Engelbedingungen für nilpotente und auflösbare Gruppen

I n a u g u r a l - D i s s e r t a t i o n

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

vorgelegt von

Evija Ribnere

aus Jelgava

15. Februar 2007

Aus dem Mathematischen Institut
der Heinrich-Heine-Universität Düsseldorf

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

Referent: Prof. Dr. F. Grunewald

Koreferent: Prof. Dr. S. Schröer

Tag der mündlichen Prüfung: 25.01.2007

Engelbedingungen für nilpotente und auflösbare Gruppen

Auflösbarkeitskriterien in zwei Variablen für endliche Gruppen (Kapitel 1–5)

Eine endliche Gruppe G heißt nilpotent, wenn eine natürliche Zahl n existiert, so dass $[[[x_0, x_1], x_2], \ldots, x_n] = 1$ für alle $x_0, x_1, \ldots, x_n \in G$ gilt, wobei $[x, y] := x^{-1}y^{-1}xy$ den Kommutator bezeichnet.

Zorn zeigte im Jahr 1963, dass die Nilpotenz einer endlichen Gruppe durch eine Kommutatorgleichung in nur zwei Variablen verifiziert werden kann: Eine endliche Gruppe G ist genau dann nilpotent, wenn für ein $n \in \mathbb{N}$ und alle $x, y \in G$ die Engelbedingung $e_n(x, y) = 1$ erfüllt ist. Dabei wird $e_n(x, y)$ induktiv definiert durch $e_1(x, y) = [x, y]$ und $e_n(x, y) = [e_{n-1}(x, y), y]$.

Ähnlich wie die Nilpotenz, wird die Auflösbarkeit einer Gruppe mittels einer Kommutatorgleichung in mehreren Variablen definiert. Es war lange Zeit offen, ob die Auflösbarkeit einer endlichen Gruppe auch durch Ausdrücke in nur zwei Variablen charakterisierbar ist. Im Jahr 2003 fanden Grunewald et al. solche: Eine endliche Gruppe G ist genau dann auflösbar, wenn für ein $n \in \mathbb{N}$ und alle $x, y \in G$ gilt $u_n(x, y) = 1$. Dabei ist $u_1(x, y) = x^{-2}y^{-1}x$ und $u_n(x, y) = [u_{n-1}(x, y)^{x^{-1}}, u_{n-1}(x, y)^{y^{-1}}]$, wobei a^b für $a^{-1}ba$ steht.

Bray, Wilson und Wilson bewiesen im Jahr 2005 die gleiche Aussage für eine andere Sequenz, die sie durch $s_1(x, y) = x$ und $s_n(x, y) = [s_{n-1}(x, y)^{-y}, s_{n-1}(x, y)]$ definierten.

In dieser Arbeit wird ein solcher Satz für sechs weitere Sequenzen bewiesen. Diese sind von der folgenden Gestalt: Man definiert $v_1(x, y) := f(x, y)$ und $v_n(x, y) := [v_{n-1}(x, y)^{g(x,y)}, v_{n-1}(x, y)^{h(x,y)}]$ für feste Ausdrücke $f(x, y), g(x, y), h(x, y)$ in x und y. Ein Beispiel ist: $f(x, y) = yx^2$, $g(x, y) = y^{-1}x^{-1}$ und $h(x, y) = x^{-1}$.

Nilpotenzklasse einer Engel Gruppe (Kapitel 6)

Eine Gruppe heißt n–Engel Gruppe, wenn sie die Engelbedingung $e_n(x, y) = 1$ erfüllt. Nach dem Satz von Zorn sind endliche n–Engel Gruppen nilpotent. Das kleinste n, für das $[[[x_0, x_1], x_2], \ldots, x_n] = 1$ gilt, heißt die Nilpotenzklasse von G und das kleinste n, für das $e_n(x, y) = [[[x, y], y], \ldots, y] = 1$ erfüllt ist, die Engel Länge.

Offensichtlich ist jede nilpotente Gruppe von der Nilpotenzklasse n eine n–Engel Gruppe. Es stellt sich die Frage, ob man die Nilpotenzklasse einer n–Engel Gruppe nach oben abschätzen kann.

Für $n \leqslant 4$ ist die Antwort bekannt. 1–Engel Gruppen sind genau die abelschen Gruppen. Levi zeigte 1942, dass 2–Engel Gruppen höchstens von der Nilpotenzklasse 3 sind. Heinecken bewies im Jahr 1961, dass 3–Engel Gruppen von der Nilpotenzklasse 4 sind, wenn sie keine Elemente der Ordnungen 2 und 5 enthalten. 4–Engel Gruppen sind höchstens von der Nilpotenzklasse 7, wenn sie keine Elemente der Ordnungen 2, 3 und 5 enthalten (Traustason, Havas, Vaughan–Lee, 2005). Es gibt bisher keine ähnliche Aussagen über höhere Engel Gruppen. Es ist bekannt, dass die Einschränkungen an die Ordnung der Elemente notwendig sind.

Im Kapitel 6 wird gezeigt: Für jede Primzahl $p < n$ gibt es n–Engel p–Gruppen von beliebig großer Nilpotenzklasse – anders ausgedrückt, für jede Abschätzung der Nilpotenzklasse einer n–Engel Gruppe müssen die Elemente der Ordnungen $p < n$ ausgeschlossen werden.

Engel–identities for nilpotent and solvable groups

solvability conditions in two variables for finite groups (chapter 1–5)

A group G is nilpotent by definition if for some $n \in \mathbb{N}$ and all $x_0, x_1, \ldots, x_n \in G$ the identity $[[[x_0, x_1], x_2], \ldots, x_n] = 1$ holds, the bracket stands for the commutator $[x, y] := x^{-1}y^{-1}xy$.

In 1963 Zorn showed the nilpotency of a finite group can be expressed by an identity involving only two variables: A finite group G is nilpotent if and only if it satisfies for some $n \in \mathbb{N}$ and all $x, y \in G$ the Engel–identity $e_n(x, y) = 1$. Here $e_1(x, y) = [x, y]$ and $e_n(x, y)$ is inductively defined by $e_n(x, y) = [e_{n-1}(x, y), y]$.

Similarly, the usual definition of solvability involves many variables. For a long time it was a open question whether solvability can be described by an identity in only two variables as well. In 2003 Grunewald et al. found such sequence: A finite group G is solvable if and only if it satisfies the identity $u_n(x, y) = 1$ for some $n \in \mathbb{N}$ and all $x, y \in G$. Here $u_n(x, y)$ is defined by $u_1(x, y) = x^{-2}y^{-1}x$ and $u_n(x, y) = [u_{n-1}(x, y)^{x^{-1}}, u_{n-1}(x, y)^{y^{-1}}]$, where we write a^b for $a^{-1}ba$.

Bray, Wilson, and Wilson showed in 2005 a similar result for another sequence, namely $s_1(x, y) = x$ and $s_n(x, y) = [s_{n-1}(x, y)^{-y}, s_{n-1}(x, y)]$.

In this thesis we prove the theorem for six further sequences. Each of these sequences is of the following form: We start with a special expression for $v_1(x, y) := f(x, y)$ and then define inductively $v_n(x, y) := [v_{n-1}(x, y)^{g(x,y)}, v_{n-1}(x, y)^{h(x,y)}]$, where $f(x, y), g(x, y), h(x, y)$ are expressions in x and y. One example is $f(x, y) = yx^2$, $g(x, y) = y^{-1}x^{-1}$, and $h(x, y) = x^{-1}$.

nilpotency class vs. Engel–length (chapter 6)

We call G an n–Engel group, if the Engel–identity $e_n(x, y) = 1$ holds in G. By Zorn's Theorem finite n–Engel groups are nilpotent. Further, we call the minimal n with $[[[x_0, x_1], x_2], \ldots, x_n] = 1$ the nilpotency class, and the minimal n with $e_n(x, y) = [[[x, y], y], \ldots, y] = 1$ the Engel length of G.

Obviously, every nilpotent group of class n is an n–Engel group. Therefore, one asks: What can be said about the nilpotency class of an n–Engel group?

For $n \leqslant 4$ the answer is known. 1–Engel groups are precisely the abelian groups. Levi showed in 1942 that 2–Engel groups are nilpotent of class at most 3. Heinecken proved in 1961 that a 3–Engel group is nilpotent of class at most 4 assuming that it has no elements of order 2 or 5. 4–Engel groups are nilpotent of class at most 7 if they have no elements of order 2, 3 or 5 (Traustason, Havas, Vaughan–Lee, 2005). There is no similar result for higher Engel groups. It is known that in the above theorems the assumptions on the order of the elements are necessary.

In Chapter 6 we will show: For any prime $p < n$ there exists an n–Engel p–group with arbitrary large nilpotency class – in other words, any bound on the nilpotency class for an n–Engel group must exclude groups with elements of order p for all primes $p < n$.

Inhaltsverzeichnis

Einleitung

Sei G eine Gruppe und $1 \in G$ das neutrale Element. Für $x, y \in G$ sei

$$[x, y] := x^{-1}y^{-1}xy$$

der *Kommutator* von x und y. Seien weiter

$$[x_1, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n] \text{ und } x^y := y^{-1}xy.$$

Für G definieren wir zwei Ketten von Normalteilern

$$\begin{array}{ccccccccccc} G = G^0 & \trianglerighteq & G^1 & \trianglerighteq & G^2 & \trianglerighteq & \ldots & \trianglerighteq & G^i & \trianglerighteq & \ldots \\ G = G^{(0)} & \trianglerighteq & G^{(1)} & \trianglerighteq & G^{(2)} & \trianglerighteq & \ldots & \trianglerighteq & G^{(i)} & \trianglerighteq & \ldots \end{array}$$

durch

$$\begin{array}{lllll} G^i & := & [G^{i-1}, G] & = & \langle\, [x, y] \mid x \in G^{i-1}, y \in G \rangle \qquad \text{und} \\ G^{(i)} & := & [G^{(i-1)}, G^{(i-1)}] & = & \langle\, [x, y] \mid x \in G^{(i-1)}, y \in G^{(i-1)} \rangle. \end{array}$$

Die Gruppe $G^1 = G^{(1)} = \langle\, [x, y] \mid x, y \in G \rangle$ heißt die *Kommutatoruntergruppe* von G. Gilt $G^1 = \langle 1 \rangle$, so heißt G *kommutativ.*

Eine Gruppe G heißt *nilpotent,* falls ein $k \in \mathbb{N}$ existiert, so dass $G^k = \langle 1 \rangle$. Die kleinste natürliche Zahl k, die das erfüllt, heißt die *Nilpotenzklasse* von G. Eine Gruppe G heißt *auflösbar,* falls ein $k \in \mathbb{N}$ existiert, so dass $G^{(k)} = \langle 1 \rangle$. Die kleinste natürliche Zahl k mit dieser Eigenschaft heißt die *Auflösungslänge* von G.

Aus dieser Definition folgt, dass eine Gruppe G genau dann nilpotent ist, wenn ein $k \in \mathbb{N}$ existiert, so dass $[\, x_0, x_1, \ldots, x_k \,] = 1$ für alle $x_0, x_1, \ldots, x_k \in G$ gilt. Das bedeutet, dass man die Nilpotenz von G mit einer Gleichung in $k+1$ Variablen beschreiben kann. Analog wird für die Beschreibung der Auflösbarkeit eine Gleichung in 2^k Variablen benötigt.

Für endliche Gruppen ist es möglich, die Nilpotenz und die Auflösbarkeit mit einer Kommutatorgleichung in nur zwei Variablen zu beschreiben.

Dieses Problem wurde in Vergangenheit von zahlreichen Autoren untersucht. Der Ausgangspunkt dieser Theorie ist der folgende Satz von Zorn.

Satz 0.1. *[Z63] G sei eine endliche Gruppe und die Sequenz $e = (e_1, e_2, \dots)$ für feste $x, y \in G$ definiert durch*

$$e_1 = [x, y] \quad \textit{und} \quad e_n = [e_{n-1}, y].$$

Dann gilt: G ist nilpotent $\Leftrightarrow$ es gibt ein $k \in \mathbb{N}$ mit $e_k(x, y) = 1$ für alle $x, y \in G$.

Die ersten Folgenglieder von e:

$$\begin{aligned} e_1 = \ & [x, y] && = x^{-1}y^{-1}xy, \\ e_2 = \ & [x, y, y] && = y^{-1}x^{-1}yxy^{-1}x^{-1}y^{-1}xy^2, \\ e_3 = \ & [x, y, y, y] && = y^{-2}x^{-1}yxyx^{-1}y^{-1}xy^{-1}x^{-1}yxy^{-1}x^{-1}y^{-1}xy^3. \end{aligned}$$

Wir schreiben e_i, wenn es als Wort in x und y gemeint ist, und $e_i(x, y)$, wenn feste x und y aus einer endlichen Gruppe G eingesetzt werden.

Die Bedingung $e_k(x, y) = 1$ nennt man *Engelbedingung* nach dem deutschen Mathematiker Friedrich Engel, der die zum Satz von Zorn analoge Aussage für Lie–Algebren bewies.

Für nilpotente Gruppen ist eine Verallgemeinerung des Satzes von Zorn bekannt:

Satz 0.2. *[H67, III.6.1.] G sei eine endliche Gruppe. Seien $k \in \mathbb{N}$, $i_j \in \{1, \dots, k\}$ mit $i_1 \neq i_2$. Dann gilt: G ist nilpotent, wenn $[x_{i_1}, x_{i_2}, \dots, x_{i_k}] = 1$ für alle $x_i \in G$.*

Der Satz besagt auch, dass zum Beispiel die Bedingungen $[x, y, y] = 1$ oder $[x, y, x, y] = 1$ die Nilpotenz erzwingen. Man kann fast beliebige nichttriviale Sequenzen als Kommutatorgleichungen in zwei Variablen bilden, um die Nilpotenz einer endlichen Gruppe nachzuweisen. Insbesondere gibt es unendlich viele Sequenzen mit dieser Eigenschaft.

Grunewald et al. haben im Jahr 2003 gezeigt, dass eine Sequenz existiert, die eine analoge Aussage für endliche auflösbare Gruppen beweist:

Satz 0.3 ($\mathbf{u_n}$–Satz). *[BGGKPP] G sei eine endliche Gruppe und die Sequenz $u = (u_1, u_2, \dots)$ definiert durch*

$$u_1 = x^{-2}y^{-1}x \quad \textit{und} \quad u_n = [u_{n-1}^{x^{-1}}, u_{n-1}^{y^{-1}}].$$

Dann gilt: G ist auflösbar $\Leftrightarrow$ es gibt ein $k \in \mathbb{N}$ mit $u_k(x, y) = 1$ für alle $x, y \in G$.[1]

[1] In diesem Satz ist $[x, y] := xyx^{-1}y^{-1}$.

Für eine weitere Sequenz haben Bray, Wilson und Wilson im Jahr 2005 die analoge Aussage gezeigt:

Satz 0.4 ($\mathbf{s_n}$–Satz). *[BWW05] G sei eine endliche Gruppe und die Sequenz $s = (s_1, s_2, \dots)$ definiert durch*

$$s_1 = x \quad \textit{und} \quad s_n = [s_{n-1}^{-y}, s_{n-1}].$$

Dann gilt: G ist auflösbar $\Leftrightarrow$ es gibt ein $k \in \mathbb{N}$ mit $s_k(x, y) = 1$ für alle $x, y \in G$.

Die u_n- und s_n-Sätze beweisen die gleiche Aussage für verschiedene Sequenzen. Bis jetzt sind diese zwei die einzigen bekannten Sequenzen, die eine solche Aussage erfüllen.

Die Beweise der beiden Sätze sind von sehr unterschiedlicher Natur. Der Beweis zu dem s_n– Satz benutzt gruppentheorethische Methoden, ist aber nur für diese eine Sequenz konstruiert worden und nicht für weitere Sequenzen anwendbar. Der Beweis zu dem u_n–Satz benutzt Methoden aus der algebraischen Geometrie und ist teilweise für andere Sequenzen erweiterbar.

Es stellte sich die Frage: Für welche weitere Sequenzen ist eine zu den u_n- und s_n– Sätzen analoge Aussage möglich?

Wir geben eine neue Definition der Sequenzen für auflösbare Gruppen an:

Definition 0.5. Sei $F = \langle x, y \rangle$ die freie Gruppe mit zwei Erzeugenden und $f, g, h \in F$. Die Sequenz $v = (v_1, v_2, \dots)$ sei definiert durch

$$v_1 := f \quad \text{und} \quad v_n := [v_{n-1}^g, v_{n-1}^h].$$

Die Sequenzen v wurden so konstruiert, dass in einer endlichen auflösbaren Gruppe G, die die Auflösungslänge k hat, die Gleichung $v_{k+1}(x, y) = 1$ für alle $x, y \in G$ gilt. Damit ist schon eine Richtung in einem zu den u_n– und s_n– Sätzen analogen Satz erfüllt.

Wir wählen sechs geeignete Sequenzen aus und beweisen die zu den u_n– und s_n– Sätzen analoge Aussage.

Hauptsatz 0.1. *Die sechs Sequenzen $v = (v_1, v_2, v_3, \dots)$ seien definiert durch:*

(1) $v_1 := yx^2, \quad v_n := [v_{n-1}^{y^{-1}x^{-1}}, v_{n-1}^{x^{-1}}]$;
(2) $v_1 := yx^2, \quad v_n := [v_{n-1}^{y^{-1}x^{-1}}, v_{n-1}^{yx}]$;
(3) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{x}]$;
(4) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{y^{-1}}]$;
(5) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{xyx}]$;
(6) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{y^{-1}x^{-1}y^{-1}}]$.

G sei eine endliche Gruppe und v eine der sechs Sequenzen. Dann gilt: G ist auflösbar $\Leftrightarrow$ es gibt ein $k \in \mathbb{N}$ mit $v_k(x, y) = 1$ für alle $x, y \in G$.

Die Beweise für die Sequenzen (1) und (2) sind analog. Für die Sequenzen $(3), (4), (5)$ und (6) folgt der Beweis in trivialer Weise aus dem Beweis des u_n-Satzes.

Für die erste Sequenz wird der Hauptsatz in den Kapiteln 4 und 5 vollständig bewiesen.

Für den Beweis werden teilweise Verfahren aus dem Beweis zu dem u_n– Satz benutzt. Allerdings, haben wir den neuen Beweis so durchgeführt, dass er möglicherweise für noch 274 weitere Sequenzen, die wir im Anhang B angeben, anwendbar ist. Zusätzlich ist der neue Beweis an einigen Stellen deutlich einfacher, weil wir einige neue Ideen zur Lösung der Probleme benutzt haben.

