t \neq k} \mathrm{GF}(p^t) \right| \\ &= p^k - \left| \bigcup_{t \in \pi(k)} \mathrm{GF}(p^{\frac{k}{t}}) \right| \\ &= p^k - \sum_{\varnothing \neq M \subseteq \pi(k)} (-1)^{|M|+1} \, p^{T_{k,M}} \end{aligned}$$

Anwenden von Lemma 1.2 auf die Mengen der Bahnen der maximalen Teilkörper von $\mathrm{GF}(p^k)$ liefert nun die Behauptung. □

2.4 Satz *Sei p prim und $k \in \mathbb{N}$.*

1. *Es gilt*

$$\omega(\mathrm{SL}(2,p)) = \begin{cases} 3 & \text{falls } p = 2 \\ p+2 & \text{sonst} \end{cases}$$

Für $k > 1$ gilt

$$\begin{aligned} \omega(\mathrm{SL}(2,p^k)) &= \omega(\mathrm{GF}(p^k)) + \begin{cases} 1 & \text{falls } p = 2 \\ 2 & \text{sonst} \end{cases} \\ &= \frac{p^k}{k} + \sum_{\varnothing \neq M \subseteq \pi(k)} (-1)^{|M|} \left(\frac{p^{T_{k,M}}}{k} - \omega(\mathrm{SL}(2,p^{T_{k,M}})) \right) \end{aligned}$$

2. *Für $p = 2$ ist $\mathrm{PSL}(2,p^k) \cong \mathrm{SL}(2,p^k)$. Für ungerades p gilt*

$$\omega(\mathrm{PSL}(2,p)) = \frac{p+3}{2}$$

und

$$\begin{aligned} \omega(\mathrm{PSL}(2,p^k)) &= \frac{p^k + H(p,k)}{2k} \\ &\quad + \sum_{\varnothing \neq M \subseteq \pi(k)} (-1)^{|M|} \left(\frac{p^{T_{k,M}}}{2k} - \omega(\mathrm{PSL}(2,p^{T_{k,M}})) \right) \end{aligned}$$

wobei

$$H(p,k) = \begin{cases} 0 & \text{falls } 2 \nmid k \\ p^{\frac{k}{2}} - 1 & \text{falls } k \text{ Zweierpotenz} \\ p^{\frac{k}{2}} + \sum\limits_{\varnothing \neq M \subseteq \pi(k)\setminus\{2\}} (-1)^{|M|}\, p^{\mathrm{ggT}_{t \in M} \frac{k}{2t}} & \text{sonst} \end{cases}$$

Beweis : Wir wählen aus

$$\mathfrak{K} := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix} \,\middle|\, a \in \mathrm{GF}(p^k) \right\}$$

ein Repräsentantensystem $\mathfrak{R}$ für die Menge der Bahnen von $\mathrm{SL}(2,p^k)$ unter der Operation von $\mathrm{Aut}(\mathrm{SL}(2,p^k))$. (Diese Wahl von $\mathfrak{R}$ ist möglich gemäß Lemma 2.1). Zu bestimmen ist $|\mathfrak{R}|$. Bahnenzerlegung induziert auf $\mathfrak{K}\backslash\mathrm{Z}(\mathrm{SL}(2,p^k))$ eine Partition in Mengen der Form

$$\mathfrak{K}_a = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & a^{p^i} \end{pmatrix} \,\middle|\, i = 0, \ldots, k-1 \right\}$$

für $a \in \mathrm{GF}(p^k)$, denn sind $X, Y \in \mathrm{SL}(2,p^k)$ in rationaler Normalform und lassen sich unter der Operation von $\mathrm{Aut}(\mathrm{SL}(2,p^k))$ ineinander überführen, so genügt dafür ein Körperautomorphismus α, angewandt auf die jeweiligen Einträge : $((g^{-1}Xg)^\alpha = Y \Leftrightarrow g^{-1}Xg = Y^{\alpha^{-1}}) \underset{\text{Lemma 1.6}}{\Longrightarrow} X = g^{-1}Xg,\ X^\alpha = Y$ (vgl. Lemma 1.7). Die Gleichung aus Teil (1) für Primkörper sowie die erste Gleichung für den Fall $k > 1$ ergeben sich jetzt direkt aus dem Umstand, daß

die beiden Bahnen im Zentrum von $\mathrm{SL}(2,p^k)$ für $p=2$ zusammenfallen; die verbleibende Gleichung erhalten wir dann daraus mit Lemma 2.3 und Lemma 1.1.

Wir betrachten nun die Gruppen $\mathrm{PSL}(2,p^k)$ für ungerade Primzahlen p. Es bezeichne $\kappa : \mathrm{SL}(2,p^k) \to \mathrm{PSL}(2,p^k),\ x \mapsto x\,\mathrm{Z}(\mathrm{SL}(2,p^k))$ die kanonische Projektion. Uns interessiert deren Verhalten auf der Menge $\mathfrak{K}$. Wegen

$$\begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix}^{\kappa} = \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}^{\kappa} \quad \text{und} \quad \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$$

fusionieren $\mathfrak{K}_{-a}$ und $\mathfrak{K}_a$ unter κ, ebenso wie die beiden im Zentrum von $\mathrm{SL}(2,p^k)$ liegenden Bahnen. Da die Automorphismen von $\mathrm{SL}(2,p^k)$ und $\mathrm{PSL}(2,p^k)$ in natürlicher Bijektion zueinander stehen (Lemma 1.7, Teil 2), können wir nun nach obigem o.B.d.A. $a \in \mathrm{GF}(p^k)_{\max}$ annehmen und die übrigen Fälle mit Lemma 1.2 abhandeln. Im Fall $a = -a^{p^i}$ für ein $i \in \mathbb{N}$ ist $\mathfrak{K}_{-a} = \mathfrak{K}_a$, wir erhalten also eine Bahn der Länge k, andernfalls eine der Länge $2k$. Es bezeichne $H(p,k)$ die Anzahl der Elemente, die in Bahnen der Länge k liegen. Für ungerade k ist offensichtlich $H(p,k) = 0$. Der Fall $a = -a^{p^i}$ tritt genau dann ein, wenn a und $-a$ zueinander konjugiert, also Lösung einer irreduziblen quadratischen Gleichung $(x-a)(x+a) = x^2 - a^2 = x^2 - b = 0$ über $\mathrm{GF}(p^{\frac{k}{2}})$ sind. Zu jedem Nichtquadrat $b \in \mathrm{GF}(p^{\frac{k}{2}})$, dessen Quadratwurzeln in keinem echten Teilkörper von $\mathrm{GF}(p^k)$ liegen, gibt es folglich zwei derartige Elemente. Da es nach Lemma 1.4, Teil 6 für $t \in \mathbb{N}$ in $\mathrm{GF}(p^t)$ genau $\frac{1}{2}(p^t-1)$ Nichtquadrate gibt, ergeben sich mit Lemma 1.4, Teil 2 und 3 sowie Lemma 1.2 die angegebenen Formeln für $H(p,k)$ für gerade k. Analog wie beim Beweis von Teil (1) erhalten wir jetzt die Behauptung. □

2.5 Beispiel *Da* $\mathrm{GF}(729)$ *der kleinste Körper mit ungerader Charakteristik und bezüglich der Inklusionsrelation nicht totalgeordnetem Teilkörperverband ist, wollen wir zur Illustration des im Beweis dargestellten Gedankenganges exemplarisch den Wert von* $\omega(\mathrm{PSL}(2,729))$ *bestimmen.*

Hierzu zählen wir die zu $\mathrm{SL}(2,729)$ gehörigen Mengen $\mathfrak{K}_a$, und wenden das im Beweis angegebene Kriterium für die Gleichheit von $\mathfrak{K}_a$ und $\mathfrak{K}_{-a}$ an. Jeweils separat zu zählen sind die durch $\{\mathfrak{K}_a, \mathfrak{K}_{-a}\}$ gegebenen Äquivalenzklassen mit $\underbrace{a \in \mathrm{GF}(3)}_{\text{Fall 1}}$, $\underbrace{a \in \mathrm{GF}(9)_{\max}}_{\text{Fall 2}}$, $\underbrace{a \in \mathrm{GF}(27)_{\max}}_{\text{Fall 3}}$ sowie $\underbrace{a \in \mathrm{GF}(729)_{\max}}_{\text{Fall 4}}$:

- Fall 1 liefert eine Klasse der Länge 1 (für $a=0$) und eine der Länge 2.
- Es ist $|\mathrm{GF}(9)_{\max}| = 9-3 = 6$. In $\mathrm{GF}(3)$ gibt es ein Nichtquadrat, folglich liefert Fall 2 eine Klasse der Länge 1 und eine der Länge 2.
- Es ist $|\mathrm{GF}(27)_{\max}| = 27-3 = 24$. Da 27 keine Quadratzahl ist, gibt es in Fall 3 nur Klassen der Länge 2, und zwar $\frac{24}{6} = 4$ Stück.
- Es ist $|\mathrm{GF}(729)_{\max}| = 729-27-9+3 = 696$. In $\mathrm{GF}(27)_{\max}$ gibt es $\frac{|\mathrm{GF}(27)_{\max}|}{2} = 12$ Nichtquadrate, Fall 4 liefert folglich $\frac{2\cdot 12}{6} = 4$ Klassen der Länge 1 und $\frac{696-2\cdot 12}{12} = 56$ Klassen der Länge 2.