Im Kapitel 6 behandeln wir eine andere Frage.

Sei $e = (e_1, e_2, e_3, \dots)$ die Sequenz aus dem Satz von Zorn.

Definition 0.6. G sei eine Gruppe.

G erfüllt die *n–te Engelbedingung,* falls $e_n(x, y) = 1$ für alle $x, y \in G$. Eine Gruppe, die die n–te Engelbedingung erfüllt, nennen wir *n–Engel Gruppe.*

Ist G eine Gruppe von der Nilpotenzklasse k, dann ist G eine k–Engel Gruppe, denn aus $[x_0, x_1, \dots, x_k] = 1$ für alle $x_1, \dots, x_k \in G$ folgt $e_k(x, y) = [x, \underbrace{y, \dots, y}_{k}] = 1$ für alle $x, y \in G$.

Nun stellt sich die Frage, inwiefern die „Umkehrung“ gilt, d.h. ob man die Nilpotenzklasse einer k–Engel Gruppe nach oben abschätzen kann.

- Die 1–Engel Gruppen sind genau die abelschen Gruppen.
- Für die 2–Engel Gruppen zeigte F. W. Levi, dass sie höchstens von der Nilpotenzklasse 3 sind [Le42].
- Heinecken zeigte, dass 3–Engel Gruppen höchstens von der Nilpotenzklasse 4 sind, wenn sie keine Elemente der Ordnungen 2 und 5 haben [He61].
- Eine 4–Engel Gruppe ist höchstens von der Nilpotenzklasse 7, wenn sie keine Elemente der Ordnungen 2, 3 und 5 hat [Tr95] [HVL05].

  In diesen Fällen war die k–Engel Gruppe nicht notwendig endlich.
- Für höhere Engel Gruppen gibt es bisher keine analogen Aussagen.

Man sieht, dass immer mehr Elemente mit bestimmten Ordnungen bei diesen Abschätzungen ausgeschlossen werden.

Wir zeigen eine allgemeinere Aussage: Wenn man die Nilpotenzklasse einer k–Engel Gruppe abschätzen möchte, muss man fordern, dass die Gruppe keine Elemente der Ordnung p für alle Primzahlen $p < k$ enthält. Das folgt aus dem folgenden Satz.

Satz 0.7. *Sei p eine Primzahl und $n \in \mathbb{N}$. Es existiert eine $(p+1)$–Engel p–Gruppe von der Nilpotenzklasse n.*

Also finden wir für jedes $k \in \mathbb{N}$ und alle Primzahlen $p < k$ eine k–Engel p–Gruppe, die von beliebig großer Nilpotenzklasse ist.

Aus dem Beweis zu dem vorherigen Satz kann man noch eine Aussage schließen:

Satz 0.8. *Sei p eine Primzahl. Dann existiert eine unendliche $(p+1)$–Engel p–Gruppe, die nicht nilpotent ist. Für alle $n \in \mathbb{N}$ enthält diese Gruppe eine von n Elementen erzeugte Untergruppe von der Nilpotenzklasse mindestens $n+1$.*

Analoge Probleme kann man auch in auflösbaren Gruppen für die Sequenzen u, s oder v formulieren. Zum Beispiel habe ich in meiner Diplomarbeit gezeigt, dass wenn alle Elemente einer endlichen Gruppe die Gleichung $u_2(x, y) = 1$ erfüllen, so ist die Auflösungslänge von G höchstens 2.

An dieser Stelle möchte ich danken: Fritz Grunewald für die Anregung zur selbstständigen Arbeit, Jens Piontkowski für die Diskussionsbereitschaft zu jeder Tageszeit sowie den Mitarbeitern des Mathematischen Instituts der HHU–Düsseldorf für nette Diskussionen, die mich auf einige neue Ideen brachten.

Kapitel 1

Beweisskizze des $\mathbf{u_n}$–Satzes

Da wir die Hauptschritte von dem u_n– Beweis übernehmen, geben wir eine Beweisskizze an.

($\Rightarrow$) Ist G auflösbar mit der Auflösungslänge k, so ist $u_{k-1}(x,y) = 1$ für alle $x, y \in G$. Das ist erfüllt, weil $u_{k-1}(x,y) \in G^{(k)}$ ist.

($\Leftarrow$) Die andere Beweisrichtung ist komplizierter. Es wird gezeigt: Ist G nicht auflösbar, so gibt es $x, y \in G$, so dass $u_k(x,y) \neq 1$ für alle $k \in \mathbb{N}$.

Sei G das kleinste Gegenbeispiel, also eine nicht auflösbare endliche Gruppe mit der minimalen Ordnung, in der für ein $k \in \mathbb{N}$ die Gleichung $u_k(x,y) = 1$ für alle x und y gilt. Dann ist G einfach, weil für alle Normalteiler von G ebenfalls $u_k(x,y) = 1$ gelten würde. Thompson [Th68] hat bewiesen, dass eine endliche einfache Gruppe, die nur auflösbare Untergruppen besitzt, entweder

(1) $\mathrm{PSL}(3, \mathbb{F}_3)$ oder

(2) $\mathrm{PSL}(2, \mathbb{F}_q)$, wenn $q = p^n$, $q \geq 4$ und p Primzahl, oder

(3) $\mathrm{Sz}(2^n)$, wobei $n \in \mathbb{N}, n \geq 3$ und ungerade, ist.

Wir geben die Definitionen der Gruppen $\mathrm{PSL}(3, \mathbb{F}_3)$, $\mathrm{PSL}(2, \mathbb{F}_q)$ und $\mathrm{Sz}(2^n)$ an.

Definition 1.1.

$$\mathrm{PSL}(3, \mathbb{F}_3) := \mathrm{SL}(3, \mathbb{F}_3)$$

ist eine endliche einfache Gruppe mit 5616 Elementen.

Definition 1.2. Seien p eine Primzahl, $n \in \mathbb{N}$ und $q = p^n$. Dann heißt

$$\mathrm{PSL}(2, \mathbb{F}_q) := \mathrm{SL}(2, \mathbb{F}_q)/\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$$

projektive spezielle lineare Gruppe über $\mathbb{F}_q$.

Definition 1.3. Für $m \in \mathbb{N}$ seien $n := 2m+1$ und $\theta : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ der Authomorphismus von $\mathbb{F}_{2^n}$, gegeben durch $\theta(a) = a^{2^{m+1}}$.

Seien

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

$$M(\lambda) = \begin{pmatrix} \lambda^{1+2^m} & 0 & 0 & 0 \\ 0 & \lambda^{2^m} & 0 & 0 \\ 0 & 0 & \lambda^{-2^m} & 0 \\ 0 & 0 & 0 & \lambda^{2^{-1-2^m}} \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Dann heißt

$$\mathrm{Sz}(2^n) = \langle S(a,b), M(\lambda), T \mid a,b,\lambda \in \mathbb{F}_{2^n}, \lambda \neq 0 \rangle \leq GL(4, \mathbb{F}_{2^n})$$

Suzuki Gruppe über $\mathbb{F}_{2^n}$ [S62, s. 133],[HB82, XI.3].

Zuerst wird der folgende Satz bewiesen:

Satz 1.4. *[BGGKPP] Sei G eine der folgenden Gruppen:*

(1) $\mathrm{PSL}(3, \mathbb{F}_3)$,

(2) $\mathrm{PSL}(2, \mathbb{F}_q)$, *wenn* $q = p^n$, $q \geq 4$ *und p Primzahl,*

(3) $\mathrm{Sz}(2^n)$, *wobei* $n \in \mathbb{N}, n \geq 3$ *und ungerade.*

Dann existieren $x, y \in G$, so dass $u_1(x,y) \neq 1$ und $u_1(x,y) = u_2(x,y)$.

Nach Satz 1.4 gibt es in jeder von diesen Gruppen Elemente x und y, für die $1 \neq u_1(x,y) = u_2(x,y)$ gilt. Nach der Konstruktion von u_n gilt dann $1 \neq u_1(x,y) = u_k(x,y)$ für alle $k \in \mathbb{N}$.

Beweisskizze von Satz 1.4.(vgl. [BGGKPP])

(1) Für $\mathrm{PSL}(3, \mathbb{F}_3)$ wird einfach ein Beispiel gefunden.

(2) Für $\mathrm{PSL}(2, \mathbb{F}_q)$ seien

$$x(t) := \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \text{ und } y(a,b) := \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix}$$

Matrizen mit Einträgen aus $\mathbb{Z}[t,a,b]$. Wählt man t, a, b aus $\mathbb{F}_q$, so sind $x, y \in \mathrm{PSL}(2, \mathbb{F}_q)$.

Sei I_0 das Ideal in $\mathbb{Z}[t,a,b]$, erzeugt von den vier polynomialen Einträgen der Matrix

$$u_1(x(t),y(a,b))-1$$

und I das Ideal, erzeugt von den vier polynomialen Einträgen der Matrix

$$u_1(x(t),y(a,b))-u_2(x(t),y(a,b)).$$

Reduziert man die Koeffizienten modulo p, so erhält man Ideale I und I_0 in $\mathbb{F}_p[t,a,b]$. Es wird gezeigt, dass die Nullstellenmenge $V(I)$ eine Kurve und $V(I_0)=\emptyset$ in $\mathbb{A}^3(\mathbb{F}_q)$ ist. Zu zeigen bleibt, dass $V(I)\setminus V(I_0)=V(I)$ mindestens einen Punkt in $\mathbb{A}^3(\mathbb{F}_q)$ hat.

Mit der Hasse–Weil Schranke [FJ86, 3.14] wird gezeigt, dass für $q\geqslant 593$ die Kurve $V(I)$ rationale Punkte in $\mathbb{A}^3(\mathbb{F}_q)$ hat. Für $4\leqslant q<593$ werden Beispiele direkt mit dem Computer berechnet.

(3) Für den Fall $\mathrm{Sz}(2^{2m+1})$ werden folgende Matrizen mit Einträgen aus $\mathbb{F}_2[a,b,c,d,a_0,b_0,c_0,d_0]$ definiert:

$$x(a,b,a_0,b_0):=\begin{pmatrix} a^2a_0+ab+b_0 & b & a & 1\\ aa_0+b & a_0 & 1 & 0\\ a & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}$$

und

$$y(c,d,c_0,d_0):=\begin{pmatrix} c^2c_0+cd+d_0 & d & c & 1\\ cc_0+d & c_0 & 1 & 0\\ c & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}.$$

Sei I_0 das Ideal in $\mathbb{F}_2[a,b,c,d,a_0,b_0,c_0,d_0]$, erzeugt von den 16 polynomialen Einträgen der Matrix

$$u_1(x(a,b,a_0,b_0),y(c,d,c_0,d_0))-1$$

und I das Ideal, erzeugt von den 16 polynomialen Einträgen der Matrix

$$u_1(x(a,b,a_0,b_0),y(c,d,c_0,d_0))-u_2(x(a,b,a_0,b_0),y(c,d,c_0,d_0)).$$

Die Nullstellenmenge $V(I)$ ist eine Fläche in $\mathbb{A}^8(\mathbb{F}_{2^{2m+1}})$ und $V(I_0)=\{(0,0,0,0,0,0,0,0)\}$.

Die Punkte $(a,b,c,d,a_0,b_0,c_0,d_0)\in V(I)\setminus V(I_0)$ sind Nullstellen der Gleichung u_1-u_2, aber sie garantieren noch nicht, dass $x(a,b,a_0,b_0)$ und $y(c,d,c_0,d_0)$ Elemente der $\mathrm{Sz}(2^{2m+1})$ sind.

Um solche Punkte zu finden, braucht man noch folgende Hilfsmittel:

Die Abbildung α sei definiert durch

$$\begin{array}{lll} \alpha: & \mathbb{A}^8(\overline{\mathbb{F}}_2) & \longrightarrow \quad \mathbb{A}^8(\overline{\mathbb{F}}_2) \\ & (a,b,c,d,a_0,b_0,c_0,d_0) & \longmapsto \quad (a_0,b_0,c_0,d_0,a^2,b^2,c^2,d^2). \end{array}$$

Ist $(a,b,c,d,a_0,b_0,c_0,d_0) \in V(I) \setminus V(I_0)$ ein Fixpunkt von α^{2m+1}, d.h. $\alpha^{2m+1}(a,b,c,d,a_0,b_0,c_0,d_0) = (a,b,c,d,a_0,b_0,c_0,d_0)$, so gilt

$(a_0^{2^m}, b_0^{2^m}, c_0^{2^m}, d_0^{2^m}, a^{2^{m+1}}, b^{2^{m+1}}, c^{2^{m+1}}, d^{2^{m+1}}) = (a,b,c,d,a_0,b_0,c_0,d_0)$.

Dann ist $a = a^{2^{2m+1}} = a^{2^n}$, also $a \in \mathbb{F}_{2^n}$ und $a_0 = a^{2^{m+1}} = \theta(a)$. Dasselbe gilt für b, c und d. Damit sind $x(a,b,a_0,b_0) = TS(a,b)$ und $y(c,d,c_0,d_0) = TS(c,d)$ Elemente von $\mathrm{Sz}(2^n)$.

Mit der Lefschetzschen Fixpunktformel [BGGKPP, 3.6] wird gezeigt, dass für $2m+1 > 48$ die Abbildung α^{2m+1} mehr als einen Fixpunkt aus $V(I)$ hat. Für $3 \leqslant 2m+1 \leqslant 48$ werden Beispiele ausgerechnet.

□

Kapitel 2

Neue Sequenzen

Es stellte sich die Frage, für welche anderen Sequenzen die Aussagen wie in den u_n– und s_n– Sätzen möglich sind. In diesem Kapitel beschreiben wir eine neue Idee für die Konstruktion der Sequenzen. Dann werden wir einige geeignete Sequenzen auswählen und für diese die zu den u_n– und s_n– Sätzen analoge Aussage beweisen.

2.1 Definition

Definition 2.1. Sei $F = \langle x, y\rangle$ die freie Gruppe mit zwei Erzeugern und $f, g, h \in F$. Die Sequenz $v = (v_1, v_2, \dots)$ sei definiert durch

$$v_1 := f \text{ und } v_n := [v_{n-1}^g, v_{n-1}^h].$$

Wir schreiben v_i, wenn es als Element der freien Gruppe F gemeint ist und $v_i(x, y)$, wenn feste x und y aus einer endlichen Gruppe G eingesetzt werden. Jede Sequenz wird durch ein Tripel $(f, g, h) \in F^3$ festgelegt. Sei

$$S_0 := \{(f, g, h) \in F^3\}$$

die Menge der so konstruierten Sequenzen. Das sind unendlich viele, jedoch sind einige von ihnen trivial.

Beispiel 2.2. Für $f = xy$, $g = x$ und $h = y$ ist $v_1 = xy$ und $v_n = [v_{n-1}^x, v_{n-1}^y]$. Also $v = (v_1, v_2, \dots)$ mit

$$\begin{aligned} v_1 = &\ xy, \\ v_2 = &\ x^{-1}y^{-3}x^{-1}y^2xy^{-1}xy^2, \\ v_3 = &\ x^{-1}y^{-2}x^{-1}yx^{-1}y^{-2}xy^3x^2y^{-3}x^{-1}yx^{-1}y^{-2}xy^3xyx^{-2}y^{-3}x^{-1}y^2xy^{-1}xy^2xy^{-1} \\ &\ x^{-1}y^{-3}x^{-1}y^2xy^{-1}xy^3, \dots . \end{aligned}$$

Für $f = xy$, $g = x$ und $h = y^{-1}$ ist $v_1 = xy$ und $v_n = [v_{n-1}^x, v_{n-1}^{y^{-1}}]$, aber $v = (xy, 1, 1, 1, 1, \dots)$.

Wir fassen einige Eigenschaften der Sequenzen zusammen:

Lemma 2.3. *G sei eine Gruppe, $v = (v_1, v_2, \dots)$ eine Sequenz aus 2.1. Dann gilt:*

(1) Ist G auflösbar mit der Auflösungslänge k, so ist $v_{k+1}(x, y) = 1$ für alle $x, y \in G$.

(2) Gilt $v_k(x, y) = v_{k+1}(x, y)$ für $x, y \in G$, so gilt für alle $n \geqslant k$ auch $v_k(x, y) = v_n(x, y)$.

(3) Ist $k \in \mathbb{N}$ mit $v_k(x, y) = 1$ für $x, y \in G$, so gilt für alle $n \geqslant k$ ebenfalls $v_n(x, y) = 1$.

Beweis. (1) Wir zeigen mit Induktion, dass $v_{k+1}(x, y) \in G^{(k)}$ für alle $k \in \mathbb{N}$ und alle $x, y \in G$. Für alle x und y aus G gilt:

$$v_2(x, y) = [v_1(x, y)^g, v_1(x, y)^h] \in G^{(1)} = [G, G].$$

Sei nun $v_k(x, y) \in G^{(k-1)}$, dann sind auch $v_k(x, y)^g$ und $v_k(x, y)^h$ in $G^{(k-1)}$, weil $[a, b]^c = [a^c, b^c]$. Damit ist

$$v_{k+1}(x, y) = [v_k(x, y)^g, v_k(x, y)^h] \in G^{(k)} = [G^{(k-1)}, G^{(k-1)}].$$

Wenn G auflösbar ist mit der Auflösungslänge k, so ist $G^{(k)} = 1$ und damit $v_{k+1}(x, y) = 1$ für alle $x, y \in G$.

(2) Ist $v_k(x, y) = v_{k+1}(x, y)$, dann gilt

$$v_{k+2}(x, y) = [v_{k+1}(x, y)^g, v_{k+1}(x, y)^h] = [v_k(x, y)^g, v_k(x, y)^h] = v_{k+1}(x, y)$$

für alle $x, y \in G$. Induktiv folgt $v_k(x, y) = v_n(x, y)$ für alle $n \geqslant k$.

(3) Analog zu (2). □

2.2 Geeignete Sequenzen

Aus dem Lemma 2.3 sehen wir, dass alle Sequenzen in 2.1 so konstruiert wurden, dass sie schon eine Beweisrichtung der zu u_n– und s_n– Sätzen analogen Aussage erfüllen. Es gilt:

Ist G auflösbar, so existiert ein $k \in \mathbb{N}$, so dass $v_k(x, y) = 1$ für alle $x, y \in G$.

Es gilt ebenfalls: Ist $1 \neq v_1(x,y) = v_2(x,y)$, so gilt $1 \neq v_1(x,y) = v_n(x,y)$ für alle $n \in \mathbb{N}$.

Wenn wir beweisen, dass für eine Sequenz v in jeder der Gruppen

- $\mathrm{PSL}(3, \mathbb{F}_3)$,
- $\mathrm{PSL}(2, \mathbb{F}_q)$, wenn $q = p^n$, $q \geq 4$ und p Primzahl,
- $\mathrm{Sz}(2^n)$, wobei $n \in \mathbb{N}, n \geq 3$ und ungerade,

x und y mit $1 \neq v_1(x,y) = v_2(x,y)$ existieren, so erfüllt diese Sequenz eine zu den u_n– und s_n– Sätzen analoge Aussage.

Die Menge S_0 enthält unendlich viele Sequenzen. Wir untersuchen davon die einfachsten. Sei

$$F_3 := \{a_1 a_2 a_3 \mid a_1, a_2, a_3 \in \{1, x, y, x^{-1}, y^{-1}\}\}$$

die Teilmenge der Worte aus F, die höchstens die Länge 3 haben. Die Menge

$$S_1 := \{(f,g,h) \mid f,g,h \in F_3\} \subseteq S_0$$

hat dann 140608 Elemente. Diese Sequenzen berechnen wir mit einem einfachem MAGMA Programm, das im Anhang A.1 angegeben wird.

Aus der Menge S_1 wählen wir solche Sequenzen, für die der $\mathrm{PSL}(2, \mathbb{F}_q)$–Beweis (vgl.1.4) durchführbar ist. Zuerst benötigen wir einige Definitionen.

Für fest gewählte $f,g,h \in F$ sei $v = (v_1, v_2, \dots)$ die Sequenz zu f,g,h. Weiter seien

$$x = x(t) := \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \text{ und } y = y(a,b) := \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix}$$

Matrizen mit Einträgen aus dem Polynomring $\mathbb{Q}[t,a,b]$.

Wir definieren

$$\begin{aligned} \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} &:= v_2(x,y) - v_1(x,y) \\ &= [f(x,y)^{g(x,y)}, f(x,y)^{h(x,y)}] - f(x,y) \text{ und} \\ \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} &:= v_1(x,y) - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= f(x,y) - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Seien I, I_0 die von den Einträgen der Matrizen erzeugten Ideale in $\mathbb{Q}[t,a,b]$ und $V(I), V(I_0)$ die Nullstellenmengen in dem affinen Raum $\mathbb{A}^3(\mathbb{Q})$, also

$$\begin{aligned} I &:= \langle m_{11}, m_{12}, m_{21}, m_{22}\rangle, \\ I_0 &:= \langle n_{11}, n_{12}, n_{21}, n_{22}\rangle, \\ V(I) &:= \{(t,a,b) \in \mathbb{A}^3(\mathbb{Q}) \mid r(t,a,b) = 0 \ \forall r \in I\}, \\ V(I_0) &:= \{(t,a,b) \in \mathbb{A}^3(\mathbb{Q}) \mid r(t,a,b) = 0 \ \forall r \in I_0\}. \end{aligned}$$

Da alle Polynome in I und I_0 aus $\mathbb{Z}[t,a,b]$ sind, können wir sie modulo p reduzieren. Das liefert Ideale I und I_0 in $\mathbb{F}_p[t,a,b]$ und die Nullstellenmengen

$$V_q(I) := \{(t,a,b) \in \mathbb{A}^3(\mathbb{F}_q) \mid r(t,a,b) = 0 \ \forall r \in I\},$$

$$V_q(I_0) := \{(t,a,b) \in \mathbb{A}^3(\mathbb{F}_q) \mid r(t,a,b) = 0 \ \forall r \in I_0\}, \text{ mit } q = p^n.$$

Bemerkung 2.4. Es gilt $V(I_0) \subseteq V(I)$ und $V_q(I_0) \subseteq V_q(I)$, weil nach Lemma 2.3 aus $v_1 = 1$ auch $v_2 = 1$ folgt, und damit $v_1 = v_2$.

Wir sind an solchen Sequenzen $v = (v_1, v_2, \dots)$ interessiert, für die die Menge $V(I) \setminus V(I_0)$ nicht leer ist.

Dafür berechnen wir zunächst für jedes $(f,g,h) \in S_1$ die Dimensionen von $V(I)$ und $V(I_0)$. (MAGMA Programm im Anhang A.2).

Die Berechnungen zeigen, dass $\dim V(I), \dim V(I_0) \in \{-1, 0, 1\}$, wobei dim $= -1$ bedeutet, dass die Menge leer ist. Sei

$$S_2 := \{(f,g,h) \in S_1 \mid \dim V(I) = 1 \text{ und } \dim V(I_0) = -1\} \subseteq S_1 \subseteq S_0.$$

Hier haben wir solche Sequenzen ausgewählt, bei denen der Abstand der Dimensionen von $V(I)$ und $V(I_0)$ am größten war. Das war etwas „grob“, aber wir wollten die Menge der Sequenzen reduzieren und nur die günstigsten behalten.

Aus der Menge S_2 wählen wir solche Sequenzen, die für kleine Primzahlpotenzen q tatsächlich Lösungen von $v_1(x,y) = v_2(x,y)$ und $v_1(x,y) \neq 1$ in $\mathrm{PSL}(2, \mathbb{F}_q)$ haben. Für eine fest gewählte Sequenz v sei

$$A_q(v) :=\mid \{(a,b) \in PSL(2, \mathbb{F}_q) \mid v_1(a,b) = v_2(a,b) \text{ und } v_1(a,b) \neq 1\} \mid .$$

Sei

$$S_3 := \{(f,g,h) \in S_2 \mid A_q(v) \neq 0 \text{ für } 5 \leq q \leq 31\} \subseteq S_2 \subseteq S_1 \subseteq S_0.$$

Die Menge S_3 enthält 274 Sequenzen, die sind im Anhang B aufgelistet.

Als Erstes bemerken wir, dass einige Sequenzen trivialerweise die analoge Aussage zu den u_n– und s_n– Sätzen erfüllen, weil die Gleichungen $v_1 = v_2$ und $u_1 = u_2$ für diese äquivalent sind. Im Abschnitt 2.3 wird dieser Satz formuliert. Dann werden wir zwei weitere Sequenzen aus S_3 auswählen, im Kapitel 3 die die analoge Aussage zu den u_n– und s_n– Sätzen formulieren und in den Kapiteln 4 und 5 vollständig beweisen. Der Beweis wird konstruktiv angegeben, so dass er auch für jede andere Sequenz aus S_3 durchführbar ist.

2.3 Vier neue Sequenzen

Satz 2.5. *Die vier Sequenzen $v = (v_1, v_2, v_3, \dots)$ seien definiert durch:*

(1) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{x}];$
(2) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{y^{-1}}];$
(3) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{xyx}];$
(4) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{y^{-1}x^{-1}y^{-1}}];$

G sei eine endliche Gruppe und v eine der vier Sequenzen. Dann gilt: G ist auflösbar $\Leftrightarrow$ es gibt ein $k \in \mathbb{N}$ mit $v_k(x, y) = 1$ für alle $x, y \in G$.

Beweis. Der Beweis folgt direkt aus dem Beweis zu dem u_n-Satz (vgl. Kapitel 1). Denn für jede der Sequenzen ist die Gleichung $v_1 = v_2$ äquivalent zu $u_1 = u_2$. Für die Sequenz $u = (u_1, u_2, \dots)$ ist

$$\begin{aligned} & u_1 && = u_2 \\ \Leftrightarrow\ & x^{-2}y^{-1}x && = x^{-3}y^{-1}x^2yx^{-1}yx^2y^{-1} \\ \Leftrightarrow\ & y^{-1}x^{-1} && = x^{-1}y^{-1}x^2yx^{-1}yx^2y^{-1}x^{-2} \end{aligned}$$

Und für die vier Sequenzen $v = (v_1, v_2, \dots)$ gilt:

$$\begin{aligned} & v_1 && = v_2 \\ \Leftrightarrow\ & xy && = yxy^{-2}x^{-1}yx^{-1}y^{-2}xy^2. \end{aligned}$$

Das ist dieselbe Gleichung, wenn wir x durch y^{-1} und y durch x^{-1} ersetzen.

Zu zeigen bleibt, dass $v_1(x, y) \neq 1$, also $y^{-1}x^{-1} \neq 1$ für die speziellen x und y aus dem Beweis von dem Satz 1.4, für die $1 \neq u_1(x, y) = u_2(x, y)$ galt.

(1) Der Fall $\mathrm{PSL}(2, \mathbb{F}_q)$. Für

$$x(t) = \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \text{ und } y(a, b) = \begin{pmatrix} 1 & a \\ b & 1 + ab \end{pmatrix}$$

ist $y^{-1}x^{-1} = \begin{pmatrix} a & -ta+ab+1 \\ -1 & t-b \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ für alle $a, b, t \in \mathbb{F}_q$.

(2) Der Fall $\mathrm{Sz}(2^{2m+1})$. Sind

$$x(a,b,a_0,b_0) = \begin{pmatrix} a^2a_0+ab+b_0 & b & a & 1 \\ aa_0+b & a_0 & 1 & 0 \\ a & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

und

$$y(c,d,c_0,d_0) = \begin{pmatrix} c^2c_0+cd+d_0 & d & c & 1 \\ cc_0+d & c_0 & 1 & 0 \\ c & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

dann folgt aus $y^{-1}x^{-1} = 1$ auch $a = b = c = d = a_0 = b_0 = c_0 = d_0 = 0$.

(3) Der Fall $\mathrm{PSL}(3, \mathbb{F}_3)$. In diesem Fall wurden keine speziellen x und y aus $\mathrm{PSL}(3, \mathbb{F}_3)$ ausgewählt. Aber wir können den Satz für diese Gruppe direkt beweisen. Mit MAGMA berechnen wir, dass es $x, y \in PSL(3, \mathbb{F}_3)$ gibt mit $v_1(x,y) = v_2(x,y)$ und $v_1(x,y) \neq 1$ für alle vier Sequenzen (A.3).

Wir haben gezeigt, dass die Aussage des Satzes 1.4 für alle vier Sequenzen v gilt, mit den Bemerkungen 2.3 gilt die Behauptung (vgl. Beweisskizze von dem u_n-Satz). □

Kapitel 3

Hauptsatz

In diesem Kapitel werden wir für die vier Sequenzen aus 2.3 und zwei neue Sequenzen die analoge Aussage zu den u_n– und s_n– Sätzen formulieren. In dem Beweis werden die Hauptschritte aus dem Beweis des u_n-Satzes benutzt, allerdings, werden die Zwischenschritte konstruktiv angegeben. Das bedeutet, dass man diesen Beweis für jede Sequenz aus S_3 durchführen kann. Zusätzlich wird der neue Beweis an einigen Stellen deutlich einfacher.

Hauptsatz 3.1. *Die 6 Sequenzen $v = (v_1, v_2, v_3, \dots)$ seien definiert durch:*

(1) $v_1 := yx^2, \quad v_n := [v_{n-1}^{y^{-1}x^{-1}}, v_{n-1}^{x^{-1}}];$
(2) $v_1 := yx^2, \quad v_n := [v_{n-1}^{y^{-1}x^{-1}}, v_{n-1}^{yx}];$
(3) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{x}];$
(4) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{y^{-1}}];$
(5) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{xyx}];$
(6) $v_1 := xy, \quad v_n := [v_{n-1}^{yx^{-1}y^{-1}}, v_{n-1}^{y^{-1}x^{-1}y^{-1}}];$

G sei eine endliche Gruppe und v eine der sechs Sequenzen. Dann gilt: G ist auflösbar $\Leftrightarrow$ es gibt ein $k \in \mathbb{N}$ mit $v_k(x, y) = 1$ für alle $x, y \in G$.

Bemerkung 3.1. Für Sequenzen (3), (4), (5) und (6) wurde die Aussage schon im Satz 2.5 bewiesen. Die Gleichungen $v_1 = v_2$ sind für die Sequenzen (1) und (2) aus (3.1) gleich, weil

(1) $v_1 = v_2 \Leftrightarrow yx^2 = [(yx^2)^{y^{-1}x^{-1}}, (yx^2)^{x^{-1}}] = xyx^{-2}y^{-2}x^{-2}yx^3,$

(2) $v_1 = v_2 \Leftrightarrow yx^2 = [(yx^2)^{y^{-1}x^{-1}}, (yx^2)^{yx}] = xyx^{-2}y^{-2}x^{-2}yx^3.$

Genauso die Gleichung $v_1 \neq 1$.

Nach Konstruktion von $v = (v_1, v_2, v_3, \dots)$ (vgl. Beweisskizze von dem u_n-Satz) und obiger Bemerkung müssen wir nur den folgenden Satz beweisen.

Satz 3.2. *Seien* $v_1 = yx^2$ *und* $v_2 = [(yx^2)^{y^{-1}x^{-1}}, (yx^2)^{x^{-1}}]$

und G *eine der folgenden Gruppen:*

(1) $\mathrm{PSL}(2, \mathbb{F}_q)$, *wenn* $q = p^n$, $q \geq 4$ *und* p *Primzahl,*

(2) $\mathrm{Sz}(2^n)$, *wobei* $n \in \mathbb{N}, n \geq 3$ *und ungerade,*

(3) $\mathrm{PSL}(3, \mathbb{F}_3)$.

Dann existieren $x, y \in G$, *so dass* $v_1(x, y) \neq 1$ *und* $v_1(x, y) = v_2(x, y)$.

Beweis von Satz 3.2

(1) Der Fall $G = PSL(2, \mathbb{F}_q)$ wird im Kapitel 4 bewiesen,

(2) Der Fall $G = Sz(2^n)$ wird im Kapitel 5 bewiesen.

(3) Sei $G = PSL(3, \mathbb{F}_3)$. Die Gruppe G hat 5616 Elemente. Mit dem MAGMA Programm, das wir im Anhang A.3 angeben, können wir ausrechnen, dass für 44928 von 31539456 Paaren $(x, y) \in G^2$ die Bedingungen $v_1(x, y) = v_2(x, y)$ und $v_1(x, y) \neq 1$ gelten.

Kapitel 4

Beweis für $\mathrm{PSL}(2, \mathbb{F}_q)$

In diesem Kapitel beweisen wir den folgenden Satz:

Satz 4.1. *Seien*

$$v_1 := yx^2 \text{ und } v_2 := [(yx^2)^{y^{-1}x^{-1}}, (yx^2)^{x^{-1}}].$$

Für jedes $q = p^k$, ($k \in \mathbb{N}$, p Primzahl, $q \geq 4$) gibt es $x, y \in PSL(2, \mathbb{F}_q)$, so dass $v_1(x, y) = v_2(x, y)$ und $v_1(x, y) \neq 1$.

Wir erinnern an einige bekannte Eigenschaften von $\mathrm{PSL}(2, \mathbb{F}_q)$ [DSW]:

(1) $|PSL(2, \mathbb{F}_q)| = \begin{cases} q(q^2-1), & \text{wenn } q \text{ gerade,} \\ q(q^2-1)/2, & \text{wenn } q \text{ ungerade,} \end{cases}$

(2) $\mathrm{PSL}(2, \mathbb{F}_q) = \langle T, S \rangle$, wobei $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$,

(3) $\mathrm{PSL}(2, \mathbb{F}_q)$ ist einfach für $q \geq 4$.

Für den Beweis von Satz 4.1 setzen wir

$$x(t) := \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \text{ und } y(a, b) := \begin{pmatrix} 1 & a \\ b & 1 + ab \end{pmatrix}$$

als Matrizen mit den Einträgen aus $\mathbb{Z}[t, a, b]$. Für $t, a, b \in \mathbb{F}_q$ sind $x(t), y(a, b) \in PSL(2, \mathbb{F}_q)$. Wir wollen zeigen, dass $t, a, b \in \mathbb{F}_q$ existieren mit

$$v_1(x(t), y(a, b)) = v_2(x(t), y(a, b)) \text{ und } v_1(x(t), y(a, b)) \neq 1.$$

Die Gleichung $v_1 = v_2$ ist äquivalent zu $y^{-2}x^{-2}yx = x^2y^{-1}x^{-1}y$ und $v_1 \neq 1$ ist äquivalent zu $yx^2 \neq 1$.

Wir setzen

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} := y(a,b)^{-2}x(t)^{-2}y(a,b)x(t) - x(t)^2y(a,b)^{-1}x(t)^{-1}y(a,b),$$
$$\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} := y(a,b)x(t)^2 - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und erhalten

$$\begin{aligned}
m_{11} &= -t^3a^2b^2 - t^3ab - t^2a^3b^2 + t^2a^2b^3 - 2t^2a^2b + 2t^2ab^2 - t^2a + t^2b + \\
&\quad ta^3b^3 + ta^3b + 4ta^2b^2 + 2ta^2 + 2tab - tb^2 - t + ab^2 + 2a + b, \\
m_{12} &= t^3a^2b + t^3a - t^2a^2 + t^2ab - ta^2b^3 - 2ta^2b - 4tab^2 - 4ta - 2tb + a^2b^2 + \\
&\quad a^2 + 3ab + 2, \\
m_{21} &= t^3ab^2 + t^3b + t^2a^2b^2 - t^2ab^3 + 2t^2ab - 2t^2b^2 - ta^2b^3 - ta^2b - 4tab^2 - \\
&\quad 2ta - tb - b^2 - 2, \\
m_{22} &= t^2a^2b - t^2ab^2 + t^2a - t^2b - ta^2b^2 - ta^2 + tab^3 + 2tb^2 + t - ab^2 - a - 2b,
\end{aligned}$$

$$\begin{aligned}
n_{11} &= t^2 + ta - 2, \\
n_{12} &= -t - a, \\
n_{21} &= t^2b + tab + t - b, \\
n_{22} &= -tb - ab - 2.
\end{aligned}$$

Seien I, I_0 die von den Einträgen der Matrizen erzeugten Ideale in $\mathbb{Z}[t,a,b]$,

$$\begin{aligned}
I &:= \langle m_{11}, m_{12}, m_{21}, m_{22} \rangle, \\
I_0 &:= \langle n_{11}, n_{12}, n_{21}, n_{22} \rangle.
\end{aligned}$$

Reduziert man die Gleichungen $m_{11}, \ldots, m_{22}, n_{11}, \ldots, n_{22}$ modulo p, so erhält man die Ideale I, I_0 in $\mathbb{F}_p[t,a,b]$ und die Nullstellenmengen $V_q(I)$ und $V_q(I_0)$ in $\mathbb{A}^3(\mathbb{F}_q)$.

$$\begin{aligned}
V_q(I) &:= \{(t,a,b) \in \mathbb{A}^3(\mathbb{F}_q) \mid r(t,a,b) = 0 \ \forall r \in I\}, \\
V_q(I_0) &:= \{(t,a,b) \in \mathbb{A}^3(\mathbb{F}_q) \mid r(t,a,b) = 0 \ \forall r \in I_0\}.
\end{aligned}$$

Jetzt ist unsere Behauptung äquivalent dazu, dass $V_q(I) \setminus V_q(I_0)$ für jede Primzahlpotenz q mindestens einen Punkt (t,a,b) besitzt. Dieser Punkt liefert dann $x(t)$ und $y(a,b)$ in $\mathrm{PSL}(2,\mathbb{F}_q)$ mit $v_1(x(t),y(a,b)) = v_2(x(t),y(a,b))$ und $v_1(x(t),y(a,b)) \neq 1$.