Aufsummieren der gegebenen Klassenanzahlen sowie Berücksichtigung der Bahn des Neutralelements liefert als Ergebnis $\omega(\mathrm{PSL}(2,729)) = 69$. □

2.6 Korollar *Für prime p und $k \in \mathbb{N}$ gilt :*

1. $$\omega(\mathrm{SL}(2,p^k)) > \frac{p^k}{k}, \quad \omega(\mathrm{PSL}(2,p^k)) > \frac{p^k}{(2-\delta_{2,p})k}$$

2. $$\lim_{k\to\infty} \frac{\omega(\mathrm{SL}(2,p^k))}{\frac{p^k}{k}} = \lim_{k\to\infty} \frac{\omega(\mathrm{PSL}(2,p^k))}{\frac{p^k}{(2-\delta_{2,p})k}} = 1$$

3. *Es sei $p \neq 2$ und k prim. Dann gilt :*

$$\omega(\mathrm{SL}(2,p^k)) = \frac{p^k + (k-1)p + 2k}{k}$$

Ist $k \neq 2$, so gilt :

$$\omega(\mathrm{PSL}(2,p^k)) = \frac{p^k + (k-1)p + 3k}{2k}$$

Beweis :

1. Diese Ungleichungen gelten, da kein $\mathfrak{K}_a$ länger als k ist, unter κ nie mehr als je zwei $\mathfrak{K}_a$ fusionieren und da die Bahn des Neutralelements keine der Mengen $\mathfrak{K}_a$ trifft (vgl. den Beweis des Satzes).

2. Die Anzahl der maximalen Teilkörper von $\mathrm{GF}(p^k)$ ist gleich der Anzahl der verschiedenen Primteiler von k, also sicher nicht größer als $\log_2(k)$. Für einen maximalen Teilkörper K von $\mathrm{GF}(p^k)$ gilt $|K| \leq p^{\frac{k}{2}}$, und $\mathrm{SL}(2,K)$ zerfällt unter der Operation von $\mathrm{Aut}(\mathrm{SL}(2,p^k))_{\{\mathrm{SL}(2,K)\}}$ in nicht mehr als $|K|+2$ Bahnen. Wegen $|\mathfrak{K}_a| = k$ für $a \in \mathrm{GF}(p^k)_{\max}$ (vgl. den Beweis des Satzes) gilt

$$\omega(\mathrm{SL}(2,p^k)) \leq \frac{p^k}{k} + (p^{\frac{k}{2}}+2)\log_2(k) + 2 = (1 + \underbrace{\frac{k(p^{\frac{k}{2}}+2)\log_2(k)+2k}{p^k}}_{\to 0 \text{ für } k\to\infty})\frac{p^k}{k},$$

und mit der Ungleichung aus Teil (1) folgt die Behauptung. Die Aussage für $\omega(\mathrm{PSL}(2,p^k))$ zeigt man völlig analog.

3. Diese Gleichungen folgen direkt durch Einsetzen in die Formeln im 1. bzw. 2. Teil des Satzes. □

2.7 Satz *Sei $q = p^k$ Primzahlpotenz. Dann gilt $\omega(\mathrm{PGL}(2,q)) = \omega(\mathrm{SL}(2,q))$.*

Beweis : Es kann o.B.d.A. q ungerade angenommen werden (ansonsten ist ohnehin $\mathrm{PGL}(2,q) \cong \mathrm{SL}(2,q)$). Wir gehen analog vor wie im Beweis von Satz 2.4. Es bezeichne $\kappa : \mathrm{GL}(2,q) \to \mathrm{PGL}(2,q),\ x \mapsto x\,\mathrm{Z}(\mathrm{GL}(2,q))$ die kanonische Projektion. Es seien $a, b, c \in \mathrm{GF}(q)$. Die rationale Normalform von

$$\begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \quad \text{ist} \quad \begin{pmatrix} 0 & bc^2 \\ 1 & ac \end{pmatrix},$$

also fallen für alle a, b, c die Bahnen von

$$\begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix} \in \mathrm{GL}(2,q) \quad \text{und} \quad \begin{pmatrix} 0 & bc^2 \\ 1 & ac \end{pmatrix} \in \mathrm{GL}(2,q)$$

unter der Operation von $\mathrm{Aut}(\mathrm{GL}(2,q))$ unter κ zusammen. Zu $a = 0$ erhalten wir also zwei Bahnen von $\mathrm{PGL}(2,q)$ unter der Operation von $\mathrm{Aut}(\mathrm{PGL}(2,q))$: je eine für b Quadrat und b Nichtquadrat in $\mathrm{GF}(q)$. Im Falle $a \neq 0$ wählen wir $c := a^{-1}$. Wir sehen hier nun, daß es genügt, die durch Bahnenzerlegung auf der Menge

$$\mathfrak{K} := \left\{ \begin{pmatrix} 0 & d \\ 1 & 1 \end{pmatrix} \,\middle|\, d \in \mathrm{GF}(q) \right\}$$

induzierte Partition zu betrachten. Mit fast wörtlich derselben Argumentation wie im Beweis von Satz 2.4 schließen wir, daß die Elemente dieser Partition von der Gestalt

$$\mathfrak{K}_d = \left\{ \begin{pmatrix} 0 & d^{p^i} \\ 1 & 1 \end{pmatrix} \,\middle|\, i = 0, \ldots, k-1 \right\}$$

für $d \in \mathrm{GF}(q)\backslash\{0\}$ sind. Bestimmen wir nun deren Anzahl unter Verwendung von Lemma 2.3 und berücksichtigen schlußendlich noch die Bahn des Neutralelements, so erhalten wir durch Vergleich mit Satz 2.4, Teil 1 die Behauptung. □

2.8 Lemma *Es sei q ungerade Primzahlpotenz, $G := \mathrm{GL}(2,q)$ und $Z := \mathrm{Z}(G)$. Dann lassen sich alle Automorphismen von Z zu Automorphismen von ganz G fortsetzen.*

Beweis : Es sei Ψ wie in Lemma 1.7, $\psi_l \in \Psi$ und $a \in \mathrm{GF}(q)$. Dann gilt

$$\psi_l \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a^{2l} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{2l+1} & 0 \\ 0 & a^{2l+1} \end{pmatrix}.$$

Da $q-1$ gerade ist, lassen sich alle zu $q-1$ teilerfremden Zahlen $\tilde{l}$ in der Form $\tilde{l} = 2l+1$ schreiben, es gibt also zu jedem Automorphismus $\sigma_{\tilde{l}}$ von $Z \cong \mathrm{C}_{q-1}$ (vgl. Lemma 1.3) einen Automorphismus $\psi_l \in \Psi \subseteq \mathrm{Aut}(G)$ so, daß $\psi_l|_Z = \sigma_{\tilde{l}}$. □

2.9 Lemma *Sei $p \neq 2$ prim und $t = 2r$ ein gerader Teiler von $p-1$. Dann gibt es ein $s \in \{0, \ldots, \frac{p-1}{t} - 1\}$ so, daß für $l := (2s+1)r$ gilt :* $\mathrm{ggT}(2l+1, p-1) = 1$.