Um $V(I)$ zu verstehen, berechnen wir mit MAGMA die Gröbnerbasis bezüglich der lexikographischen Termordnung von I [GP02, 1.6] :

```
R<t,a,b> := PolynomialRing(IntegerRing(), 3);
x := Matrix(2, [t,-1,1,0]);
```

```
y := Matrix(2, [1,a,b,1+a*b]);
M:= y^-2*x^-2*y*x - x^2*y^-1*x^-1*y;
I:=ideal< R |{ M[i,j] : i in [1..2], j in [1..2]} > ;
Groebner(I);
I;
```

$$
\begin{aligned}
I[1] &= t^2b^2 + t^2 + tb^3 + a^4b^4 - a^4 - 2a^3b^5 + 5a^3b^3 - a^3b + a^2b^6 - 8a^2b^4 + \\
&\quad 13a^2b^2 - 6a^2 + 2ab^5 - 16ab^3 + 12ab + b^6 + 3b^4 - 13b^2 - 4, \\
I[2] &= ta + tb^3 + a^4b^4 - a^4 - 2a^3b^5 + 5a^3b^3 - a^3b + a^2b^6 - 8a^2b^4 + 14a^2b^2 - \\
&\quad 5a^2 + 2ab^5 - 16ab^3 + 16ab + b^6 + 3b^4 - 12b^2 + 2, \\
I[3] &= tb^4 - t + a^4b^5 + a^4b^3 - 2a^3b^6 + 3a^3b^4 - a^3 + a^2b^7 - 7a^2b^5 + 9a^2b^3 - \\
&\quad 3a^2b + 2ab^6 - 14ab^4 + 8ab^2 - 5a + b^7 + 4b^5 - 6b^3 + 6b, \\
I[4] &= 2tb^2 + 2t + 2a^3b^2 + 2a^3 - 2a^2b^3 + 6a^2b - 6ab^2 + 10a - 2b^3 - 12b, \\
I[5] &= a^5b^2 + a^5 + a^4b^3 + 5a^4b - 5a^3b^4 + 5a^3 + 3a^2b^5 - 16a^2b^3 + 4a^2b + \\
&\quad 7ab^4 - 28ab^2 - a + 3b^5 + 15b^3 - 3b, \\
I[6] &= 2a^4b^2 + 2a^4 - 4a^3b^3 + 4a^3b + 2a^2b^4 - 12a^2b^2 + 10a^2 + 4ab^3 - 22ab + \\
&\quad 2b^4 + 10b^2 - 2.
\end{aligned}
$$

Als Nächstes suchen wir eine Teilmenge von $V_q(I)$, die besser zu verstehen ist.

Wir betrachten I als Ideal in dem Polynomring $\mathbb{Q}[t, a, b]$ und berechnen das Radikalideal von I. Dann wählen wir die Erzeuger des Radikalideals in $\mathbb{Z}[t, a, b]$ und definieren damit ein neues Ideal J in $\mathbb{Z}[t, a, b]$.

Weiter prüfen wir, dass $I \subseteq J$ ist. Das ist äquivalent zu $V_q(J) \subseteq V_q(I)$.

```
B:=Basis(I);
R1<t,a,b> := PolynomialRing(Rationals(), 3);
I1:=ideal<R1| { B[i] : i in [1..#B]} >;
RadicalDecomposition(I1);
```

Wir erhalten:

```
[
    Ideal of Polynomial ring of rank 3 over Rational Field
    Lexicographical Order
    Variables: t, a, b
    Dimension 1, Radical, Prime
    Groebner basis:
    [
        t*a - t*b + 1,
        t*b^2 + t + a^3*b^2 + a^3 - a^2*b^3 + 3*a^2*b - 3*a*b^2
              + 5*a - b^3 - 6*b,
        a^4*b^2 + a^4 - 2*a^3*b^3 + 2*a^3*b + a^2*b^4 - 6*a^2*b^2
```

```
            + 5*a^2 + 2*a*b^3 - 11*a*b + b^4 + 5*b^2 - 1
    ]
]
```

Hier definieren wir das ideal J und prüfen, dass $I \subseteq J$ gilt.

```
J:=ideal< R | t*a - t*b + 1,
              t*b^2 + t + a^3*b^2 + a^3 - a^2*b^3 + 3*a^2*b
              - 3*a*b^2 + 5*a - b^3 - 6*b,
              a^4*b^2 + a^4 - 2*a^3*b^3 + 2*a^3*b + a^2*b^4
              - 6*a^2*b^2 + 5*a^2 + 2*a*b^3 - 11*a*b + b^4
              + 5*b^2 - 1 >;
I subset J;   \\ true
```

Also setzen wir

$$\begin{aligned} J := \langle\ & (a-b)t + 1, \\ & (b^2+1)t + a^3b^2 + a^3 - a^2b^3 + 3a^2b - 3ab^2 + 5a - b^3 - 6b, \\ & a^4b^2 + a^4 - 2a^3b^3 + 2a^3b + a^2b^4 - 6a^2b^2 + 5a^2 + 2ab^3 - 11ab + b^4 + 5b^2 - 1\ \rangle. \end{aligned}$$

Wir bezeichnen die Erzeuger von J mit $J[1], J[2]$ und $J[3]$.

Es genügt, dass wir im Folgenden die Menge $V_q(J)$ betrachten. Wir wollen zeigen, dass die Teilmenge $V_q(J) \setminus V_q(I_0) \subseteq V_q(I) \setminus V_q(I_0)$ nicht leer ist.

Um den Beweis zu vereinfachen, zeigen wir, dass $V_q(J) \setminus V_q(I_0) = V_q(J)$.

Hilfssatz 4.2. *Für alle q gilt: $V_q(J) \cap V_q(I_0) = \emptyset$.*

Beweis. Angenommen, es gibt ein $(t, a, b) \in V_q(J) \cap V_q(I_0)$. Weil $(t, a, b) \in V_q(I_0)$ ist, gilt $a = -t,\ a = -b$ und $2 = 0$. Insbesondere $V_q(I_0) = \emptyset$ für $p \neq 2$.

Falls $p = 2$, so gilt $a = -b = b$. Eingesetzt in die erste Gleichung von J ergibt sich $(a-b)t + 1 = 1 \in J \cap I_0$, damit ist $V_q(J) \cap V_q(I_0) = \emptyset$. □

Wir wollen zeigen, dass die wesentliche Bedingung für die Existenz eines Elements in $V_q(J)$ durch $J[3]$ gegeben ist, weil die Variable t in $J[1]$ und $J[2]$ linear vorkommt und $J[1]$ und $J[2]$ modulo $J[3]$ die gleiche Gleichung ergeben. Wenn $J[3]$ genug Nullstellen (a, b) hat, existiert somit ein t mit $(t, a, b) \in V_q(J)$.

Hilfssatz 4.3. *Sei*

$$f := J[3] = a^4b^2 + a^4 - 2a^3b^3 + 2a^3b + a^2b^4 - 6a^2b^2 + 5a^2 + 2ab^3 - 11ab + b^4 + 5b^2 - 1.$$

Es gilt für alle q: Ist $|V_q(f)| \geq 7$, dann ist $V_q(J) \neq \emptyset$.

Beweis. Sei $(a,b) \in \mathbb{F}_q^2$ mit $f(a,b) = 0$.

Wir werden zuerst zeigen, dass wenn $a \neq b$ und $b^2 \neq -1$ gilt, so können wir ein t mit $(t,a,b) \in V_q(J)$ finden. Dann zeigen wir, dass es höchstens sechs Punkte $(a,b) \in V_q(f)$ mit der Eigenschaft $a = b$ oder $b^2 = -1$ geben kann.

1. Fall: Gilt $a \neq b$ und $b^2 \neq -1$, so erhalten wir

$$t = \frac{1}{b-a}$$

aus $J[1]$ oder

$$t = \frac{a^3b^2 + a^3 - a^2b^3 + 3a^2b - 3ab^2 + 5a - b^3 - 6b}{-b^2 - 1}$$

aus $J[2]$. Zu zeigen bleibt, dass

$$\frac{1}{b-a} = \frac{a^3b^2 + a^3 - a^2b^3 + 3a^2b - 3ab^2 + 5a - b^3 - 6b}{-b^2 - 1}, \text{ also}$$

$$-b^2 - 1 = (b-a)(a^3b^2 + a^3 - a^2b^3 + 3a^2b - 3ab^2 + 5a - b^3 - 6b)$$

gilt. Dafür berechnen wir:

$$\begin{aligned}
& -b^2 - 1 - (b-a)(a^3b^2 + a^3 - a^2b^3 + 3a^2b - 3ab^2 + 5a - b^3 - 6b) \\
= \; & -b^2 - 1 - a^3b^3 - a^3b + a^2b^4 - 3a^2b^2 + 3ab^3 - 5ab + b^4 + 6b^2 + a^4b^2 + a^4 \\
& -a^3b^3 + 3a^3b - 3a^2b^2 + 5a^2 - ab^3 - 6ab \\
= \; & a^4b^2 + a^4 - 2a^3b^3 + 2a^3b + a^2b^4 - 6a^2b^2 + 5a^2 + 2ab^3 - 11ab + b^4 + 5b^2 - 1 \\
= \; & f(a,b) = 0.
\end{aligned}$$

Also ist $(t,a,b) \in V_q(J)$.

2. Fall: Gilt $b^2 = -1$, dann ist

$$\begin{aligned}
f(a,b) &= -a^4 + a^4 + 2a^3b + 2a^3b + a^2 + 6a^2 + 5a^2 - 2ab - 11ab + 1 - 5 - 1 \\
&= 4a^3b + 12a^2 - 13ab - 5.
\end{aligned}$$

Es gibt höchstens zwei Möglichkeiten für b und zu festem b höchstens drei Möglichkeiten für a. Insgesamt sind das maximal sechs solche (a,b).

3. Fall: Gilt $a = b$, dann ist

$$\begin{aligned}
f(a,b) &= a^6 + a^4 - 2a^6 + 2a^4 + a^6 - 6a^4 + 5a^2 + 2a^4 - 11a^2 + a^4 + 5a^2 - 1 \\
&= -a^2 - 1 \\
&= -b^2 - 1.
\end{aligned}$$

Das sind Punkte (a,b), die schon im 2. Fall vorkommen.

Insgesamt gibt es höchstens sechs Nullstellen von $f(a,b)$, für die $b^2 = -1$ oder $a = b$ gilt. Wenn wir sieben Nullstellen von f finden, können wir nach dem 1. Fall einen Punkt in $V_q(J)$ bestimmen. □

Im Folgenden wollen wir zeigen, dass $|V_q(f)| \geq 7$ für alle q.

$V_q(f)$ ist eine Kurve in dem zweidimensionalen affinen Raum mit Koordinaten a und b. Wir können die Anzahl der Punkte in $\mathbb{F}_q$ wie in [BGGKPP] mit der Hasse–Weil Formel für singuläre Kurven abschätzen.

Lemma 4.4. *[FJ86, 3.14] Sei $C \subseteq \mathbb{P}^n$ eine absolut irreduzible projektive Kurve über $\mathbb{F}_q$ und N_q die Anzahl der rationalen Punkte von C. Dann gilt:*

$$N_q \geq (q+1) - 2p_a\sqrt{q},$$

wobei p_a das arithmetische Geschlecht von C ist.

Für das Lemma brauchen wir eine absolut irreduzible projektive Kurve. Wir bilden daher den projektiven Abschluss von $V_q(f)$ und beachten dabei, wieviele Punkte dazugekommen sind.

Bezeichnung 4.5. Sei C_q der projektive Abschluss von $V_q(f)$ in $\mathbb{P}^2(\mathbb{F}_q)$. Also

$$C_q = \{(h : a : b) \in \mathbb{P}^2(\mathbb{F}_q) \mid F(h,a,b) = 0\}, \text{ wobei}$$

$$\begin{aligned} F(h,a,b) = \quad & -h^6 + 5h^4a^2 - 11h^4ab + 5h^4b^2 + h^2a^4 + 2h^2a^3b - 6h^2a^2b^2 + \\ & 2h^2ab^3 + h^2b^4 + a^4b^2 - 2a^3b^3 + a^2b^4. \end{aligned}$$

die Homogenisierung von $f(a,b)$ ist.
Seien

$$U_0 = \{(1 : a : b) \in \mathbb{P}^2(\mathbb{F}_q)\},$$

$$U_1 = \{(h : 1 : b) \in \mathbb{P}^2(\mathbb{F}_q)\},$$

$$U_2 = \{(h : a : 1) \in \mathbb{P}^2(\mathbb{F}_q)\}$$

die affinen Überdeckungen von $\mathbb{P}^2(\mathbb{F}_q)$ und

$$H_\infty = \{(0 : a : b) \in \mathbb{P}^2(\mathbb{F}_q)\}$$

die unendlich ferne Hyperebene.

Bemerkung 4.6. C_q hat genau drei Punkte auf H_∞ , denn

$$C_q \cap H_\infty = V_q(a^4b^2 - 2a^3b^3 + a^2b^4) = V_q(a^2b^2(a-b)^2) = \{(0:0:1), (0:1:0), (0:1:1)\}$$

für alle q. Das bedeutet, dass $|C_q| = |V_q(f)| + 3$ ist.

4.1 Die Irreduzibilität der Kurve C_q

Nun müssen wir zeigen, dass C_q absolut irreduzibel, also irreduzibel über dem algebraischen Abschluss von $\mathbb{F}_q$ ist.

Bezeichnung 4.7. Sei $\overline{\mathbb{F}}_q$ der algebraische Abschluss von $\mathbb{F}_q$, wir definieren

$$\overline{C}_q := \{(h : a : b) \in \mathbb{P}^2(\overline{\mathbb{F}}_q) \mid F(h, a, b) = 0\}.$$

Angenommen, die Kurve $\overline{C}_q$ hat eine Zerlegung

$$\overline{C}_q = R \cup S,$$

wobei

$$F(h, a, b) = r(h, a, b)s(h, a, b) \text{ mit } R = V(r(h, a, b)) \text{ und } S = V(s(h, a, b)),$$

so dass R und S keine gemeinsame Komponente haben.

Dann gilt nach dem Satz von Bezout [Ha77, 7.8]:

$$\sum_{j=1}^{t} i(R, S; P_j) = \deg(r) \cdot \deg(s),$$

dabei sind $R \cap S = \{P_1, \ldots, P_t\}$ die Schnittpunkte von R und S und $i(R, S; P_j)$ die Schnittmultiplizität [Ha77, I.5] von R und S in P_j.

Da $F = rs$ und $\deg F = \deg r + \deg s$, können wir für $\deg F = 6$ die Möglichkeiten für $\deg r \cdot \deg s$ bestimmen, also $\deg r \cdot \deg s \in \{1 \cdot 5,\ 2 \cdot 4,\ 3 \cdot 3\} = \{5, 8, 9\}$.

Wir werden alle Möglichkeiten für die Schnittmultiplizitäten $i(R, S; P_j)$ bestimmen und zeigen, dass $\sum i(R, S; P_j) \notin \{5, 8, 9\}$. Daraus folgt dann, dass es keine Zerlegung von $\overline{C}_q$ gibt.

Seien $\{Q_1, \ldots, Q_k\}$ die singulären Punkte von $\overline{C}_q$. Dann sind die Schnittpunkte $P_1, \ldots, P_t \in \{Q_1, \ldots, Q_k\}$.

Wir bestimmen die Singularitäten von $\overline{C}_q$ und deren Auflösungsgraphen. Die Schnittmultiplizität in einem Punkt P ist nach [Fu98, 12.4.2]

$$i(R, S; P) = \sum_{Q} m_Q(R) m_Q(S),$$

wobei Q die unendlich fernen Punkte [Ha77, V.3.9.1] von P durchläuft und m_Q deren Multiplizitäten [Ha77, I.5] sind. Daher können wir aus den Auflösungsgraphen alle möglichen Schnittmultiplizitäten zweier Komponenten ablesen.

Zuerst bestimmen wir die singulären Punkte von $\overline{C}_q$.

Hilfssatz 4.8. *Sei $q = p^k$ und $p \notin \{37, 143\}$. Dann hat $\overline{C}_q$ in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ genau die drei singulären Punkte*

$$Q_1 = (0:1:0),\ Q_2 = (0:1:1) \text{ und } Q_3 = (0:0:1).$$

Beweis. Wir suchen die Singularitäten in der affinen Karte $U_0 = \mathbb{P}^2(\overline{\mathbb{F}}_q) \setminus H_\infty$. In U_0 hat $\overline{C}_q$ die Gleichung $F(1, a, b) = f(a, b)$.

Wir bezeichnen mit

$$I_1 = \langle \frac{\partial f(a,b)}{\partial a}, \frac{\partial f(a,b)}{\partial b}, f(a,b) \rangle$$

sowohl das Ideal in $\mathbb{Z}[a, b]$ als auch das reduzierte Ideal in $\mathbb{F}_q[a, b]$.

```
R<h,a,b> := PolynomialRing(IntegerRing(), 3);
F:= -h^6 + 5*h^4*a^2 - 11*h^4*a*b + 5*h^4*b^2 + h^2*a^4
    + 2*h^2*a^3*b - 6*h^2*a^2*b^2 + 2*h^2*a*b^3 + h^2*b^4
    + a^4*b^2 - 2*a^3*b^3 + a^2*b^4;
a1:=hom<R -> R |1,a,b>;
F1:=a1(F);
I1:=ideal< R |Basis(JacobianIdeal(F1)) , F1>;
Groebner(I1);
I1;
```

$$\begin{aligned} I_1[1] &= a + 26b^3 + 10024b, \\ I_1[2] &= 2b^4 + 51b^2 + 866, \\ I_1[3] &= 74b^2 + 12580, \\ I_1[4] &= 15947. \end{aligned}$$

Da $15947 = 37 \cdot 143$ eine Einheit in $\mathbb{F}_q$ ist, gilt $1 \in I_1$. Schließlich wurden die Fälle $p = 37$ und $p = 143$ ausgeschlossen. Daraus folgt, dass $\overline{C}_q$ keine singulären Punkte aus $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ in U_0 hat, falls $p \notin \{37, 143\}$.

Weiter suchen wir die singulären Punkte von $\overline{C}_q$ in H_∞. Nach Bemerkung 4.6 ist

$$C_q \cap H_\infty = \{(0:0:1), (0:1:0), (0:1:1)\}.$$

Wir müssen überprüfen, dass diese Punkte singulär sind. Dafür bestimmen wir

die partiellen Ableitungen von F:

$$\begin{aligned}
\frac{\partial F(h,a,b)}{\partial h} &= -6h^5 + 20h^3a^2 - 44h^3ab + 20h^3b^2 + 2ha^4 + 4ha^3b - 12ha^2b^2 \\
&\quad +4hab^3 + 2hb^4 \\
\frac{\partial F(h,a,b)}{\partial a} &= 10h^4a - 11h^4b + 4h^2a^3 + 6h^2a^2b - 12h^2ab^2 + 2h^2b^3 + 4a^3b^2 \\
&\quad -6a^2b^3 + 2ab^4 \\
\frac{\partial F(h,a,b)}{\partial b} &= -11h^4a + 10h^4b + 2h^2a^3 - 12h^2a^2b + 6h^2ab^2 + 4h^2b^3 + 2a^4b \\
&\quad -6a^3b^2 + 4a^2b^3
\end{aligned}$$

Wenn wir die Punkte $(0,0,1), (0,1,0)$ und $(0,1,1)$ in diese Gleichungen einsetzen, erhalten wir 0. Damit sind alle drei Punkte singulär. □

Als Nächstes bestimmen wir die Auflösungen von $\overline{C}_q$ in den singulären Punkten. Die Definitionen von Auflösung, Auflösungsgraph etc., sowie die Erklärung zu dem Verfahren sind im [Ha77] und [dJP00] zu finden.

Hilfssatz 4.9. *Seien $q = p^k$, $p \neq 2$, $\overline{C}_q$ aus (4.7) und*

$$Q_1 = (0:1:0),\ Q_2 = (0:1:1),\ Q_3 = (0:0:1)$$

die singulären Punkte von $\overline{C}_q$. Angenommen, $\overline{C}_q = R \cup S$, so dass R und S keine gemeinsame Komponente haben. Dann gilt:

(1) $Q_1 = (0:1:0)$ hat den Auflösunggraph A_1 und $i(R,S;Q_1) \in \{0,1\}$,
(2) $Q_2 = (0:1:1)$ hat den Auflösunggraph A_3 und $i(R,S;Q_2) \in \{0,2\}$,
(3) $Q_3 = (0:0:1)$ hat den Auflösunggraph A_1 und $i(R,S;Q_3) \in \{0,1\}$.

Beweis. (1) Wir arbeiten auf der affinen Karte $U_1 = \{(h:1:b) \in \mathbb{P}^2(\overline{\mathbb{F}}_q)\}$, also $Q_1 = (0,0)$. Dort ist die Kurve $\overline{C}_q$ gegeben durch das Polynom

$$-h^6 + 5h^4 - 11h^4b + 5h^4b^2 + h^2 + 2h^2b - 6h^2b^2 + 2h^2b^3 + h^2b^4 + b^2 - 2b^3 + b^4.$$

Es hat die homogene Komponente vom kleinstem Grad $h^2 + b^2$. Es gilt

$$h^2 + b^2 = (h - \sqrt{-1}b)(h + \sqrt{-1}b).$$

Da $p \neq 2$ ist, hat die Kurve $\overline{C}_q$ in Q_1 zwei verschiedene Tangenten, also ist Q_1 ein gewöhnlicher Doppelpunkt. Damit schneiden sich bei Q_1 zwei Zweige von $\overline{C}_q$ transversal, also $i(R,S;Q_1) = 0$, falls beide Zweige R oder S angehören, oder $i(R,S;Q_1) = 1$ sonst.

(2) Wir betrachten den Punkt $Q_2 = (0,1)$ in U_1. Zuerst führen wir eine Koordinatentransformation durch, indem wir den Punkt $(0,1)$ auf $(0,0)$ verschieben. Das geschieht, indem wir die Variable b in $\mathbb{F}_q[h,b]$ durch $b+1$ ersetzen.

Sei $C := \overline{C}_q \cap U_1$.

$$C = V(-h^6 + 5h^4b^2 - h^4b - h^4 + h^2b^4 + 6h^2b^3 + 6h^2b^2 + b^4 + 2b^3 + b^2).$$

Das Polynom hat die homogene Komponente vom kleinsten Grad

$$b^2 = b \cdot b,$$

damit hat C zwei gleiche Tangenten.

Wir blasen C auf durch die Variablensubstitution $h \mapsto h, b \mapsto hb$. Dann ist die strikte Transformierte von C gleich

$$C^{(1)} = V(b^4h^4 + b^4h^2 + 6b^3h^3 + 2b^3h + 5b^2h^4 + 6b^2h^2 + b^2 - bh^3 - h^4 - h^2),$$

der exzeptionelle Divisor ist $E^{(1)} = V(h)$ und $Q_2^{(1)} = E^{(1)} \cap C^{(1)} = (0,0)$. Die homogene Komponente vom kleinsten Grad ist

$$b^2 - h^2 = (b+h)(b-h),$$

also hat die Kurve $C^{(1)}$ in $(0,0)$ zwei verschiedene Tangenten. Der Punkt $(0,0)$ ist ein gewöhnlicher Doppelpunkt von $C^{(1)}$, damit hat C in Q_2 hat den Auflösunggraph A_3.

Bei Q_2 schneiden sich zwei Zweige von $\overline{C}_q$. Falls beide Zweige R oder S angehören, gilt $i(R,S;Q_2) = 0$.

Betrachten wir den Fall, dass die beiden Zweige verschiedenen Komponenten anliegen, also $Q_2 \in R \cap S$. Auf Grund von

$$2 = m_{Q_2}(\overline{C}_q) = m_{Q_2}(R \cap S) = m_{Q_2}(R) + m_{Q_2}(S)$$

und $m_{Q_2}(R)$, $m_{Q_2}(S) \geq 1$, folgt

$$m_{Q_2}(R) = m_{Q_2}(S) = 1,$$

d. h. die Komponenten R und S sind glatt in Q_2. Da beim Aufblasen Q_2 nur das eine Urbild $Q_2^{(1)}$ aus $C^{(1)}$ hat, gilt $Q_2^{(1)} \in R^{(1)} \cap S^{(1)}$, wobei $R^{(1)}$ und $S^{(1)}$ die strikten Transformierten von R und S sind. Analog wie oben folgt

$$m_{Q_2^{(1)}}(R^{(1)}) = m_{Q_2^{(1)}}(S^{(1)}) = 1.$$

Da $Q_2^{(1)}$ ein gewöhnlicher Doppelpunkt von $C^{(1)}$ ist, werden sich die beiden Komponenten in einer weiteren Aufblasung nicht treffen. Daher gilt nach der Noetherschen Schnittpunktformel [Fu98, 12.4.2] in diesem Fall:

$$i(R,S;P) = m_{Q_2}(R)m_{Q_2}(S) + m_{Q_2^{(1)}}(R^{(1)})m_{Q_2^{(1)}}(S^{(1)}) = 1\cdot 1 + 1\cdot 1 = 2.$$

(3) Wir arbeiten auf der affinen Karte $U_2 = \{(h : a : 1) \in \mathbb{P}^2(\mathbb{F}_q)\}$, also $Q_3 = (0,0)$. Die Kurve $\overline{C}_q$ ist gegeben durch das Polynom

$$-h^6 + 5h^4a^2 - 11h^4a + 5h^4 + h^2a^4 + 2h^2a^3 - 6h^2a^2 + 2h^2a + h^2 + a^4 - 2a^3 + a^2.$$

Es hat die homogene Komponente vom kleinsten Grad

$$h^2 + a^2 = (h + \sqrt{-1}a)(h - \sqrt{-1}a).$$

Dann hat $\overline{C}_q$ in Q_3 zwei verschiedene Tangenten und Q_3 ist ein gewöhnlicher Doppelpunkt. Analog zum Fall Q_1 ist $i(R,S;Q_3) \in \{0,1\}$. □

Wie aus dem Beweis ersichtlich, müssen wir den Fall $p = 2$ getrennt betrachten.

Hilfssatz 4.10. *Sei $\overline{C}_{2^n}$ wie in (4.7) und*

$$Q_1 = (0:1:0),\ Q_2 = (0:1:1),\ Q_3 = (0:0:1)$$

die singulären Punkte von $\overline{C}_{2^n}$. Angenommen, $\overline{C}_{2^n} = R \cup S$, so dass R und S keine gemeinsame Komponente haben. Dann gilt

(1) $Q_1 = (0:1:0)$ hat den Auflösunggraph A_4 und $i(R,S;Q_1) = 0$,
(2) $Q_2 = (0:1:1)$ hat den Auflösunggraph A_7 und $i(R,S;Q_2) \in \{0,4\}$,
(3) $Q_3 = (0:1:0)$ hat den Auflösunggraph A_4 und $i(R,S;Q_3) = 0$.

Beweis. $\overline{C}_{2^n} = V(h^6+h^4a^2+h^4ab+h^4b^2+h^2a^4+h^2b^4+a^4b^2+a^2b^4) \subseteq \mathbb{P}^2(\overline{\mathbb{F}}_{2^n})$.
(1) Wir arbeiten auf der affinen Karte U_1, also $Q_1 = (0,0)$. Sei $C := \overline{C}_{2^n} \cap U_1$. Dann ist C gegeben durch das Polynom

$$h^6 + h^4 + h^4b + h^4b^2 + h^2 + h^2b^4 + b^2 + b^4.$$

Es hat die homogene Komponente vom kleinsten Grad $h^2 + b^2$. In $\overline{\mathbb{F}}_2$ zerfällt dieses Polynom in zwei gleiche Linearfaktoren

$$h^2 + b^2 = (h + b)^2,$$

also hat C in $(0,0)$ zwei gleiche Tangenten.

Wir blasen auf durch die Variablensubstitution $h \mapsto h, b \mapsto hb$. Dann ist die strikte Transformierte von C gleich

$$C^{(1)} = V(h^4 + h^2 + h^3b + h^4b^2 + 1 + h^4b^4 + b^2 + h^2b^4),$$

der exzeptionelle Divisor ist $E^{(1)} = V(h)$ und $E^{(1)} \cap C^{(1)} = (0, 1)$.

Nach der Transformation von $(0, 1)$ auf $(0, 0)$ ist

$$C^{(1)} = V(h^2b^4 + h^3b + h^4b^2 + b^2 + h^4 + h^3 + h^4b^4).$$

Das Polynom hat die homogene Komponente vom kleinsten Grad b^2. Also hat $C^{(1)}$ in $(0, 0)$ zwei gleiche Tangenten.

Mit der zweiten Aufblasung $h \mapsto h, b \mapsto hb$ erhalten wir

$$C^{(2)} = V(h^4b^4 + h^2b + h^4b^2 + b^2 + h^2 + h + h^6b^4),$$

$E^{(2)} = V(h)$ und $E^{(2)} \cap C^{(2)} = (0, 0)$. Die Kurve $C^{(2)}$ ist glatt in $(0, 0)$.

Die Kurve $\overline{C}_q$ hat in Q_1 einen Zweig und den Auflösungsgraph A_4, also $i(R, S; Q_1) = 0$.

(2) Wir betrachten den Punkt $Q_2 = (0, 1)$ in U_1.

Nach der Transformation von $(0, 1)$ auf $(0, 0)$ ist

$$C = V(h^2b^4 + h^4b + h^4b^2 + b^4 + b^2 + h^6 + h^4).$$

Die homogene Komponente vom kleinsten Grad ist b^2, also C hat in $(0, 0)$ zwei gleiche Tangenten.

Wir blasen auf durch die Transformation $h \mapsto h, b \mapsto hb$. Dann ist

$$C^{(1)} = V(h^4b^4 + h^3b + h^4b^2 + h^2b^4 + b^2 + h^4 + h^2),$$

der exzeptionelle Divisor ist $E^{(1)} = V(h)$ und $Q_2^{(1)} := E^{(1)} \cap C^{(1)} = (0, 1)$.

Das Polynom hat die homogene Komponente vom kleinsten Grad

$$b^2 + h^2 = (b + h)^2,$$

und damit zwei gleiche Tangenten.

Mit der zweiten Aufblasung $h \mapsto hb, b \mapsto b$ erhalten wir die strikte Transformierte

$$C^{(2)} = V(h^4b^6 + h^3b^2 + h^4b^4 + h^2b^4 + 1 + h^4b^2 + h^2),$$

den exzeptionellen Divisor $E^{(2)} = V(b)$ und $Q_2^{(2)} := E^{(2)} \cap C^{(2)} = (1, 0)$.

Wir verschieben $(1,0)$ auf $(0,0)$ und erhalten

$$C^{(2)} = V(h^2b^4 + h^4b^6 + h^4b^2 + h^2b^2 + h^2 + b^6 + h^4b^4 + h^3b^2 + hb^2).$$

Das Polynom hat die homogene Komponente vom kleinsten Grad h^2, damit zwei gleiche Tangenten in $(0,0)$.

Die dritte Aufblasung $h \mapsto hb, b \mapsto b$ liefert die strikte Transformierte

$$C^{(3)} = V(h^2b^4 + h^4b^8 + h^4b^4 + h^2b^2 + h^2 + b^4 + h^4b^6 + h^3b^3 + hb),$$

den exzeptionellen Divisor $E^{(3)} = V(b)$ und $Q_2^{(3)} := E^{(3)} \cap C^{(3)} = (0,0)$. Das Polynom hat den Term vom kleinstem Grad

$$h^2 + hb = h(h+b),$$

damit hat $C^{(3)}$ zwei verschiedene Tangenten in $(0,0)$, insbesondere ist der Punkt $(0,0)$ ein gewöhnlicher Doppelpunkt von $C^{(3)}$.

Bei Q_2 schneiden sich zwei Zweige von $\overline{C}_{2^n}$. Falls beide Zweige R oder S angehören, gilt $i(R,S;Q_2) = 0$.

Wir betrachten den Fall, dass beide Zweige in verschiedenen Komponenten liegen. Die Multiplizitäten in den Punkten Q_2, $Q_2^{(1)}$, $Q_2^{(2)}$ und $Q_2^{(3)}$ sind alle gleich 2 und $Q_2^{(3)}$ ist ein gewöhnlicher Doppelpunkt. Wie im Fall 2 von dem Hilfssatz 4.9 folgt:

$$i(R,S;P) = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 = 4.$$

(3) Der Beweis für Q_3 ist analog zum dem Fall (1). □

Jetzt können wir beweisen, dass $\overline{C}_q$ irreduzibel ist.

Satz 4.11. *Falls $p \notin \{37, 143\}$, so ist die Kurve $\overline{C}_q$ irreduzibel und hat den Grad 6.*

Beweis. Zuerst bemerken wir, dass das Polynom F quadratfrei ist. Das ist erfüllt, denn nach dem Hilfssatz 4.8 wissen wir, dass die gemeinsamen Nullstellen von F und den Ableitungen von F drei Punkte sind und damit die Dimension 0 haben. Hätte F einen mehrfachen Faktor, so hätten F und die Ableitungen von F einen gemeinsamen Faktor, insbesondere hätte die gemeinsame Nullstellenmenge von F und den Ableitungen die Dimension 1.

Da F quadratfrei ist, hat C_q den Grad von F, nämlich 6.

Wir nehmen an, dass die Kurve $\overline{C}_q = V_q(F)$ nicht irreduzibel ist.

Dann können wir eine Zerlegung

$$\overline{C}_q = R \cup S$$

finden, wobei

$$F(h,a,b) = r(h,a,b)s(h,a,b),$$
$$R = V(r(h,a,b)) \text{ und } S = V(s(h,a,b)),$$

so dass R, S keine gemeinsame Komponente haben. Nach dem Satz von Bezout [Ha77, 7.8] gilt:

$$\sum_{j=1}^{t} i(R,S;P_j) = \deg(r) \cdot \deg(s),$$

wenn $R \cap S = \{P_1, \ldots, P_t\}$ die Schnittpunkte von R und S sind und $i(R,S;P_j)$ die Schnittmultiplizität in P_j ist. Aus $\deg(F) = 6$ folgt, dass

$$\sum_{j=1}^{t} i(R,S;P_j) = \deg(r) \cdot \deg(s) \in \{5,8,9\}.$$

Die Schnittpunkte $P_1, \ldots, P_t$ sind in der Menge $\{Q_1, \ldots, Q_k\}$ der singulären Punkte von $\overline{C}_q$ enthalten, also $\sum_{j=1}^{t} i(R,S;P_j) = \sum_{j=1}^{k} i(R,S;Q_j)$.

Nach Hilfssatz 4.9 ist

$$\sum_{j=1}^{3} i(R,S;Q_j) \in \{0,1,2,3,4\},$$

falls $q \neq 2^k$ und im Hilfssatz 4.10 haben wir gezeigt, dass

$$\sum_{j=1}^{3} i(R,S;Q_j) \in \{0,4\}$$

für $q = 2^k$.

Das ist ein Widerspruch, also ist $\overline{C}_q$ irreduzibel. □

4.2 Eine Abschätzung von $|C_q|$

Bemerkung 4.12. In dem Beweis von dem Satz 4.1 reicht es, die Primzahlpotenzen $q = 2^k$, $q = 3^k$ und $q = p$ für Primzahlen $p \geq 5$ zu betrachten.

Beweis. Da $\mathbb{F}_p$ ein Unterkörper von $\mathbb{F}_{p^k}$ ist, gilt $V_p(J) \subseteq V_{p^k}(J)$ für alle $k \in \mathbb{N}$. Für den Satz 4.1 war $q \geq 4$ vorausgesetzt. □

Satz 4.13. *Sind die Mengen $V_{37}(J)$ und $V_{143}(J)$ nicht leer, so ist $V_q(J) \neq \emptyset$ für $q \geq 419$.*

Beweis. Aus der Voraussetzung und Bemerkung 4.12 folgt, dass $V_q(J) \neq \emptyset$, wenn q eine Potenz von 37 oder 143 ist.