Beweis : Wegen $r|l$ gilt $\mathrm{ggT}(2l+1, t) = 1$, es genügt also zu zeigen, daß es ein l mit den geforderten Eigenschaften so gibt, daß für den größten zu t teilerfremden Teiler $\tilde{t}$ von $p-1$ die Bedingung $\mathrm{ggT}(2l+1, \tilde{t}) = 1$ erfüllt ist. Da jedoch l und damit wegen $2 \nmid \tilde{t}$ auch $2l+1$ für $s = 0, \ldots, \frac{p-1}{t} - 1$ ein vollständiges Restsystem (mod $\tilde{t}$) durchläuft und $\varphi(\tilde{t}) > 0$ ist, ist dies stets der Fall. □

2.10 Satz *Sei $p \neq 2$ prim. Dann gilt*

$$\begin{aligned}\omega(\mathrm{GL}(2,p)) &= 2\tau(p-1) + \sum_{t|p-1} \frac{p-1}{\mathrm{ggT}(t,2)} \\ &= (p+1)\,\tau(p-1) - \frac{p-1}{2}\,\tau\left(\frac{p-1}{2}\right)\end{aligned}$$

Beweis : Wir setzen $G := \mathrm{GL}(2,p)$ sowie $Z := \mathrm{Z}(G)$, und wählen aus

$$\mathfrak{K} := Z \cup \left\{ M(a,b) := \begin{pmatrix} 0 & b \\ -1 & a \end{pmatrix} \,\middle|\, a,b \in \mathrm{GF}(p),\ b \neq 0 \right\}$$

ein Repräsentantensystem $\mathfrak{R}$ für die Menge der Bahnen von G unter der Operation von $\mathrm{Aut}(G)$. (Diese Wahl ist möglich, da für alle $a,b \in \mathrm{GF}(p)$ die Matrix $-M(-a,b) \sim M(a,b)$ in rationaler Normalform ist, und die Menge der $M(a,b)$ damit nach Lemma 2.1 ein Repräsentantensystem für die Menge der zu $G\backslash Z$ gehörigen Konjugiertenklassen von G bildet). Die Gruppe $Z \cong \mathrm{C}_{p-1}$ zerfällt nach Lemma 1.3 unter der Operation von $\mathrm{Aut}(Z)$ in $\tau(p-1)$ Bahnen. Da sich nach Lemma 2.8 alle Automorphismen von Z zu Automorphismen von ganz G fortsetzen lassen, impliziert dies $|\mathfrak{R} \cap Z| = \tau(p-1)$. Es verbleibt die Untersuchung von $\mathfrak{K}\backslash Z$. Wir betrachten zunächst den Fall $a = 0$. Hierzu sei $\mathfrak{B} := \{M(0,b) \mid b \in \mathrm{GF}(p)^*\}$. Es gilt

$$\psi_l(M(0,b)) = \begin{pmatrix} 0 & b^{l+1} \\ -b^l & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & b^{2l+1} \\ -1 & 0 \end{pmatrix} = M(0, b^{2l+1}),$$

und da $p-1$ gerade ist, läßt sich jeder zu $p-1$ teilerfremde Exponent in der Form $2l+1$ schreiben, $\mathrm{Aut}(G)_{\{\mathfrak{B}\}}$ operiert also nach Lemma 1.3 auf $\mathfrak{B}$ wegen $\mathrm{GF}(p)^* \cong \mathrm{C}_{p-1}$ wie $\mathrm{Aut}(\mathrm{C}_{p-1})$ auf C_{p-1}, die Menge $\mathfrak{B}$ zerfällt somit unter dieser Operation in $\tau(p-1)$ Bahnen. Da sich kein Element von $\mathfrak{B}$ durch einen Automorphismus der Gruppe G auf ein Element von $\mathfrak{K}\backslash\mathfrak{B}$ abbilden läßt, erhalten wir $|\mathfrak{R} \cap \mathfrak{B}| = \tau(p-1)$. Ist $\mathrm{ord}(b) = t$, so hat die Bahn von $M(0,b)$ unter der Operation von $\mathrm{Aut}(G)_{\{\mathfrak{B}\}}$ die Länge $\varphi(t)$. (Vgl. Lemmata 1.3, 1.4 und 1.7). Im Fall $a \neq 0$ gilt für ungerade t Entsprechendes, für gerade t fusionieren zusätzlich noch die Bahnen von $M(a,b)$ und $M(-a,b)$ unter der Operation von $\mathrm{Aut}(G)$, was eine Verdopplung der Länge der Bahn von $M(a,b)$ von $\mathfrak{K}$ unter der Operation von $\mathrm{Aut}(G)_{\{\mathfrak{K}\}}$ auf $2\varphi(t)$ bewirkt, denn für $l \in \mathbb{N}$ gilt

$$\psi_l(M(a,b)) = \begin{pmatrix} 0 & b^{l+1} \\ -b^l & ab^l \end{pmatrix} \sim \begin{pmatrix} 0 & b^{2l+1} \\ -1 & ab^l \end{pmatrix} = M(ab^l, b^{2l+1})$$

sowie $b^l \neq 1 \wedge b^{2l+1} = b \Leftrightarrow \mathrm{ord}(b) \nmid l \wedge \mathrm{ord}(b) \mid 2l \Leftrightarrow b^l = -1$, die Existenz eines geeigneten $\psi_l \in \Psi$ folgt aus Lemma 2.9. Summation über die möglichen Ordnungen von b, also die Teiler von $p-1$, liefert den behaupteten Wert für $\omega(\mathrm{GL}(2,p))$. Die Gültigkeit der zweiten Formel ergibt sich dann daraus, daß die Anzahl der geraden Teiler von $p-1$ gleich $\tau(\frac{p-1}{2})$ ist. □

2.11 Satz *Es gilt* $\omega(\mathrm{PSL}(3,3)) = 9$.

Beweis : Es sei $G := \mathrm{SL}(3,3)$. Da $\mathrm{Z}(G)$ trivial ist (siehe Lemma 1.5 oder den Beweis von Lemma 2.1), ist $G \cong \mathrm{PSL}(3,3)$. Es sei ϕ wie in Lemma 1.7 und $\mathfrak{K}$ das in Lemma 2.1 angegebene Repräsentantensystem für die Konjugiertenklassen von G. Nach Lemma 1.7 genügt es zu untersuchen, welche Konjugiertenklassen durch ϕ fusioniert werden. Da ϕ auf 1×1 - Blöcken wie die Identität und auf 2×2 - Blöcken wie eine Konjugation wirkt, reicht es, die Wirkung von ϕ auf den Konjugiertenklassen zu betrachten, deren Elemente eine rationale Normalform A besitzen, die aus einem einzigen 3×3 - Block besteht. Ist

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & b \\ 0 & 1 & a \end{pmatrix},$$

so ist $\chi(A) = x^3 - ax^2 - bx - 1$, und $\phi(A)$ ist konjugiert zur Begleitmatrix von $\chi(\phi(A)) = -x^3(\chi(A)(\frac{1}{x})) = -x^3((\frac{1}{x})^3 - a(\frac{1}{x})^2 - b(\frac{1}{x}) - 1) = x^3 + bx^2 + ax - 1$:

$$\phi(A) \sim \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -a \\ 0 & 1 & -b \end{pmatrix},$$

und wenn wir uns jetzt dazu das Repräsentantensystem $\mathfrak{K}$ für die Konjugiertenklassen von G anschauen, sehen wir, daß von den in Frage kommenden neun Matrizen sechs jeweils paarweise durch Automorphismen von G ineinander übergeführt werden können. Es ist also $\omega(G) = |\mathfrak{K}| - \frac{6}{2} = 12 - 3 = 9$. □

2.12 Bemerkung *Die Gruppe* $\mathrm{PSL}(3,3) \cong \mathrm{SL}(3,3) =: G$ *hat die Ordnung* $\frac{1}{2}(3^3-1)(3^3-3)(3^3-3^2) = 2^4 \cdot 3^3 \cdot 13 = 5616$, *und enthält Elemente der Ordnungen 1, 2, 3, 4, 6, 8 und 13. Bringen wir die im Beweis des Satzes konstruierten Repräsentanten auf Jordan'sche Normalform, so erhalten wir das folgende Repräsentantensystem für die Menge der Bahnen in der Gruppe* G *unter der Operation von* $\mathrm{Aut}(G)$ *:*

$$\left\{ \begin{array}{lll}
\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\text{Ordnung 1, Bahnlänge 1}}, & \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}}_{\text{Ordnung 2, Bahnlänge 117}}, & \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}}_{\text{Ordnung 4, Bahnlänge 702}}, \\
\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\text{Ordnung 3, Bahnlänge 104}}, & \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\text{Ordnung 3, Bahnlänge 624}}, & \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}}_{\text{Ordnung 6, Bahnlänge 936}}, \\
\underbrace{\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}}_{\text{Ordnung 8, Bahnlänge 1404}}, & \underbrace{\begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{\text{Ordnung 13, Bahnlänge jeweils 864}}, & \underbrace{\begin{pmatrix} 0 & 1 & 1 \\ -1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{\text{Ordnung 13, Bahnlänge jeweils 864}}
\end{array} \right\}$$

(Die Bahnlängen wurden mit Hilfe von GAP *berechnet)*

Kapitel 3

Die Suzuki - Gruppen

Wir nehmen in diesem Kapitel laufend Bezug auf Lemma 1.8 und übernehmen die dortigen Bezeichnungen.

3.1 Lemma *Es sei n ungerade, s ein Teiler von n und $q = 2^n = \tilde{q}^s$. Dann gilt :*

$$\mathrm{ggT}(q^2+1, |\mathrm{GL}(4,\tilde{q})|) \mid \tilde{q}^2+1$$

Beweis : Nach Lemma 1.5 gilt

$$\begin{aligned}|\mathrm{GL}(4,\tilde{q})| &= (\tilde{q}^4-1)(\tilde{q}^4-\tilde{q})(\tilde{q}^4-\tilde{q}^2)(\tilde{q}^4-\tilde{q}^3)\\ &= \tilde{q}^6(\tilde{q}-1)^2(\tilde{q}^2-1)^2(\tilde{q}^2+1)(\tilde{q}^2+\tilde{q}+1),\end{aligned}$$

daher genügt es zu zeigen, daß $q^2+1 = \tilde{q}^{2s}+1$ zu $\tilde{q}-1$, $\tilde{q}^2-1$ und $\tilde{q}^2+\tilde{q}+1$ teilerfremd ist :

- Wegen $(\tilde{q}-1)|(\tilde{q}^{2s}-1)$ läßt $\tilde{q}^{2s}+1$ bei Division durch $\tilde{q}-1$ den Rest 2. Die Teilerfremdheitsbedingung ist erfüllt, da $\tilde{q}-1$ ungerade.

  Ersetzen von $\tilde{q}-1$ durch $\tilde{q}^2-1$ liefert die gesuchte Aussage für den zweiten der genannten Faktoren.

- Polynomdivision von $\tilde{q}^{2s}+1$ durch $\tilde{q}^2+\tilde{q}+1$ liefert für $s \equiv 0 \pmod 3$ den Rest 2, für $s \equiv 1 \pmod 3$ den Rest $-\tilde{q}$ und für $s \equiv 2 \pmod 3$ den Rest $\tilde{q}+1$. Da dieser stets teilerfremd zum Divisor ist, folgt die Behauptung. □

3.2 Definition *Es bezeichne*

1. *Σ die von ς_q erzeugte zyklische Gruppe, wobei wir den Automorphismus ς_q von $\mathrm{Sz}(q)$ mit seiner nat. Fortsetzung auf ganz $\mathrm{GL}(4,q)$ identifizieren,*
2. *$\mathrm{Sz}(q)_{\max}$ die Menge aller Elemente von $\mathrm{Sz}(q)$, die zu keinem Element einer Unter-Suzuki-Gruppe $\mathrm{Sz}(\tilde{q}) \lneq \mathrm{Sz}(q)$ (mit $\tilde{q} = 2^t$ für einen Teiler t von n) konjugiert sind ($\mathrm{Sz}(q)_{\max} \subset \mathrm{Sz}(q)$ ist offensichtlich charakteristisch),*
3. *$\mathfrak{K}_{K(q)_{\max}}$ die Menge der Konjugiertenklassen von $\mathrm{Sz}(q)$, die einen nichtleeren Schnitt mit $K(q)_{\max} := K(q) \cap \mathrm{Sz}(q)_{\max}$ haben und*
4. *$\mathfrak{K}_{U_i(q)_{\max}}$ $(i = 1, 2)$ die Menge der Konjugiertenklassen von $\mathrm{Sz}(q)$, deren Schnitt mit $U_i(q)_{\max} := U_i(q) \cap \mathrm{Sz}(q)_{\max}$ nicht leer ist.*

3.3 Lemma *Die Gruppe Σ operiert halbregulär auf den Mengen $\mathfrak{K}_{K(q)_{\max}}$ und $\mathfrak{K}_{U_i(q)_{\max}}$ $(i = 1, 2)$.*

Beweis :

- Da sich Exponentiation und Anwendung von Automorphismen in der Reihenfolge vertauschen lassen, operiert Σ auf $K(q)$ wie $\mathrm{Aut}(K)$ auf $K\backslash\{0\}$, und damit auch auf $K(q)_{\max}$ wie $\mathrm{Aut}(K)$ auf $K_{\max}$. Weil $K(q)$ TI-Untergruppe von $\mathrm{Sz}(q)$ und $|\mathrm{N}_{\mathrm{Sz}(q)}(K(q)) : K(q)| = 2$ ist, liegen höchstens jeweils zwei Elemente von $K(q)_{\max} \subseteq K(q)\backslash\{1\}$ in jeder der betrachteten Konjugiertenklassen. Wegen $\kappa^T = \kappa^{-1}$ für $\kappa \in K(q)$ sind es jedoch auch mindestens zwei Elemente, und zwar jeweils Paare der Form (κ, κ^{-1}). Da die Menge der in $K(q)_{\max}$ liegenden Paare (κ, κ^{-1}) ein Blocksystem für die Operation von Σ auf $K(q)_{\max}$ bildet und n ungerade ist, operiert Σ wie behauptet halbregulär auf $\mathfrak{K}_{K(q)_{\max}}$.

- Es sei $i \in \{1, 2\}$ und g ein Element von $U_i(q)_{\max}$. Wir zeigen zunächst, daß g als Element von $\mathrm{GL}(4, q)$ zu keinem Element einer Untergruppe $\mathrm{GL}(4, \tilde{q}) \lneq \mathrm{GL}(4, q)$ (mit $\tilde{q} = \sqrt[s]{q}$ für einen Teiler s von n) konjugiert ist. Da $U_i(q)$ als zyklische Gruppe nach Lemma 1.3 zu jedem Teiler t der Gruppenordnung genau eine Untergruppe der Ordnung t besitzt, ist die Ordnung von g sicher kein Teiler der Ordnung von $U_i(\tilde{q}) \lneq U_i(q)$, und wegen $\mathrm{ggT}(|U_1(q)|, |U_2(q)|) = 1$ und $|U_{3-i}(\tilde{q})| \mid |U_{3-i}(q)|$ auch keiner von $|U_1(\tilde{q})| \cdot |U_2(\tilde{q})| = \tilde{q}^2 + 1$. Wegen $|U_1(q)| \cdot |U_2(q)| = q^2 + 1$ ist $\mathrm{ord}(g)$ ein Teiler von $q^2 + 1$, nach Lemma 3.1 jedoch keiner der Ordnung von $\mathrm{GL}(4, \tilde{q})$. Daher ist g wie behauptet zu keinem Element von $\mathrm{GL}(4, \tilde{q})$ konjugiert, und die rationale Normalform von g enthält somit einen Eintrag aus $\mathrm{GF}(q)_{\max}$. Deren Bahn unter der Operation von Σ hat folglich offensichtlich die Länge n, und die Elemente dieser Bahn sind nach Lemma 2.2 alle ebenfalls in rationaler Normalform, liegen nach Definition derselbigen also in paarweise verschiedenen Konjugiertenklassen. Folglich operiert Σ wie behauptet ebenfalls halbregulär auf der Menge $\mathfrak{K}_{U_i(q)_{\max}}$. □

3.4 Hauptsatz *Es sei $m \in \mathbb{N}$, $n := 2m + 1$ und $q := 2^n$. Dann gilt :*

$$\omega(\mathrm{Sz}(q)) \;=\; \omega(\mathrm{PSL}(2, q)) + 2$$

Beweis : Aus argumentationstechnischen Gründen lassen wir die Konstruktion von $\mathrm{Sz}(q)$ auch für $q = 2$ zu (es ist dann $\mathrm{Sz}(2) \cong \langle (2\,4\,3\,5), (1\,2)(3\,4) \rangle$). Sei nun $q > 2$ und $g \in \mathrm{Sz}(q)_{\max}$. Dann ist g zu keinem seiner Bilder unter einer von der Identität verschiedenen Potenz des Automorphismus ς_q konjugiert ($g \sim \varsigma_q^k(g) \Rightarrow n|k$), denn die Konjugierten von $S(q)$, $K(q)$, $U_1(q)$ und $U_2(q)$ bilden eine Partition von $\mathrm{Sz}(q)$ in Untergruppen, $S(q) \cap \mathrm{Sz}(q)_{\max} = \varnothing$ und die Gruppe Σ operiert nach Lemma 3.3 halbregulär auf den Mengen $\mathfrak{K}_{K(q)_{\max}}$ und $\mathfrak{K}_{U_i(q)_{\max}}$ $(i = 1, 2)$. Weil die Menge der Elemente von Σ ein Repräsentantensystem für die Menge der Elemente von $\mathrm{Out}(\mathrm{Sz}(q)) = \mathrm{Aut}(\mathrm{Sz}(q))/\mathrm{Inn}(\mathrm{Sz}(q))$ bildet, fusionieren deshalb von den zu $\mathrm{Sz}(q)_{\max}$ gehörigen Konjugiertenklassen von $\mathrm{Sz}(q)$ unter der Operation von $\mathrm{Aut}(\mathrm{Sz}(q))$ jeweils n Stück. Zumal nun eine beliebige Unter-Suzuki-Gruppe $\mathrm{Sz}(\tilde{q}) \leq \mathrm{Sz}(q)$ insgesamt $\tilde{q} + 3$ Konjugiertenklassen besitzt, führt dies mit praktisch derselben Argumentation wie im Beweis

von Lemma 2.3 zu

$$\omega(\mathrm{Sz}(q)) = \frac{q+3}{n} + \sum_{\varnothing \neq M \subseteq \pi(n)} (-1)^{|M|} \left(\frac{2^{T_{n,M}}+3}{n} - \omega(\mathrm{Sz}(2^{T_{n,M}})) \right).$$