Sei jetzt $p \notin \{37, 143\}$. Im Hilfssatz 4.3 haben wir gezeigt, dass $V_q(J) \neq \emptyset$ gilt, wenn $|V_q(f)| \geq 7$ ist. Außerdem wissen wir nach Bemerkung 4.6, dass $|V_q(f)|+3 = |C_q|$. Nach Satz 4.11 ist die Kurve C_q absolut irreduzibel und vom Grad 6. Das arithmetische Geschlecht p_a von C_q berechnen wir mit der Formel [Ha77, I.7.2]:

$$p_a = \frac{(d-1)(d-2)}{2} = \frac{5 \cdot 4}{2} = 10,$$

wobei d der Grad von C_q ist. Nach der Hasse–Weyl Formel 4.4 gilt:

$$\begin{aligned} & |C_q| && \geq (q+1) - 2p_a\sqrt{q}, \text{ also} \\ |V_q(f)| = \; & |C_q| - 3 && \geq (q+1) - 2 \cdot 10\sqrt{q} - 3. \end{aligned}$$

Durch das Einsetzen von $q = 419$ erhalten wir, dass

$$(419+1) - 20\sqrt{419} - 3 \approx 7.6$$

ist. Aus der Monotonie der Funktion $(q+1) - 20\sqrt{q} - 3$ folgt, dass

$$(q+1) - 20\sqrt{q} - 3 \geq 7,$$

wenn $q \geq 419$ ist. □

Satz 4.14. *$V_q(J) \neq \emptyset$ für $4 \leq q < 419$ und $q \neq 8$.*

Beweis. Wir berechnen mit MAGMA $|V_q(f)|$ für die Primzahlen $5 \leq p < 419$ sowie für die Primzahlpotenzen $4 \leq 2^k < 419$ und $9 \leq 3^k < 419$.

```
for p in [1..419] do
 if IsPrime(p) eq true then
 M:={ <a,b> : a,b in GF(p) |
      a^4*b^2 + a^4 - 2*a^3*b^3 + 2*a^3*b + a^2*b^4 - 6*a^2*b^2
      + 5*a^2 + 2*a*b^3 - 11*a*b + b^4 + 5*b^2 - 1 eq 0};
 print p, #M;
 end if;
end for;
```

p	$\lvert V_p(f)\rvert$	p	$\lvert V_p(f)\rvert$	p	$\lvert V_p(f)\rvert$	p	$\lvert V_p(f)\rvert$	p	$\lvert V_p(f)\rvert$
2	1	61	64	149	154	239	246	347	342
3	0	67	56	151	140	241	258	349	352
5	14	71	90	157	186	251	238	353	418
7	8	73	70	163	176	257	352	359	402
11	12	79	84	167	140	263	264	367	334
13	22	83	68	173	146	269	246	373	360
17	20	89	78	179	162	271	274	379	334
19	28	97	110	181	214	277	270	383	354
23	4	101	100	191	242	281	314	389	402
29	42	103	108	193	188	283	288	397	346
31	24	107	110	197	198	293	290	401	456
37	38	109	104	199	156	307	334	409	456
41	56	113	128	211	218	311	372	419	464
43	40	127	116	223	244	313	392		
47	36	131	100	227	208	317	376		
53	42	137	132	229	186	331	334		
59	56	139	172	233	254	337	288		

q	$\lvert V_q(f)\rvert$	q	$\lvert V_q(f)\rvert$
2^2	5	3^2	26
2^3	1	3^3	42
2^4	13	3^4	66
2^5	21	3^5	180
2^6	77		
2^7	141		
2^8	189		

Ist $|V(f)| \geq 7$, so ist nach dem Hilfssatz 4.3 die Menge $V(J)$ nicht leer.

Für $q \in \{4, 8, 23\}$ ist $|V(f)| < 7$. Eine MAGMA Rechnung ergibt, dass

$$\begin{aligned} V_4(f) &= \{(\omega+1, 0), (0, \omega+1), (\omega, 0), (1, 1), (0, \omega)\} \text{ und} \\ V_{23}(f) &= \{(0, 16), (7, 0), (0, 7), (16, 0)\}, \end{aligned}$$

wenn $\mathbb{F}_4 = \{0, 1, \omega, \omega+1\}$ ist. Die beiden Mengen enthalten Elemente (a, b) mit $a \neq b$ und $b^2 \neq -1$. Nach dem Fall 1 im Hilfssatz 4.3 finden wir ein t, sodass $(t, a, b) \in V_q(J)$ ist.

Also ist die Menge $V_q(J)$ nicht leer für $4 \leq q < 419$ und $q \neq 8$. □

Bemerkung 4.15. Im Fall $q = 8$ ist die Menge $V_8(f) = \{(1, 1)\}$, also können wir daraus keine Punkte aus $V_8(J)$ konstruieren. Das bedeutet aber nicht, dass

die Menge der Lösungen von $v_1 = v_2$ und $v_1 \neq 1$ in $\mathrm{PSL}(2, \mathbb{F}_8)$ leer ist, da wir mit der Wahl von $x(t)$ und $y(a, b)$ diese Menge eingeschränkt haben. Mit dem folgenden MAGMA Programm erhalten wir, dass es genau 3024 Paare $(x, y) \in PSL(2, \mathbb{F}_8)^2$ gibt mit $v_1(x, y) = v_2(x, y)$ und $v_1(x, y) \neq 1$.

```
G:=PSL(2,8);
M:={ <x,y> : x,y in G |
     ((y*x^2)^(y^-1* x^-1),(y*x^2)^(x^-1)) eq y*x^2 eq true
     and y*x^2 ne G!1 eq true };
#M;
```

Beweis von Satz 4.1. Im Satz 4.14 haben wir gezeigt, dass die Mengen $V_{37}(J)$ und $V_{143}(J)$ nicht leer sind. Dann ist nach Satz 4.13 die Menge $V_q(J)$ nicht leer für alle Primzahlpotenzen $q \geq 419$. Also ist $V(J)$ nicht leer für alle Primzahlpotenzen $q \geq 4$ und $q \neq 8$. Zusammen mit der Bemerkung 4.15 folgt die Behauptung. □

Kapitel 5

Beweis für Suzuki Gruppen

In diesem Kapitel werden einige Computerberechnungen mit dem Computeralgebra System SINGULAR [GP02] statt MAGMA durchgeführt. Für die Beweise müssen wir die Gröbnerbasen von Idealen mit 8 Variablen und 529 erzeugenden Elementen berechnen. Diese Berechnungen sind für die lexikographische Termordnung `lp` zu aufwendig. Stattdessen benutzen wir die Produkttermordnung in SINGULAR, bei der den ersten der Variablen die lexikographische Termordnung zugewiesen wird und den restlichen die graduierte reverse lexikographische Termordnung `dp` [GP02, 1.2]. Das verringert die Rechenzeit erheblich.

In diesem Kapitel beweisen wir den folgenden Satz:

Satz 5.1. *Sei*

$$v_1 = yx^2 \text{ und } v_2 = [(yx^2)^{y^{-1}x^{-1}}, (yx^2)^{x^{-1}}].$$

Für jedes ungerade n existieren Elemente $x, y \in \mathrm{Sz}(2^n)$, so dass $v_1(x,y) \neq 1$ und $v_1(x,y) = v_2(x,y)$ gilt.

Die Suzuki Gruppen $\mathrm{Sz}(2^n)$ haben wir im Kapitel 1 definiert. Der Automorphismus $\theta : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ war definiert durch $\theta(a) = a^{2^{m+1}}$, wobei $n = 2m + 1$.

Wir erinnern an einige bekannte Eigenschaften der Suzuki Gruppen [HB82, 3], [BWW05]:

(1) $|\mathrm{Sz}(2^n)| = 2^{2n}(2^n - 1)(2^{2n} + 1)$,

(2) $\mathrm{Sz}(2^n)$ ist einfach,

(3) $S(a,b)S(c,d) = S(a + c, b + d + \theta(a)c)$,

(4) $\langle S(a,b) \mid a, b \in \mathbb{F}_{2^n} \rangle$ ist eine Untergruppe von $\mathrm{Sz}(2^n)$ mit q^{2n} Elementen, hat den Exponent 4 und ist von der Nilpotenzklasse 2,

(5) $\langle M(\lambda) \mid \lambda \in \mathbb{F}_{2^n}^* \rangle \simeq \mathbb{F}_{2^n}^*$,

(6) $S(a,b)^{M(\lambda)} = S(\lambda a, \lambda\theta(\lambda)b)$,

(7) $\langle S(a,b), M(\lambda) \mid a,b,\lambda \in \mathbb{F}_{2^n}, \lambda \neq 0 \rangle$ ist eine auflösbare Untergruppe von $\mathrm{Sz}(2^n)$ mit der Auflösungslänge 4,

(8) Jedes $g \in \mathrm{Sz}(2^n)$ hat eine eindeutige Darstellung als entweder $g = S(a,b)M(\lambda)$ oder $g = S(c,d)^{-1}S(a,b)M(\lambda)TS(c,d)$ für $a,b,c,d,\lambda \in \mathbb{F}_{2^n}, \lambda \neq 0$.

Die Eigenschaft (8) zeigt, dass wir für x und y entweder Matrizen der Gestalt $S(a,b)M(\lambda)$ oder $S(c,d)^{-1}S(a,b)M(\lambda)TS(c,d)$ wählen können. Dabei dürfen x und y nicht beide von der Form $S(a,b)M(\lambda)$ sein, weil sie dann in der auflösbaren Untergruppe $\langle S(a,b), M(\lambda) \mid a,b,\lambda \in \mathbb{F}_{2^n}, \lambda \neq 0 \rangle$ wären.

Nun wählen wir möglichst einfache x und y, setzen für die Variablen Elemente aus $\mathbb{F}_{2^n}$ ein und berechnen mit MAGMA inwiefern sie die Gleichung $v_1(x,y) = v_2(x,y)$ erfüllen.

x	y	Anzahl der $(a,b,c,d) \in \mathbb{F}_{2^n}^4$ mit $v_1(x,y) = v_2(x,y)$	
		$n=3$	$n=5$
$S(a,b)T$	$S(c,d)T$	0	0
$S(a,b)$	$S(c,d)T$	0	0
$S(a,b)T$	$S(c,d)$	13	21
$TS(a,b)$	$TS(c,d)$	0	0
$S(a,b)$	$TS(c,d)$	0	0
$TS(a,b)$	$S(c,d)$	13	21
$TS(a,b)$	$S(c,d)T$	0	0
$S(a,b)T$	$TS(c,d)$	0	0

Für $x = S(a,b)T$ und $y = S(c,d)$ gibt es auch Lösungen der Gleichung $v_1(x,y) = v_2(x,y)$ in $\mathrm{Sz}(2^7), \mathrm{Sz}(2^9)$ und $\mathrm{Sz}(2^{11})$.

Für den Beweis von Satz 5.1 machen wir den Ansatz

$$x := S(a,b)T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & a \\ 0 & 1 & \theta(a) & a\theta(a)+b \\ 1 & a & b & a^2\theta(a)+ab+\theta(b) \end{pmatrix}$$

und

$$y := S(c,d) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ c & 1 & 0 & 0 \\ c\theta(c)+d & \theta(c) & 1 & 0 \\ c^2\theta(c)+cd+\theta(d) & d & c & 1 \end{pmatrix},$$

dies sind invertierbare Matrizen mit Einträgen aus dem Polynomring $\mathbb{F}_2[a,b,c,d]$.

Sei $n = 2m+1$. Als Erstes prüfen wir, für welche $a,b,c,d \in \mathbb{F}_{2^n}$ die Gleichung $v_1(x,y) = 1$ gilt.

Hilfssatz 5.2. *Für $x = S(a,b)T$ und $y = S(c,d)$ aus $\mathrm{Sz}(2^n)$ gilt $v_1(x,y) = 1$ genau dann, wenn $a = b = c = d = 0$.*

Beweis. Wenn wir $x = S(a,b)T$ und $y = S(c,d)$ in $v_1(x,y) = 1$ einsetzen, erhalten wir 16 Polynomiale Gleichungen in a,b,c,d, abhängig von m. Wir bezeichnen diese mit n_{ij}, also

$$\begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} \\ n_{21} & n_{22} & n_{23} & n_{24} \\ n_{31} & n_{32} & n_{33} & n_{34} \\ n_{41} & n_{42} & n_{43} & n_{44} \end{pmatrix} := v_1(x,y) - 1.$$

Wir geben einige Werte von n_{ij} an:

$$\begin{aligned} n_{12} &= a, \\ n_{13} &= b, \\ n_{21} &= a + c, \\ n_{31} &= a^{1+2^{m+1}} + ac^{2^{m+1}} + c^{1+2^{m+1}} + b + d, \end{aligned}$$

Aus $n_{12} = 0$ und $n_{13} = 0$ folgt $a = b = 0$. Aus $n_{21} = 0 + c = 0$ folgt $c = 0$. Aus $n_{31} = 0 + d = 0$ folgt $d = 0$.

Andererseits ist $S(0,0)S(0,0)TS(0,0)T = T^2 = 1$. □

Die gewählten $x(a,b)$ und $y(c,d)$ sind von $n = 2m+1$ abhängig, weil dieses in den Einträgen $\theta(a) = a^{2^{m+1}}$ (bzw. $\theta(b), \theta(c), \theta(d)$) vorkommt. Deshalb ersetzen wir $\theta(a), \theta(b), \theta(c), \theta(d)$ durch neue Variablen a_0, b_0, c_0, d_0. Damit sind

$$x(a,b,a_0,b_0) := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & a \\ 0 & 1 & a_0 & aa_0+b \\ 1 & a & b & a^2a_0+ab+b_0 \end{pmatrix} \text{ und}$$

$$y(c,d,c_0,d_0) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ c & 1 & 0 & 0 \\ cc_0+d & c_0 & 1 & 0 \\ c^2c_0+cd+d_0 & d & c & 1 \end{pmatrix}$$

Matrizen mit Einträgen im Ring $R := \mathbb{F}_2[a,b,c,d,a_0,b_0,c_0,d_0]$.

Die Gleichung $v_1 = v_2$ ist äquivalent zu $y^{-2}x^{-2}yx = x^2y^{-1}x^{-1}y$. Wir berechnen

$$y^{-2}x^{-2}yx - x^2y^{-1}x^{-1}y$$

für $x = x(a,b,a_0,b_0)$, $y = y(c,d,c_0,d_0)$ und erhalten eine 4×4-Matrix mit Einträgen in R, die wir mit

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$$

bezeichnen. Weiter definieren wir

$$J := \langle m_{11}, m_{12} \ldots, m_{44} \rangle$$

als das von den 16 Einträgen dieser Matrix erzeugte Ideal in R.

Sei $\overline{\mathbb{F}}_2$ der algebraische Abschluss von $\mathbb{F}_2$ und $\mathbb{A}^8 := \mathbb{A}^8(\overline{\mathbb{F}}_2)$ der affine Raum über $\overline{\mathbb{F}}_2$ mit den Koordinaten a,b,c,d,a_0,b_0,c_0,d_0. Wir betrachten die Nullstellenmenge

$$V(J) := \{(a,b,c,d,a_0,b_0,c_0,d_0) \in \mathbb{A}^8 \mid p(a,b,c,d,a_0,b_0,c_0,d_0) = 0 \; \forall p \in J\}.$$

Jeder Punkt $(a,b,c,d,a_0,b_0,c_0,d_0) \in V(J)$ entspricht Matrizen $x = x(a,b,a_0,b_0)$ und $y = y(c,d,c_0,d_0)$, die

$$v_1(x,y) = v_2(x,y)$$

erfüllen. Allerdings, müssen diese x und y im Allgemeinem keine Elemente von $\mathrm{Sz}(2^n)$ sein, weil die Abhängigkeit der Variablen a_0 von a und analog für b_0, c_0 und d_0 nicht erfüllt sein muss.

Um solche Punkte $(a,b,c,d,a_0,b_0,c_0,d_0)$ zu finden, für die auch $x(a,b,a_0,b_0)$, $y(c,d,c_0,d_0) \in \mathrm{Sz}(2^n)$ gilt, benötigen wir folgende Hilfsmittel (vgl. [BGGKPP]).

Sei $\pi : R \to R$ der Endomorphismus, definiert durch

$$\begin{array}{llll} \pi(a) = a_0, & \pi(b) = b_0, & \pi(c) = c_0, & \pi(d) = d_0, \\ \pi(a_0) = a^2, & \pi(b_0) = b^2, & \pi(c_0) = c^2, & \pi(d_0) = d^2. \end{array}$$

Der Endomorphismus π liefert einen bijektiven Morphismus $\alpha : \mathbb{A}^8 \to \mathbb{A}^8$, definiert durch:

$$\alpha(a, b, c, d, a_0, b_0, c_0, d_0) = (a_0, b_0, c_0, d_0, a^2, b^2, c^2, d^2).$$

Zunächst fassen wir einige Eigenschaften von α zusammen.

Bemerkungen 5.3.

(1) $\alpha^2(a, b, c, d, a_0, b_0, c_0, d_0) = (a^2, b^2, c^2, d^2, a_0^2, b_0^2, c_0^2, d_0^2)$, also ist α eine Quadratwurzel des Frobenius–Automorphismus,

(2) $\alpha^{2m}(a, b, c, d, a_0, b_0, c_0, d_0) = (a^{2^m}, b^{2^m}, c^{2^m}, d^{2^m}, a_0^{2^m}, b_0^{2^m}, c_0^{2^m}, d_0^{2^m})$,

(3) $\alpha^{2m+1}(a, b, c, d, a_0, b_0, c_0, d_0) = (a_0^{2^m}, b_0^{2^m}, c_0^{2^m}, d_0^{2^m}, a^{2^{m+1}}, b^{2^{m+1}}, c^{2^{m+1}}, d^{2^{m+1}})$.