Da der Summand '$\frac{3}{n}$' nach Lemma 1.1 genauso oft addiert wie subtrahiert wird, erhalten wir wegen $\omega(\mathrm{Sz}(2)) = 5 = \omega(\mathrm{PSL}(2,2)) + 2$ (vgl. Bemerkung 3.6) durch Vergleich mit dem Resultat für $\mathrm{PSL}(2,q)$ in Satz 2.4 die Behauptung. □

3.5 Korollar *Über die Aussage des Hauptsatzes hinaus ergibt sich als unmittelbare Konsequenz aus dessen Beweis, daß die Bahnenzerlegungen der Mengen der zu keinem Element von* $\mathrm{Sz}(2)$ *bzw.* $\mathrm{PSL}(2,2)$ *konjugierten Elemente von* $\mathrm{Sz}(q)$ *bzw.* $\mathrm{PSL}(2,q)$ *auf die folgende Weise in bijektiver Korrespondenz zueinander stehen : bezeichnen wir mit* $\mathrm{PSL}(2,q)_{\max}$ *die Menge der zu keinem Element einer Untergruppe* $\mathrm{PSL}(2,\tilde{q}) \lneq \mathrm{PSL}(2,q)$ *konjugierten Elemente von* $\mathrm{PSL}(2,q)$*, so zerfällt* $\mathrm{Sz}(q)_{\max}$ *unter der Operation von* $\mathrm{Aut}(\mathrm{Sz}(q))$ *in genauso viele Bahnen wie* $\mathrm{PSL}(2,q)_{\max}$ *unter der von* $\mathrm{Aut}(\mathrm{PSL}(2,q))$*; dasselbe gilt damit natürlich auch für sämtliche Paare entsprechender Untergruppen über beliebigen Teilkörpern - dies wird in Abbildung 3.1 für* $q = 2^n$, $n = p_1^{k_1} p_2^{k_2}$ *(*p_1, p_2 *ungerade Primzahlen,* $k_1, k_2 \in \mathbb{N}$*) illustriert. Dort stehen die Felder für die jeweils gleichgroßen Mengen der Bahnen, in die die Mengen der zu Elementen der beiden angegebenen Mengen konjugierten Elemente unter der Operation von* $\mathrm{Aut}(\mathrm{Sz}(q))$ *bzw.* $\mathrm{Aut}(\mathrm{PSL}(2,q))$ *zerfallen. Die Beschränkung auf Exponenten mit höchstens zwei verschiedenen Primfaktoren ist willkürlich und lediglich durch die Dimension des Papiers bedingt.*

3.6 Bemerkung *Wir wollen die Bahnenzerlegungen der Gruppen* $\mathrm{Sz}(2)$ *und* $\mathrm{PSL}(2,2)$ *miteinander vergleichen.*

Der besseren Übersichtlichkeit halber verwenden wir die oben bereits genannte Permutationsdarstellung von $\mathrm{Sz}(2)$: ein Gruppenisomorphismus von $\mathrm{Sz}(2)$ auf $G := \langle (2\ 4\ 3\ 5), (1\ 2)(3\ 4) \rangle$ ist gegeben durch $f : M(1,1) \mapsto (2\ 4\ 3\ 5)$, $T \mapsto (1\ 2)(3\ 4)$. Die Gruppe G zerfällt unter der Operation ihrer Automorphismengruppe in folgende 5 Bahnen :

$$\{()\},$$
$$\{(2\ 3)(4\ 5), (1\ 2)(3\ 4), (1\ 3)(2\ 5), (1\ 4)(3\ 5), (1\ 5)(2\ 4)\},$$
$$\{(2\ 4\ 3\ 5), (1\ 2\ 5\ 4), (1\ 3\ 4\ 5), (1\ 4\ 2\ 3), (1\ 5\ 3\ 2)\},$$
$$\{(2\ 5\ 3\ 4), (1\ 2\ 3\ 5), (1\ 3\ 2\ 4), (1\ 4\ 5\ 2), (1\ 5\ 4\ 3)\},$$
$$\{(1\ 2\ 4\ 5\ 3), (1\ 3\ 5\ 4\ 2), (1\ 4\ 3\ 2\ 5), (1\ 5\ 2\ 3\ 4)\}.$$

Die Bahnenzerlegung der Gruppe $\mathrm{SL}(2,2) \cong \mathrm{PSL}(2,2) \cong \mathrm{S}_3$ ist

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

Wir sehen hieran, daß die jeweiligen Bahnen aus Elementen der Ordnungen 1 und 2 einander jeweils sozusagen 'direkt' entsprechen, daß die Bahn aus Elementen der Ordnung 5 in $\mathrm{Sz}(2)$ eine ähnliche Rolle spielt wie die aus Elementen der Ordnung 3 in $\mathrm{PSL}(2,2)$, und daß die beiden gewissermaßen 'überzähligen' Bahnen in $\mathrm{Sz}(2)$ diejenigen aus Elementen der Ordnung 4 sind.

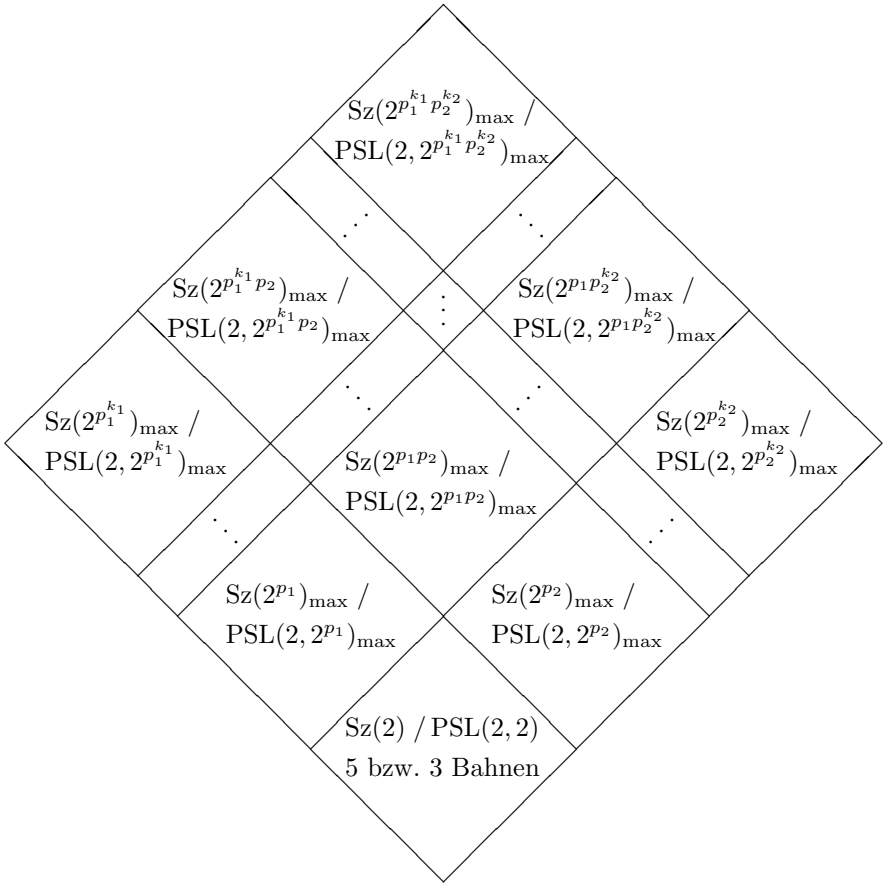

Abbildung 3.1: Bahnen von $\mathrm{Sz}(2^{p_1^{k_1}p_2^{k_2}})$ vs. Bahnen von $\mathrm{PSL}(2, 2^{p_1^{k_1}p_2^{k_2}})$

Anhang A

Tabellen

Für die Erstellung von Tabelle A.1 wurde auf die *Small Groups Library* von GAP zurückgegriffen, alle in den Tabellen A.2 - A.6 angegebenen Werte wurden mit Hilfe der in Anhang B aufgeführten GAP- Funktionen berechnet.

m $n \rightarrow$	1	2	3	4	5	6	7	8	9	10	11	12	Σ
p prim		1											1
p^2		1	1										2
$2p$			1	1									2
$3p, p \equiv 1(3)$				2									2
$3p, p \equiv 2(3)$				1									1
$4p, p \equiv 1(4)$				1	3	1							5
$4p, p \equiv 3(4)$, $p > 3$				1	2	1							4
8		1	1	3									5
12			1	1	2	1							5
16		1	1	2	6	4							14
18			1	2		2							5
24				1	3	2	4	5					15
27		1	1	2	1								5
30					1	2		1					4
32		1		6	4	12	10	8	10				51
35				1									1
36				2	4	3	2		1	2			14
40				1	1	1	4	7					14
42					1	2	1	2					6
45				1		1							2
48			1	2	1	2	3	8	8	13	7	7	52
50			1	2		2							5
54			1	1	3	3	1	3	1	2			15
55				1		1							2
56				2	1	1	4	5					13
60				1		1		2	3	5		1	13

Tabelle A.1: Anzahl der Gruppen G mit $|G| = m$ und $\omega(G) = n$

q	$\omega(\mathrm{PSL}(2,q))$	$\omega(\mathrm{SL}(2,q))$	$\omega(\mathrm{GL}(2,q))$
2	3	3	3
3	3	5	7
4	4	4	8
5	4	7	14
7	5	9	26
8	5	5	10
9	5	8	21
11	7	13	38
13	8	15	60
16	7	7	28
17	10	19	58
19	11	21	93
23	13	25	74
25	10	17	88
27	7	13	38
29	16	31	124
31	17	33	196
32	9	9	18
37	20	39	234
41	22	43	216
43	23	45	268
47	25	49	146
49	17	30	188
53	28	55	220
59	31	61	182
61	32	63	504
64	15	15	90
67	35	69	412
71	37	73	436
73	38	75	564
79	41	81	484
81	15	26	164
83	43	85	254
89	46	91	456
97	50	99	696
101	52	103	618
103	53	105	628
107	55	109	326
109	56	111	888
113	58	115	692
121	37	68	692
125	24	47	188
127	65	129	1158
128	21	21	42

Tabelle A.2: $\omega(\mathrm{PSL}(2,q))$, $\omega(\mathrm{SL}(2,q))$, $\omega(\mathrm{GL}(2,q))$

k	$\omega(\mathrm{PSL}(2,2^k))$
1	3
2	4
3	5
4	7
5	9
6	15
7	21
8	37
9	61
10	109
11	189
12	353
13	633
14	1183
15	2193
16	4117
17	7713
18	14603
19	27597
20	52489
21	99881
22	190747
23	364725
24	699253
25	1342185
26	2581429
27	4971069
28	9587581
29	18512793
30	35792569
31	69273669
32	134219797
33	260301177
34	505294129
35	981706833
36	1908881901
37	3714566313
38	7233642931
39	14096303345
40	27487816993

Tabelle A.3: $\omega(\mathrm{PSL}(2,2^k))$

k	$\omega(\mathrm{SL}(2,p^k))$
1	$p+2$
2	$\frac{1}{2}(p^2+p+4)$
3	$\frac{1}{3}(p^3+2p+6)$
4	$\frac{1}{4}(p^4+p^2+2p+8)$
5	$\frac{1}{5}(p^5+4p+10)$
6	$\frac{1}{6}(p^6+p^3+2p^2+2p+12)$
7	$\frac{1}{7}(p^7+6p+14)$
8	$\frac{1}{8}(p^8+p^4+2p^2+4p+16)$
9	$\frac{1}{9}(p^9+2p^3+6p+18)$
10	$\frac{1}{10}(p^{10}+p^5+4p^2+4p+20)$
11	$\frac{1}{11}(p^{11}+10p+22)$
12	$\frac{1}{12}(p^{12}+p^6+2p^4+2p^3+2p^2+4p+24)$
13	$\frac{1}{13}(p^{13}+12p+26)$
14	$\frac{1}{14}(p^{14}+p^7+6p^2+6p+28)$
15	$\frac{1}{15}(p^{15}+2p^5+4p^3+8p+30)$
16	$\frac{1}{16}(p^{16}+p^8+2p^4+4p^2+8p+32)$
17	$\frac{1}{17}(p^{17}+16p+34)$
18	$\frac{1}{18}(p^{18}+p^9+2p^6+2p^3+6p^2+6p+36)$
19	$\frac{1}{19}(p^{19}+18p+38)$
20	$\frac{1}{20}(p^{20}+p^{10}+2p^5+4p^4+4p^2+8p+40)$
21	$\frac{1}{21}(p^{21}+2p^7+6p^3+12p+42)$
22	$\frac{1}{22}(p^{22}+p^{11}+10p^2+10p+44)$
23	$\frac{1}{23}(p^{23}+22p+46)$
24	$\frac{1}{24}(p^{24}+p^{12}+2p^8+2p^6+2p^4+4p^3+4p^2+8p+48)$
25	$\frac{1}{25}(p^{25}+4p^5+20p+50)$
26	$\frac{1}{26}(p^{26}+p^{13}+12p^2+12p+52)$
27	$\frac{1}{27}(p^{27}+2p^9+6p^3+18p+54)$
28	$\frac{1}{28}(p^{28}+p^{14}+2p^7+6p^4+6p^2+12p+56)$
29	$\frac{1}{29}(p^{29}+28p+58)$
30	$\frac{1}{30}(p^{30}+p^{15}+2p^{10}+4p^6+2p^5+4p^3+8p^2+8p+60)$
31	$\frac{1}{31}(p^{31}+30p+62)$
32	$\frac{1}{32}(p^{32}+p^{16}+2p^8+4p^4+8p^2+16p+64)$
33	$\frac{1}{33}(p^{33}+2p^{11}+10p^3+20p+66)$
34	$\frac{1}{34}(p^{34}+p^{17}+16p^2+16p+68)$
35	$\frac{1}{35}(p^{35}+4p^7+6p^5+24p+70)$
36	$\frac{1}{36}(p^{36}+p^{18}+2p^{12}+2p^9+2p^6+6p^4+4p^3+6p^2+12p+72)$

Tabelle A.4: Polynome in $p \neq 2$ für $\omega(\mathrm{SL}(2,p^k))$, vgl. Korollar 2.6, Teil 3

k	$\omega(\mathrm{PSL}(2,p^k))$
1	$\frac{1}{2}(p+3)$
2	$\frac{1}{4}(p^2+2p+5)$
3	$\frac{1}{6}(p^3+2p+9)$
4	$\frac{1}{8}(p^4+2p^2+4p+9)$
5	$\frac{1}{10}(p^5+4p+15)$
6	$\frac{1}{12}(p^6+2p^3+2p^2+4p+15)$
7	$\frac{1}{14}(p^7+6p+21)$
8	$\frac{1}{16}(p^8+2p^4+4p^2+8p+17)$
9	$\frac{1}{18}(p^9+2p^3+6p+27)$
10	$\frac{1}{20}(p^{10}+2p^5+4p^2+8p+25)$
11	$\frac{1}{22}(p^{11}+10p+33)$
12	$\frac{1}{24}(p^{12}+2p^6+2p^4+4p^3+4p^2+8p+27)$
13	$\frac{1}{26}(p^{13}+12p+39)$
14	$\frac{1}{28}(p^{14}+2p^7+6p^2+12p+35)$
15	$\frac{1}{30}(p^{15}+2p^5+4p^3+8p+45)$
16	$\frac{1}{32}(p^{16}+2p^8+4p^4+8p^2+16p+33)$
17	$\frac{1}{34}(p^{17}+16p+51)$
18	$\frac{1}{36}(p^{18}+2p^9+2p^6+4p^3+6p^2+12p+45)$
19	$\frac{1}{38}(p^{19}+18p+57)$
20	$\frac{1}{40}(p^{20}+2p^{10}+4p^5+4p^4+8p^2+16p+45)$
21	$\frac{1}{42}(p^{21}+2p^7+6p^3+12p+63)$
22	$\frac{1}{44}(p^{22}+2p^{11}+10p^2+20p+55)$
23	$\frac{1}{46}(p^{23}+22p+69)$
24	$\frac{1}{48}(p^{24}+2p^{12}+2p^8+4p^6+4p^4+8p^3+8p^2+16p+51)$
25	$\frac{1}{50}(p^{25}+4p^5+20p+75)$
26	$\frac{1}{52}(p^{26}+2p^{13}+12p^2+24p+65)$
27	$\frac{1}{54}(p^{27}+2p^9+6p^3+18p+81)$
28	$\frac{1}{56}(p^{28}+2p^{14}+4p^7+6p^4+12p^2+24p+63)$
29	$\frac{1}{58}(p^{29}+28p+87)$
30	$\frac{1}{60}(p^{30}+2p^{15}+2p^{10}+4p^6+4p^5+8p^3+8p^2+16p+75)$
31	$\frac{1}{62}(p^{31}+30p+93)$
32	$\frac{1}{64}(p^{32}+2p^{16}+4p^8+8p^4+16p^2+32p+65)$
33	$\frac{1}{66}(p^{33}+2p^{11}+10p^3+20p+99)$
34	$\frac{1}{68}(p^{34}+2p^{17}+16p^2+32p+85)$
35	$\frac{1}{70}(p^{35}+4p^7+6p^5+24p+105)$
36	$\frac{1}{72}(p^{36}+2p^{18}+2p^{12}+4p^9+4p^6+6p^4+8p^3+12p^2+24p+81)$