Die Fixpunkte von α^n auf $V(J)$ für ungerade n liefern uns die gesuchten $x(a, b, a_0, b_0),\ y(c, d, c_0, d_0) \in \mathrm{Sz}(2^n)$. Das zeigen wir in dem folgenden Satz:

Satz 5.4. *[BGGKPP] Wenn die Abbildung α^n (n ungerade) mehr als einen Fixpunkt auf $V(J)$ hat, so gibt es $x(a, b), y(c, d) \in \mathrm{Sz}(2^n)$, so dass $v_1(x(a, b), y(c, d)) = v_2(x(a, b), y(c, d))$ erfüllt ist.*

Beweis. [BGGKPP] Sei $(a, b, c, d, a_0, b_0, c_0, d_0) \in V(J)$ ein Fixpunkt von α^{2m+1}. Da $(a, b, c, d, a_0, b_0, c_0, d_0) \in V(J)$, gilt

$$v_1(x(a, b, a_0, b_0), y(c, d, c_0, d_0)) = v_2(x(a, b, a_0, b_0), y(c, d, c_0, d_0)).$$

Weil $(a, b, c, d, a_0, b_0, c_0, d_0)$ Fixpunkt ist, folgt $a = a_0^{2^m}, a_0 = a^{2^{m+1}}$, also $a = a^{2^{2m+1}} = a^{2^n}$. Dann gilt $a \in \mathbb{F}_{2^n}$ und $a_0 = a^{2^{m+1}} = \theta(a)$. Dasselbe gilt für b, c und d. Damit liegen $x(a, b, a_0, b_0), y(c, d, c_0, d_0)$ in $\mathrm{Sz}(2^n)$. □

Wir müssen zeigen, dass α^n für alle ungeraden natürlichen Zahlen n mehr als einen Fixpunkt auf $V(J)$ hat. Dafür benutzen wir die Lefschetz–Fixpunktformel in Form des folgenden Satzes:

Satz 5.5. *[BGGKPP, 3.6] Seien $n = 2m + 1$ und U eine nichtsinguläre, α–invariante, irreduzible Teilmenge von $\mathbb{A}^8$ der Dimension 2.*

Sei $\mathrm{Fix}(U, n)$ die Menge der Fixpunkte von α^n auf U, die Menge $\overline{\mathrm{Fix}(U, n)}$ der projektive Abschluss von $\mathrm{Fix}(U, n)$ in $\mathbb{P}^8(\overline{\mathbb{F}}_2)$ und es gelte

$$|\overline{\mathrm{Fix}(U, n)}| = |\mathrm{Fix}(U, n)|.$$

Dann gilt:

$$|\mathrm{Fix}(U, n)| \geq 2^n - b^1(U)2^{3n/4} - b^2(U)2^{n/2},$$

wobei $b^i(U) = \dim H^i_{et}(U, \mathbb{Q}_\ell)$ die ℓ-adischen Betti–Zahlen sind. ($\ell \neq 2$).

Wir wollen eine nichtsinguläre, α–invariante, irreduzible Teilmenge U von $V(J)$ finden, die alle Voraussetzungen des Satzes 5.5 erfüllt. Für diese werden wir dann die Betti–Zahlen abschätzen und damit folgern, dass eine natürliche Zahl k existiert, so dass $|\operatorname{Fix}(U,n)| > 1$ für alle $n \geq k$ gilt. Für die $3 \leq n < k$ finden wir die Fixpunkte von α^n auf $V(J)$ unmittelbar mit dem Computer.

Um eine α–invariante, irreduzible Teilmenge U von $V(J)$ zu finden, untersuchen wir $V(J)$ genauer. Wir berechnen eine Basis von J und die Dimension mit SINGULAR:

```
ring R = 2, (d0,d,c0,c,b0,b,a0,a), dp;
option(redSB);
option(prot);
LIB"linalg.lib";

matrix S1[4][4] = 1,             0,  0, 0,
                  a,             1,  0, 0,
                  a*a0+b,        a0, 1, 0,
                  a^2*a0+a*b+b0, b,  a, 1;

matrix S2[4][4] = 1,             0,  0, 0,
                  c,             1,  0, 0,
                  c*c0+d,        c0, 1, 0,
                  c^2*c0+c*d+d0, d,  c, 1;

matrix T[4][4] = 0, 0, 0, 1,
                 0, 0, 1, 0,
                 0, 1, 0, 0,
                 1, 0, 0, 0;

matrix x=S1*T;
matrix y=S2;
matrix ix = inverse(x);
matrix iy = inverse(y);

matrix M = iy*iy*ix*ix*y*x - x*x*iy*ix*y;
ideal J = flatten(M);
dim(std(J));
2
```

Die Anordnung der Variablen $(d_0, d, c_0, c, b_0, b, a_0, a)$ wurde so gewählt, um die Rechenzeit zu verkürzen.

Wir brauchen eine irreduzible Komponente von $V(J)$. Dafür entfernen wir zuerst die offensichtlichen Komponenten von $V(J)$, die in den Hyperebenen $V(a)$ und $V(a_0)$ liegen. Wir setzen

$$\begin{aligned} J_a &:= (J \cap \langle at-1 \rangle) \cap R \quad \subseteq R, \\ J_0 &:= (J_a \cap \langle a_0 t-1 \rangle) \cap R \quad \subseteq R, \end{aligned}$$

dabei betrachten wir die Ideale in $R[t]$.

Das zugehörige SINGULAR Programm:

```
ring Rt = 2, (d0,d,c0,c,b0,b,a0,a,t), dp;
ideal J = imap(R,J);

ideal Jt = std(J), a*t-1;
ideal Ja = eliminate(Jt,t);

ideal Jt = std(Ja), a0*t-1;
ideal Ja0 = eliminate(Jt,t);

ideal J0 = std(Ja0);
```

Dasselbe Verfahren haben wir auch auf die anderen Hyperebenen angewendet, dadurch veränderte sich das Ideal aber nicht.

Das Ideal $J_0 \supseteq J$ hat 529 Erzeugende bezüglich der graduierten reversen lexikographischen Termordnung `dp`. Im Folgenden betrachten wir die Teilmenge $V(J_0) \subseteq V(J)$.

Wir wollen später im Wesentlichen den Satz 5.5 auf die glatten Punkte von $V(J_0)$ anwenden, dafür zeigen wir zunächst, dass $V(J_0)$ α–invariant ist.

Hilfssatz 5.6. *$V(J_0)$ ist α–invariant.*

Beweis. Zu zeigen ist, dass $\alpha(V(J_0)) \subseteq V(J_0)$ ist, also $\pi(J_0) \subseteq J_0$. Das beweisen wir mit einer SINGULAR Rechnung.

```
setring R;
ideal J0 = imap(Rt,J0);
map pi = R, d^2,d0,c^2,c0,b^2,b0,a^2,a0;


ideal SJ0 = std(J0);
ideal SpiJ0 = std(pi(J0));

reduce(SpiJ0,SJ0); // dies ergibt 0
```

□

5.1 Eine irreduzible Teilmenge von $V(J_0)$

Hilfssatz 5.7. *Es gibt genau eine* 2*–dimensionale irreduzible Komponente* $V_0 \subseteq V(J_0) \subseteq \mathbb{A}^8$.

Beweis. Wir werden $V(J_0) \subseteq \mathbb{A}^8$ in den 3–dimensionalen affinen Raum $\mathbb{A}^3 := \mathbb{A}^3(\overline{\mathbb{F}}_2)$ mit den Koordinaten a, b und c projezieren. Diese Projektion nennen wir ϕ. Wir werden zeigen, dass das Bild $\phi(V(J_0)) \subseteq \mathbb{A}^3$ eine irreduzible Hyperfläche $V(j)$ ist, und dass es eine rationale Abbildung ψ von $V(j)$ nach $V(J_0) \subseteq \mathbb{A}^8$ gibt. Dann ist $V(j)$ birational zu $V_0 := \psi(V(j))$ und das Inverse von ψ wird durch ϕ gegeben. Schließlich argumentieren wir dafür, dass V_0 die einzige zweidimensionale irreduzible Komponente von $V(J_0)$ ist.

Wir zerlegen die Projektion in fünf Schritte $\phi = \phi_5 \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$ als

$$V(J_0) \supseteq (a,b,c,d,a_0,b_0,c_0,d_0) \xrightarrow{\phi_1} (a,b,c,d,a_0,b_0,c_0) \xrightarrow{\phi_2} (a,b,c,a_0,b_0,c_0) \xrightarrow{\phi_3}$$

$$(a,b,c,a_0,b_0) \xrightarrow{\phi_4} (a,b,c,a_0) \xrightarrow{\phi_5} (a,b,c).$$

Um die Bilder von ϕ_i zu finden, berechnen wir die folgenden Ideale:

$$\begin{aligned} J_1 &:= J \cap \mathbb{F}_2[a,b,c,d,a_0,b_0,c_0], \\ J_2 &:= J \cap \mathbb{F}_2[a,b,c,a_0,b_0,c_0], \\ J_3 &:= J \cap \mathbb{F}_2[a,b,c,a_0,b_0], \\ J_4 &:= J \cap \mathbb{F}_2[a,b,c,a_0], \\ J_5 &:= J \cap \mathbb{F}_2[a,b,c]. \end{aligned}$$

```
ring S = 2, (d0,d,c0,b0,a0,b,c,a), dp;
ideal J0 = imap(Rt,J0);
ideal J1 = eliminate(J0,d0);
ideal J2 = eliminate(J1,d);
ideal J3 = eliminate(J2,c0);
ideal J4 = eliminate(J3,b0);
ideal J5 = eliminate(J4,a0);
```

Weiter berechnen wir die Gröbnerbasis jedes Zwischenideals J_i bezüglich der Produkt–Termordnung, bei der die ersten $i+1$ Variablen lexikographisch `lp` und die restlichen graduiert revers lexikographisch `dp` geordnet sind. Wünschenswert wäre es, eine Basis von J_0 bezüglich der lexikographischen Termordnung zu finden, aber das scheitert an der Rechenzeit. Die Methode mit der Produkt–Termordnung spart Rechenzeit und liefert dasselbe Ergebnis.

```
ring S0 = 2,(d0,d,c0,b0,a0,b,c,a), (lp(1),dp(7));
ideal J0 = std(imap (S,J0));
size(J0); J0;
```

Das Ideal J_0 hat 334 Erzeugende $J_0[1], \ldots, J_0[334]$, die ersten 333 enthalten die Variable d_0 nicht und $J[334]$ ist linear in d_0 mit dem Koeffizient 1.

```
J0[334]=d0+a0^3*a^2+b0*a0^2+a0*b^2+c0*c^2+c0*c*a+a0*c*a+a0*a^2+
        d*c+b*c+d*a
```

Damit ist $J_1 = \langle J_0[1], \ldots, J_0[333] \rangle$ und die Mengen $V(J_0)$ und $V(J_1)$ sind biregulär, da für jeden Punkt von $V(J_1)$ ein d_0 eindeutig mit Hilfe von $J_0[334]$ bestimmt werden kann. Also existiert eine zu ϕ_1 inverse reguläre Abbildung

$$\psi_1 : V(J_1) \longrightarrow V(J_0).$$

Weiter suchen wir eine Gröbnerbasis von J_1.

```
ring S1 = 2,(d0,d,c0,b0,a0,b,c,a), (lp(2),dp(6));
ideal J1 = std(imap (S,J1));
size(J1); J1;
```

J_1 hat 211 Erzeugende, $J_1[1], \ldots, J_1[210]$ enthalten kein d und $J_1[211]$ ist linear in d mit dem Koeffizient 1.

```
J1[211]=d+b0*a0^2*a^3+a0*a^5+c0*a0*b*c*a+a0^2*b*c*a+a0^2*b*a^2+
        c0*a0^2*c+a0^3*c+c0*b^2*c+a0*b^2*c+b0^2*a0*a+a0^3*a+
        c0*c^2*a+c0*c*a^2+a0*c*a^2+a0*a^3+b0*a0*b+b^3+b*c*a+
        b0*c+c0*a+b0*a
```

Also $J_2 = \langle J_1[1], \ldots, J_1[210] \rangle$ und wie im vorherigen Fall sind $V(J_1)$ und $V(J_2)$ biregulär mit

$$\psi_2 : V(J_2) \longrightarrow V(J_1).$$

Dasselbe Verfahren benutzen wir weiter.

```
ring S2 = 2,(d0,d,c0,b0,a0,b,c,a), (lp(3),dp(5));
ideal J2 = std(imap (S,J2));
size(J2); J2;
```

Die Basis von J_2 hat 135 Elemente, 134 von denen enthalten kein c_0 und $J_2[135]$ ist linear in c_0 mit dem Koeffizient 1.

```
J2[135]=c0+a0^2*b*c*a^4+a0^3*c^2*a^2+a0^3*a^4+a0*c*a^5+a0*a^6+
        b0*a0*b*c*a^2+a0^2*b*c*a^2+b^3*c*a^2+b0*a0*b*a^3+b*c*a^4+
        b*a^5+b0*a0^2*c^2+a0*b^2*c^2+a0^3*c*a+b0*b^2*c*a+a0^3*a^2+
        b0*b^2*a^2+a0*b^2*a^2+b0*c*a^3+a0*c*a^3+b0*a^4+a0*a^4+
        b0*a0*b*c+b^3*c+b0^2*b*a+a0^2*b*a+b*c^2*a+b0^2*a0+b0*b^2+
        b0*c^2+a0*c^2+b0*c*a+b0*a^2+b*c.
```

Damit ist $J_3 = \langle J_2[1], \ldots, J_2[134] \rangle$ und wie vorher sind $V(J_3)$ und $V(J_4)$ biregulär mit

$$\psi_3 : V(J_3) \longrightarrow V(J_2).$$

Für die Gröbnerbasis von J_3 berechnen wir:

```
ring S3 = 2,(d0,d,c0,b0,a0,b,c,a), (lp(4),dp(4));
ideal J3 = std(imap (S,J3));
size(J3); J3;
```

Die Basis von J_3 hat 85 Elemente, $J_3[1], \ldots, J_3[57]$ enthalten kein b_0, $J_3[58], \ldots, J_3[84]$ sind linear in b_0 und in $J_3[85]$ tritt b_0^2 auf. Hier haben die Variablen b_0 immer einen polynomialen Koeffizient, zum Beispiel:

```
J3[58]=(a0*a^3+a0*c+a0*a)*b0 +a0^2*a^5+a0*b*c^2*a^2+b^2*c^2*a+
       a0^2*c*a^2+a0^2*a^3+b^2*a^3+c^2*a^3+a^5+b^2*c+b^2*a+
       c^2*a+c*a^2+c+a
```

Wir bezeichnen die Koeffizienten von b_0 in $J_3[58], \ldots, J_3[84]$ mit $\beta_{58}, \ldots, \beta_{84}$. Dann gibt es eine reguläre Abbildung

$$\psi_4 : V(J_4) \setminus V(\beta_{58}, \ldots, \beta_{84}) \longrightarrow V(J_3),$$

die links–invers zu ϕ_4 ist, also $\psi_4\phi_4 = \mathrm{Id}$, denn für ein $(a, b, c, a_0) \in V(J_4) \setminus V(\beta_{58}, \ldots, \beta_{84})$ gibt es ein i mit $\beta_i(a, b, c, a_0) \neq 0$ und wir können damit den Wert b_0 eindeutig aus $J_3[i]$ bestimmen. Tatsächlich gilt auch $(a, b, c, a_0, b_0) \in V(J_3)$, da ϕ_4 eine Projektion, also surjektiv ist. Insgesamt ist also $V(J_4) \setminus V(\beta_{58}, \ldots, \beta_{84})$ durch ψ_4 biregulär zu seinem Bild in $V(J_3)$. Die Ausnahmemenge $V(\beta_{58}, \ldots, \beta_{84})$ hat die Dimension 1.

Es gilt: $J_4 = \langle J_3[1], \ldots, J_3[57] \rangle$. Wir berechnen die neue Basis von J_4:

```
ring S4 = 2,(d0,d,c0,b0,a0,b,c,a), (lp(5),dp(3));
ideal J4 = std(imap (S,J4));
size(J4); J4;
```

Die Basis von J_4 hat 147 Elemente, $J_4[1]$ enthält kein a_0, $J_4[2], \ldots, J_4[80]$ sind linear in a_0 und in $J_4[81], \ldots, J_4[147]$ treten höhere Potenzen von a_0 auf. Wir bezeichnen die Koeffizienten von a_0 in $J_4[2], \ldots, J_4[80]$ mit $\alpha_2, \ldots, \alpha_{80}$. Analog zum obigen Fall gibt es eine reguläre Abbildung

$$\psi_5 : \ V(J_5) \setminus V(\alpha_2, \ldots, \alpha_{80}) \longrightarrow V(J_4),$$

die links–invers zu ϕ_5 ist, und somit $V(J_5) \setminus V(\alpha_2, \ldots, \alpha_{80})$ biregulär zu seinem Bild in $V(J_4)$.