Tabelle A.5: Polynome in $p \neq 2$ für $\omega(\mathrm{PSL}(2,p^k))$, vgl. Korollar 2.6, Teil 3

m	$\omega(\mathrm{Sz}(2^{2m+1}))$
1	7
2	11
3	23
4	63
5	191
6	635
7	2195
8	7715
9	27599
10	99883
11	364727
12	1342187
13	4971071
14	18512795
15	69273671
16	260301179
17	981706835
18	3714566315
19	14096303347
20	53634713555
21	204560302847
22	781874936819
23	2994414645863
24	11488774559639
25	44152937528387
26	169947155749835
27	655069036708595
28	2528336632928155
29	9770521225481759
30	37800705069076955
31	146402730743793243
32	567592125344909795
33	2202596307308603183
34	8555011744329310571
35	33256101992039755031
36	129379903640264252435
37	503719091506096386003
38	1962541914958813595483
39	7651429238067273257639
40	2985002023739825454137 5

Tabelle A.6: $\omega(\mathrm{Sz}(2^{2m+1}))$

Anhang B

GAP - Funktionen

Gegenstand dieses Anhangs sind Routinen zur Berechnung von $\omega(G)$ für die im Rahmen dieser Arbeit behandelten Typen von Gruppen G. Diese sind in der GAP-Programmiersprache (siehe [GAP99]) geschrieben und dienten zur Berechnung sämtlicher in den Tabellen A.2, A.3, A.4, A.5 und A.6 angegebenen Werte. Bis auf die Funktion zur Berechnung von $\omega(\mathrm{GL}(2,q))$ für eine beliebige Primzahlpotenz q handelt es sich lediglich um Routinen zur Auswertung der in den jeweils angegebenen Sätzen vorkommenden Formelausdrücke. Aus Gründen der Platzersparnis werden rein programmiertechnische Details wie etwa die Überprüfung der Gültigkeit der Parameter etc. fortgelassen, auch wird aus naheliegenden Gründen (vgl. Hauptsatz 3.4) auf die separate Angabe eines Programmstücks zur Berechnung von $\omega(\mathrm{Sz}(q))$ verzichtet.

1. Hilfsfunktionen

   (a) `T(k,M)` ... Berechnung von $T_{k,M}$ (siehe Lemma 2.3)

   ```
   T := function (k,M) return Gcd(List(M,t->k/t)); end;
   ```

   (b) `FactorSets(k)` ... Nichtleere Mengen von Primfaktoren von $k \in \mathbb{N}$

   ```
   FactorSets :=
     k -> Difference(Combinations(Set(Factors(k))),
                     [[],[1]]);
   ```

   (c) `OddFactorSets(k)` ... Nichtleere Mengen ungerader Primfaktoren von $k \in \mathbb{N}$

   ```
   OddFactorSets :=
     k -> Difference(Combinations
                     (Difference(Set(Factors(k)),[2])),
                     [[],[1]]);
   ```

2. `OmegaSL2(q)` ... Berechnung von $\omega(\mathrm{SL}(2,q))$ für eine Primzahlpotenz q
(vgl. Satz 2.4, Tabelle A.2)

```
OmegaSL2 := function (q)

  local  p,k;

  p := SmallestRootInt(q); k := LogInt(q,p);
  if   k = 1
  then if p = 2 then return 3; else return p + 2; fi;
  else return q/k + Sum(FactorSets(k),
                        M -> (-1)^Length(M)
                           * (  p^T(k,M)/k
                              - OmegaSL2(p^T(k,M))));
  fi;
end;
```

3. `OmegaSL2Polynomial(k)` ... Berechnung eines Polynoms in $p \neq 2$
für $\omega(\mathrm{SL}(2,p^k))$, $k \in \mathbb{N}$
(vgl. Korollar 2.6, Tabelle A.4)

```
OmegaSL2Polynomial := function (k)

  local  p;

  p := Indeterminate(Integers); SetName(p,"p");
  if   k = 1 then return p + 2;
  else return p^k/k
            + Sum(FactorSets(k),
                  M -> (-1)^Length(M)
                     * (  p^T(k,M)/k
                        - OmegaSL2Polynomial(T(k,M))));
  fi;
end;
```

4. `OmegaPSL2(q)` ... Berechnung von $\omega(\mathrm{PSL}(2,q))$ für eine Primzahlpotenz q (vgl. Satz 2.4, Tabellen A.2, A.3 und A.6)

```
OmegaPSL2 := function (q)

  local  p,k,Halfs;

  p := SmallestRootInt(q); k := LogInt(q,p);
  if   q = 2 then return 3;
  elif k = 1 then return (p + 3)/2;
  else if   p = 2 then return OmegaSL2(q);
       elif k mod 2 = 1 then Halfs := 0;
       elif SmallestRootInt(k) = 2 then Halfs := p^(k/2)-1;
       else Halfs := p^(k/2)
                   + Sum(OddFactorSets(k),
                         M -> (-1)^Length(M)
                            * p^Gcd(List(M,t->k/(2*t))));
       fi;
       return Sum(FactorSets(k),
                  M -> (-1)^Length(M) * (p^T(k,M)/(2*k)
                         - OmegaPSL2(p^T(k,M))))
            + (q + Halfs)/(2*k);
  fi;
end;
```

5. `OmegaPSL2Polynomial(k)` ... Berechnung eines Polynoms in $p \neq 2$ für $\omega(\mathrm{PSL}(2,p^k))$, $k \in \mathbb{N}$ (vgl. Korollar 2.6, Tabelle A.5)

```
OmegaPSL2Polynomial := function (k)

  local  p,Halfs;

  p := Indeterminate(Integers); SetName(p,"p");
  if   k = 1 then return (p + 3)/2;
  else if   k mod 2 = 1 then Halfs := 0;
       elif SmallestRootInt(k) = 2 then Halfs := p^(k/2)-1;
       else Halfs := p^(k/2)
                   + Sum(OddFactorSets(k),
                         M -> (-1)^Length(M)
                            * p^Gcd(List(M,t->k/(2*t))));
       fi;
       return Sum(FactorSets(k),
                  M -> (-1)^Length(M) * (p^T(k,M)/(2*k)
                         - OmegaPSL2Polynomial(T(k,M))))
            + (p^k + Halfs)/(2*k);
  fi;
end;
```

6. `OmegaGL2p(p)` ... Berechnung von $\omega(\mathrm{GL}(2,p))$ für eine Primzahl $p \neq 2$ (vgl. Satz 2.10, Tabelle A.2)

```
OmegaGL2p := p ->  (p + 1)   * Tau(p - 1)
                 - (p - 1)/2 * Tau((p - 1)/2);
```

7. `OmegaGL2(q)` ... Berechnung von $\omega(\mathrm{GL}(2,q))$ für eine Primzahlpotenz q (da ich für den allgemeinen Fall keine geschlossene Formel gefunden habe, werden die Bahnen von $\mathfrak{K}$ ($\rightarrow$ Beweis von Satz 2.10) einzeln durchlaufen und abgezählt) (vgl. Tabelle A.2)

```
OmegaGL2 := function (q)

  local  AutomorphismClosure,p,k,K,f,lValues,M,M_ab,M_abs;

  AutomorphismClosure := function (m_ab)

    local  Closure,OldLength,Pos,a,b,l,
           GFAutImage,PsilImage;

    Closure := [m_ab];
    repeat OldLength := Length(Closure);
           for Pos in [1..Length(Closure)] do
             a := Closure[Pos][2]; b := Closure[Pos][1];
             GFAutImage := [Image(f,b),Image(f,a)];
             AddSet(Closure,GFAutImage);
             for l in lValues do
               PsilImage := [b^(2*l + 1), a*b^l];
               AddSet(Closure,PsilImage);
             od;
           od;
    until Length(Closure) = OldLength;
    return Closure;
  end;

  p := SmallestRootInt(q); k := LogInt(q,p);
  K := GF(q); f := FrobeniusAutomorphism(K);
  lValues := Filtered([1..q-1],l -> Gcd(2*l + 1,q - 1) = 1);
  M := Cartesian(Difference(AsList(K),[Zero(K)]),AsList(K));
  M_abs := [];
  repeat M_ab := AutomorphismClosure(M[1]);
         Add(M_abs,M_ab); M := Difference(M,M_ab);
  until M = [];
  return Length(M_abs) + Tau(q - 1);
end;
```

Anhang C

Symbolverzeichnis

$\mathbb{N}$	Menge der natürlichen Zahlen (ohne Null)
$\mathbb{Z}$	Menge der ganzen Zahlen
p	Primzahl
q	Primzahlpotenz
$l\|k$	'l teilt k'
$\pi(k)$	Menge der Primteiler von k
φ	Eulersche φ - Funktion
τ	Teileranzahlfunktion
ggT	Größter gemeinsamer Teiler
kgV	Kleinstes gemeinsames Vielfaches
$\delta_{i,j}$	Kronecker - δ
$\log_b(n)$	Logarithmus zur Basis b von n
$M, \|M\|$	Menge, Kardinalität von M
A^t	Transponierte der Matrix A
$\chi(A)$	Charakteristisches Polynom von A
$\mu(A)$	Minimalpolynom von A
K	Körper
$K[x]$	Polynomring in einer Variablen über K
GF(q)	Körper mit q Elementen
GF(q)*	Multiplikative Gruppe von GF(q)
ord(a)	Ordnung von $a \in$ GF(q)$\backslash\{0\}$ als Element von GF(q)*
GF(q)$_{\max}$	Menge der in keinem echten Teilkörper von GF(q) liegenden Elemente
α	Körperautomorphismus
σ, σ_{frob}	Frobenius - Automorphismus
Aut(K)	Automorphismengruppe von K
$\omega(K)$	Anzahl der Bahnen von K unter der Operation von Aut(K)
G	Gruppe
$\|G\|$	Gruppenordnung von G
ord(g)	Ordnung des Gruppenelements g
$g \sim h$	'g und h sind zueinander konjugiert'
$\langle g_1, \ldots, g_n \rangle$	Von $g_1, \ldots, g_n$ erzeugte Gruppe
Z(G)	Zentrum von G
C$_G(H)$	Zentralisator von H in G

$\mathrm{N}_G(H)$	Normalisator von H in G
$H \trianglelefteq G$	'H ist Normalteiler von G'
$\|G : H\|$	Index von H in G
$\mathrm{Aut}(G)$	Automorphismengruppe von G
$\mathrm{Inn}(G)$	Innere Automorphismengruppe von G
$\mathrm{Out}(G)$	Äußere Automorphismengruppe von G
$\omega(G)$	Anzahl der Bahnen von G unter der Operation von $\mathrm{Aut}(G)$
G_x	Stabilisator des Punktes x unter der Operation von G
$G_{\{M\}}$	(Mengenweiser) Stabilisator von M unter der Operation von G
$G \rtimes H$	Semidirektes Produkt der Gruppen G und H (G ist normal)
C_n	Zyklische Gruppe der Ordnung n
S_n	Symmetrische Gruppe vom Grad n
A_n	Alternierende Gruppe vom Grad n
σ_l	Siehe Lemma 1.3
$\mathrm{SL}(n,q)$	Spezielle lineare Gruppe vom Grad n über $\mathrm{GF}(q)$
$\mathrm{PSL}(n,q)$	Projektive spezielle lineare Gruppe vom Grad n über $\mathrm{GF}(q)$
$\mathrm{GL}(n,q)$	Allgemeine lineare Gruppe vom Grad n über $\mathrm{GF}(q)$
$\mathrm{PGL}(n,q)$	Projektive allgemeine lineare Gruppe vom Grad n über $\mathrm{GF}(q)$
$\Gamma\mathrm{L}(n,q)$	Allgemeine semilineare Gruppe vom Grad n über $\mathrm{GF}(q)$
$\mathrm{P}\Gamma\mathrm{L}(n,q)$	Projektive semilineare Gruppe vom Grad n über $\mathrm{GF}(q)$
$\mathrm{AGL}(n,q)$	Affine allgemeine lineare Gruppe vom Grad n über $\mathrm{GF}(q)$
κ	Kanonische Projektion von $\mathrm{SL}(n,q)$ auf $\mathrm{PSL}(n,q)$ bzw. von $\mathrm{GL}(n,q)$ auf $\mathrm{PGL}(n,q)$ (verwendet in anderer Bedeutung im Zusammenhang mit den Suzuki-Gruppen, siehe Lemma 1.8)
ϕ, ψ_l, Ψ	Siehe Lemma 1.7
$T_{k,M}$	Siehe Lemma 2.3
$H(p,k)$	Siehe Satz 2.4
$\mathfrak{K}$,	
$\mathfrak{K}_a, \mathfrak{K}_d$	Siehe Lemma 2.1 sowie die Beweise der Sätze 2.4, 2.7 und 2.10
$\mathfrak{R}$	Siehe Beweise der Sätza 2.4 und 2.10
$\mathfrak{B}$	Siehe Beweis von Satz 2.10
$M(a,b)$	In versch. Bed. verwendet in Lemma 1.8 und Satz 2.10
$\mathrm{Sz}(q)$	Suzuki - Gruppe
$S(q)$	2 - Sylowgruppe von $\mathrm{Sz}(q)$
$K(q)$,	
$H(q)$,	
$U_i(q)$	Siehe Lemma 1.8
ς_q	Von $\sigma_{frob}(K)$ induzierter Automorphismus von $\mathrm{Sz}(q)$
Σ	Von ς_q erzeugte zyklische Gruppe
$\mathbb{P}(n,q)$	n - dimensionaler projektiver Raum über $\mathrm{GF}(q)$
$p(x,y)$	Siehe Lemma 1.8
$\mathcal{O}$	Tits'sches Ovoid
$\mathrm{Sz}(q)_{\max}$,	
$K(q)_{\max}$,	
$U_i(q)_{\max}$,	
$\mathfrak{K}_{K(q)_{\max}}$,	
$\mathfrak{K}_{U_i(q)_{\max}}$	Siehe Definition 3.2
$\mathrm{PSL}(2,q)_{\max}$	Siehe Korollar 3.5

Literaturverzeichnis

[Die51] Jean Dieudonne. On the automorphisms of the classical groups. *Memoirs of the American Mathematical Society*, 2, 1951.

[Die63] Jean Dieudonne. La geometrie des groupes classiques. *Ergebnisse der Mathematik und ihrer Grenzgebiete*, 5, 1963.

[GAP99] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.1*, 1999. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[HB82] Bertram Huppert and Norman Blackburn. *Finite Groups III*. Band 243 der *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1982.

[Hup67] Bertram Huppert. *Endliche Gruppen I*. Band 134 der *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1967.

[Jun93] Dieter Jungnickel. *Finite Fields*. BI - Wissenschaftsverlag, 1993.

[Lün80] Heinz Lüneburg. *Translation Planes*. Springer-Verlag, 1980.

[Lün87] Heinz Lüneburg. *On the Rational Normal Form of Endomorphisms*. BI - Wissenschaftsverlag, 1987.

[MS97] Helmut Mäurer and Markus Stroppel. Groups that are almost homogeneous. *Geometriae Dedicata*, 68:229–243, 1997.

[Str99] Markus Stroppel. Finite simple groups with few orbits under automorphisms. Preprint, 1999.

[Suz62] Michio Suzuki. On a class of doubly transitive groups. *Annals of Mathematics*, 75:105–145, 1962.

[Tho68] John G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.

Hiermit erkläre ich, daß ich diese Arbeit selbständig angefertigt und keine anderen als die angegebenen Hilfsmittel verwendet habe.

Stuttgart, im Januar 2000