Wir erhalten, dass $J_5 = \langle J_4[1] \rangle$, wobei $J_4[1]$ ein Polynom in Variablen a, b und c ist. Wir nennen dieses Polynom j.

$$j(a,c,b) = (a^8c^{12} + a^6c^{14} + a^4c^{12})b^{12} + (a^{14}c^{10} + a^{13}c^{11} + a^{12}c^{10} + a^{11}c^{11} + a^{10}c^{14} + a^{10}c^{12} + a^{10}c^{10} + a^9c^{15} + a^9c^{11} + a^8c^{12} + a^8c^{10} + a^7c^{15} + a^7c^{13} + a^7c^{11} + a^5c^{13})b^{10} + (a^{15}c^9 + a^{14}c^{12} + a^{14}c^8 + a^{13}c^{13} + a^{12}c^{10} + a^{12}c^8 + a^{11}c^{13} + a^{11}c^9 + a^{10}c^{16} + a^{10}c^{10} + a^{10}c^8 + a^9c^{17} + a^9c^{13} + a^9c^{11} + a^8c^{12} + a^8c^8 + a^7c^{15} + a^6c^{14} + a^6c^{12} + a^4c^{12} + a^2c^{14})b^8 + (a^{22}c^6 + a^{21}c^7 + a^{20}c^8 + a^{20}c^6 + a^{19}c^9 + a^{18}c^8 + a^{17}c^7 + a^{16}c^{10} + a^{16}c^8 + a^{16}c^6 + a^{15}c^7 + a^{14}c^{14} + a^{14}c^{12} + a^{14}c^{10} + a^{14}c^8 + a^{14}c^6 + a^{13}c^{15} + a^{13}c^9 + a^{12}c^{16} + a^{12}c^{14} + a^{12}c^{12} + a^{12}c^{10} + a^{12}c^8 + a^{12}c^6 + a^{11}c^{17} + a^{11}c^{11} + a^{11}c^9 + a^{11}c^7 + a^{10}c^{16} + a^{10}c^{14} + a^9c^{15} + a^9c^{13} + a^8c^8 + a^8c^6 + a^7c^9 + a^5c^{15} + a^4c^{14} + a^4c^{12} + a^4c^{10} + a^3c^{15} + a^3c^{13})b^6 + (a^{24}c^4 + a^{21}c^5 + a^{20}c^8 + a^{20}c^4 + a^{19}c^9 + a^{19}c^5 + a^{18}c^{12} + a^{18}c^{10} + a^{18}c^6 + a^{17}c^{13} + a^{17}c^9 + a^{16}c^{12} + a^{16}c^8 + a^{15}c^{13} + a^{15}c^{11} + a^{15}c^7 + a^{14}c^{16} + a^{14}c^{10} + a^{14}c^6 + a^{13}c^{17} + a^{13}c^{11} + a^{13}c^9 + a^{13}c^7 + a^{13}c^5 + a^{12}c^{14} + a^{12}c^{12} + a^{12}c^4 + a^{11}c^{11} + a^{11}c^7 + a^{11}c^5 + a^{10}c^{16} + a^{10}c^{12} + a^{10}c^{10} + a^{10}c^6 + a^9c^{17} + a^9c^{11} + a^9c^7 + a^8c^{12} + a^8c^8 + a^8c^4 + a^7c^{13} + a^7c^{11} + a^7c^9 + a^6c^{16} + a^6c^{10} + a^6c^6 + a^5c^{17} + a^5c^{15} + a^5c^{13} + a^5c^{11} + a^4c^{12} + a^2c^{10} + c^{12})b^4 + (a^{22}c^{10} + a^{22}c^2 + a^{21}c^{11} + a^{21}c^7 + a^{19}c^{11} + a^{19}c^9 + a^{19}c^7 + a^{18}c^{14} + a^{18}c^{10} + a^{18}c^2 + a^{17}c^{15} + a^{17}c^9 + a^{16}c^{12} + a^{16}c^{10} + a^{16}c^8 + a^{15}c^{15} + a^{14}c^{10} + a^{14}c^6 + a^{14}c^2 + a^{13}c^{11} + a^{13}c^9 + a^{13}c^7 + a^{12}c^{14} + a^{11}c^{13} + a^{11}c^7 + a^{10}c^{14} + a^{10}c^6 + a^{10}c^2 + a^9c^{13} + a^8c^{10} + a^8c^8 + a^7c^{11} + a^7c^9 + a^6c^{10} + a^5c^{15} + a^5c^{13} + a^4c^{12} + a^3c^{15} + a^3c^{13} + a^2c^{14} + a^2c^{10})b^2 + (a^{24}c^8 + a^{24} + a^{22}c^{10} + a^{22}c^2 + a^{20}c^{12} + a^{18}c^{14} + a^{18}c^{10} + a^{18}c^2 + a^{16}c^8 + a^{16}c^4 + a^{14}c^{14} + a^{14}c^{10} + a^{14}c^6 + a^{14}c^2 + a^{10}c^{10} + a^{10}c^6 + a^{10}c^2 + a^8c^4 + a^8 + a^6c^{14} + a^4c^8 + a^2c^{14} + a^2c^{10} + c^8)$$

Wir werden zeigen, dass $V(J_5)$ irreduzibel ist. Dann erhalten wir eine rationale Abbildung

$$\psi : V(J_5) \dashrightarrow V(J_0)$$

induziert durch die Komposition der regulären Abbildungen $\psi_1 \circ \cdots \circ \psi_5$. Da die ψ_i links–invers zu ϕ sind, ist $V(J_5)$ birational zu seinem Bild

$$V_0 := \psi(V(J_5))$$

mit Inversem ϕ. Insbesondere ist V_0 eine irreduzible zweidimensionale Komponente von $V(J_0)$.

Hilfssatz 5.8. *$V(J_5)$ ist irreduzibel in $\mathbb{A}^3$.*

Beweis. Das Ideal $J_5 = \langle j(a,b,c)\rangle$ wird von einem Element erzeugt.

Wir zeigen, dass $j(a,c,b)$ absolut irreduzibel ist, d.h. irreduzibel in $\overline{\mathbb{F}}_2[a,c,b]$.

Zuerst zeigen wir, dass $j(a,c,b)$ keinen nichttrivialen Faktor aus $\overline{\mathbb{F}}_2[a,c]$ hat. Seien $\lambda_1,\ldots,\lambda_{12} \in \overline{\mathbb{F}}_2[a,c]$ die Koeffizienten von $j(a,c,b)$ bezüglich b.

Angenommen, es gibt ein irreduzibles Polynom $p(a,c)$, das $\lambda_1,\ldots,\lambda_{12}$ teilt. Dann wäre $\langle\lambda_1,\ldots,\lambda_{12}\rangle$ in dem Ideal $\langle p(a,c)\rangle$ enthalten und damit $V(p(a,c)) \subseteq V(\lambda_1,\ldots,\lambda_{12})$. Wir berechnen $V(\lambda_1,\ldots,\lambda_{12})$ mit SINGULAR:

```
poly j = J5[1];
ideal C = coeffs(j,b);
facstd(C);
[1]:
   _[1]=a
   _[2]=c
[2]:
   _[1]=a+1
   _[2]=c
```

Wir sehen, dass $V(\lambda_1,\ldots,\lambda_{12}) = V(a,c) \cup V(a+1,c) = \{(0,0),(-1,0)\}$ nur aus zwei Punkten besteht, insbesondere hat $V(\lambda_1,\ldots,\lambda_{12})$ die Dimension 0. Das ist ein Widerspruch, weil $V(p(a,c))$ in $\mathbb{A}^2$ die Dimension 1 hat. Damit hat $j(a,c,b)$ keinen nichttrivialen Faktor aus $\overline{\mathbb{F}}_2[a,c]$.

Angenommen, $j(a,c,b)$ ist reduzibel, also es existieren Polynome $p(a,c,b), q(a,c,b) \in \overline{\mathbb{F}}_2[a,c,b]$, die nicht aus $\overline{\mathbb{F}}_2[a,c]$ sind, so dass

$$j(a,c,b) = p(a,c,b)q(a,c,b).$$

Wir substituieren a mit 1 und b mit $\frac{x}{c}$ und betrachten das Polynom

$$\begin{aligned} j(1,c,\tfrac{x}{c}) \quad = p(1,c,\tfrac{x}{c})q(1,c,\tfrac{x}{c}) = \quad & c^2x^{12} + c^4x^{10} + (c^9+c^8+c^7+c^5+c^3)x^8 \\ & +(c^{11}+c^6+c^5)x^8 \\ & +(c^{13}+c^{12}+c^{11}+c^{10}+c^8+c^6+c^4)x^4 \\ & +c^8x^2 + (c^{12}+c^{10}) \text{ in } \overline{\mathbb{F}}_2(c)[x]. \end{aligned}$$

Das Polynom $j(1,c,\frac{x}{c})$ ist durch c^2 teilbar, allerdings kann c^2 kein echter Faktor von $j(a,b,c)$ sein, weil es aus $\overline{\mathbb{F}}_2[a,c]$ ist. Nach [BGGKPP, 3.3] ist das Polynom

$$j(1,c,\frac{x}{c})/c^2 = x^{12} + c^2x^{10} + (c^7+c^6+c^5+c^3+c)x^8 + (c^9+c^4+c^3)x^6 +$$

$$(c^{11}+c^{10}+c^9+c^8+c^6+c^4+c^2)x^4 + c^6x^2 + (c^{10}+c^8)$$

irreduzibel in $\overline{\mathbb{F}}_2[c,x]$, also auch in $\overline{\mathbb{F}}_2(c)[x]$. Dann hat entweder $p(1,c,\frac{x}{c})$ oder $q(1,c,\frac{x}{c})$ den Grad 12 bezüglich x. Daraus folgt, dass entweder $p(a,c,b)$ oder

$q(a, c, b)$ den Grad 12 bezüglich b hat. Dann ist der andere Faktor aus $\overline{\mathbb{F}}_2[a, c]$, was vorher schon ausgeschlossen war.

Also hat $j(a, c, b)$ keinen nichttrivialen Faktor in $\overline{\mathbb{F}}_2[a, c, b]$ und ist damit absolut irreduzibel. □

Fortsetzung des Beweises von Hilfssatz 5.7.

Betrachten wir dafür die Menge

$$N \subseteq V(J_5)$$

auf der die rationale Abbildung ψ nicht regulär ist. Ihr Urbild unter ϕ ist enthalten in der Menge

$$V(J_0) \cap (V(\beta_{58}, \ldots, \beta_{84}) \cup V(\alpha_2, \ldots, \alpha_{80})).$$

Mit Hilfe des unten stehenden SINGULAR Programmes kann man berechnen, dass die Dimension dieser Menge 1 ist.

```
setring(S);

ideal J4 = imap(S4,J4);
  ideal Ja0 = 0;
  intvec v=0,0,0,0,1,0,0,0;
    for (int i=1; i<=size(J4); i=i+1){
         if (deg(J4[i],v) == 1){
              Ja0 = Ja0, diff(J4[i],a0);
          }
    }
ideal J3 = imap(S3,J3);
  ideal Jb0 = 0;
  intvec v=0,0,0,1,0,0,0,0;
    for (int i=1; i<=size(J3); i=i+1){
         if (deg(J3[i],v) == 1){
              Jb0 = Jb0, diff(J3[i],b0);
          }
    }
ideal Ja0b0=intersect(Ja0,Jb0);
ideal N= J0, Ja0b0;
dim(std(N));
```

Folglich stehen die zweidimensionalen Komponenten von $V(J_0)$ und $V(J_5)$ durch ϕ in Bijektion. Da $V(J_5)$ irreduzibel ist, ist V_0 die einzige zweidimensionale Komponente von $V(J_0)$. □

Bemerkung 5.9. Wahrscheinlich ist $V_0 = V(J_0)$, aber das können wir nicht beweisen, weil die Computerberechnungen zu aufwendig werden.

Lemma 5.10. *V_0 ist α–invariant.*

Beweis. Aus dem Hilfssatz 5.6 wissen wir, dass $\alpha(V(J_0)) \subseteq V(J_0)$ gilt.

Die Abbildung $\alpha : \mathbb{A}^8 \longrightarrow \mathbb{A}^8$ ist ein bijektiver Morphismus, also ist $\alpha(V_0)$ irreduzibel und hat die Dimension 2. Da V_0 die einzige 2–dimensionale Komponente in $V(J_0)$ ist, gilt $\alpha(V_0) = V_0$. □

5.2 Eine nichtsinguläre α–invariante Teilmenge von V_0

Wir werden eine α–invariante Hyperebene $V(f) \subseteq \mathbb{A}^8$ finden so, dass $V_0 \setminus V(f)$ nichtsingulär und α–invariant ist.

Ist s ein singulärer Punkt von V_0, so ist s auch ein singulärer Punkt von $V(J_0)$. Da wir $V(J_0)$ besser kennen, suchen wir eine Menge, die die singulären Punkte von $V(J_0)$ enthält. Dann enthält sie auch die Singularitäten von V_0.

Um eine Aussage über die Singulären Punkte zu machen, bestimmen wir zuerst ein neues Erzeugendensystem von J_0, das die Struktur des Ideals verständlicher macht. Dabei benutzen wir das Verfahren aus dem Beweis von Hilfssatz 5.7. Seien

$$\begin{aligned} I_1 &:= J_0 \cap \mathbb{F}_2[a,b,c,d,a_0,b_0,c_0], \\ I_2 &:= J_0 \cap \mathbb{F}_2[a,b,c,a_0,b_0,c_0], \\ I_3 &:= J_0 \cap \mathbb{F}_2[a,b,c,a_0,b_0], \\ I_4 &:= J_0 \cap \mathbb{F}_2[a,b,a_0,b_0], \\ I_{4c} &:= J_0 \cap \mathbb{F}_2[a,b,c,a_0], \\ I_5 &:= J_0 \cap \mathbb{F}_2[a,b,a_0]. \end{aligned}$$

Dieses Mal wählen wir eine andere Eliminationsreihenfolge, weil die Hyperfläche $V(f)$, die die Singularitäten von $V(J_0)$ enthält zusätzlich α–invariant sein soll. Es bietet sich an, das Polynom f aus $\mathbb{F}_2[a, a_0]$ zu wählen.

```
setring(R);
ideal I0 = imap(Rt,J0);
ideal I1 = eliminate(I0,d0);
ideal I2 = eliminate(I1,d);
```

```
ideal I3 = eliminate(I2,c0);
ideal I4 = eliminate(I3,c);
ideal I5 = eliminate(I4,b0);
```

Wie im Beweis von Hilfssatz 5.7 berechnen wir eine Gröbnerbasis in jedem Zwischenideal.

```
ring R0 = 2,(d0,d,c0,c,b0,b,a0,a), (lp(1),dp(7));
ideal I0 = std(imap (R,I0)); I0;
ring R1 = 2,(d0,d,c0,c,b0,b,a0,a), (lp(2),dp(6));
ideal I1 = std(imap (R,I1)); I1;
ring R2 = 2,(d0,d,c0,c,b0,b,a0,a), (lp(3),dp(5));
ideal I2 = std(imap (R,I2)); I2;
ring R3 = 2,(d0,d,c0,c,b0,b,a0,a), (lp(4),dp(4));
ideal I3 = std(imap (R,I3)); I3;
ring R4 = 2,(d0,d,c0,c,b0,b,a0,a), (lp(5),dp(3));
ideal I4 = std(imap (R,I4)); I4;
ring R5 = 2,(d0,d,c0,c,b0,b,a0,a), (lp(6),dp(2));
ideal I5 = std(imap (R,I5)); I5;
```

Wir werden gleich beschreiben, wie die Gröbnerbasen dieser Ideale aussehen, um noch weitere interessante Elemente von J_0 zu finden, ändern wir nochmal die Eliminationsreihenfolge.

```
setring(R);
ideal I4c = eliminate(I3,b0);

ring R4c = 2,(d0,d,c0,b0,c,b,a0,a), (lp(5),dp(3));
ideal I4c = std(imap (R,I4c)); I4c;
```

Wir fassen die Ergebnisse zusammen:

- Das Ideal I_0 hat 359 Erzeugende, $I_0[1], \ldots, I_0[358]$ enthalten kein d_0 und $I_0[359]$ ist linear in d_0 mit dem Koeffizient 1.
- Das Ideal $I_1 = \langle I_0[1], \ldots, I_0[358] \rangle$ hat 217 Erzeugende, $I_1[1], \ldots, I_1[216]$ enthalten kein d und $I_1[217]$ ist linear in d mit dem Koeffizient 1.
- Das Ideal $I_2 = \langle I_1[1], \ldots, I_1[216] \rangle$ hat 137 Erzeugende, $I_2[1], \ldots, I_2[136]$ enthalten kein c_0 und $I_2[137]$ ist linear in c_0 mit dem Koeffizient 1.
- Das Ideal $I_3 = \langle I_2[1], \ldots, I_2[136] \rangle$ hat 183 Erzeugende, $I_3[1], \ldots, I_3[161]$ enthalten kein c, in $I_3[162], \ldots, I_3[178]$ kommt c linear vor und in $I_3[179], \ldots, I_3[183]$ treten höhere Potenzen von c auf.

- Das Ideal $I_4 = \langle I_3[1], \ldots, I_3[161] \rangle$ hat 181 Erzeugende, $I_4[1]$ enthält kein b_0, in $I_4[2], \ldots, I_4[126]$ kommt b_0 linear vor und in $I_4[127], \ldots, I_4[181]$ sind höhere Potenzen von b_0.

- Das Ideal $I_{4c} = I_3 \cap \mathbb{F}_2[a, a_0, b, c]$ hat 184 Erzeugende, $I_4[1]$ enthält kein c, in $I_{4c}[2], \ldots, I_{4c}[132]$ kommt c linear vor und in $I_{4c}[133], \ldots, I_{4c}[184]$ sind höhere Potenzen von c.

- Das Ideal $I_5 = \langle I_4[1] \rangle = \langle I_{4c}[1] \rangle$ wird von einem Element erzeugt, wir nennen dieses h. Das Polynom $h(a, a_0, b)$ hat den Grad 35 und ist im Anhang C angegeben.

Bemerkung 5.11. Aus den Berechnungen können wir ein neues Erzeugendensystem von J_0 bilden:

$$
\begin{aligned}
J_0 = \langle \quad & I_0[359], I_1[217], I_2[137], I_{4c}[2], \ldots, I_{4c}[132], I_4[2], \ldots, I_4[126], I_5[1], \\
& I_3[179], \ldots, I_3[183], I_{4c}[133], \ldots, I_{4c}[184] \rangle \\
= \langle \quad & d_0 + p_0(a, a_0, b, b_0, c, c_0, d), \\
& d + p_1(a, a_0, b, b_0, c, c_0), \\
& c_0 + p_2(a, a_0, b, b_0, c), \\
& c \cdot x_1(a, a_0, b) + p_{3,1}(a, a_0, b), \\
& \vdots \qquad\qquad\quad \vdots \\
& c \cdot x_{131}(a, a_0, b) + p_{3,131}(a, a_0, b), \\
& b_0 \cdot y_1(a, a_0, b) + p_{4,1}(a, a_0, b), \\
& \vdots \qquad\qquad\quad \vdots \\
& b_0 \cdot y_{125}(a, a_0, b) + p_{4,125}(a, a_0, b), \\
& h(a, a_0, b), \\
& \text{Polynome aus } \mathbb{F}_2[a, a_0, b, b_0, c] \text{ mit höheren } c - \text{Potenzen}, \\
& \text{Polynome aus } \mathbb{F}_2[a, a_0, b, b_0] \text{ mit höheren } b_0 - \text{Potenzen } \rangle.
\end{aligned}
$$

Wir suchen eine Teilmenge von $V(J_0)$, die die Menge der Singularitäten enthält. Dafür definieren wir die folgenden Ideale:

Bezeichnung 5.12. Seien

$$
\begin{aligned}
E_c &:= \langle x_1, x_2, \ldots, x_{131} \rangle, \\
E_{b_0} &:= \langle y_1, y_2, \ldots, y_{125} \rangle, \\
E_h &:= \left\langle \frac{\partial h(a, a_0, b)}{\partial a}, \frac{\partial h(a, a_0, b)}{\partial a_0}, \frac{\partial h(a, a_0, b)}{\partial b} \right\rangle, \\
E &:= E_c \cap E_{b_0} \cap E_h.
\end{aligned}
$$

```
setring(R);
ideal Eb0= I5;
ideal I4 = imap(R4,I4);
intvec v=0,0,0,0,1,0,0,0;
for (int i=1; i<=size(I4); i=i+1){
     if (deg(I4[i],v) == 1){
          Eb0 = Eb0, diff(I4[i],b0);
      }
}
ideal Ec= I5;
ideal I4c = imap(R4c,I4c);
intvec v=0,0,0,1,0,0,0,0;
for (int i=1; i<=size(I4c); i=i+1){
     if (deg(I4c[i],v) == 1){
          Ec = Ec, diff(I4c[i],c);
      }
}
ideal Eh = I5,jacob(I5);
ideal E=std(intersect(Ec,Eb0,Eh));
```

Als Nächstes werden wir zeigen, dass die Singularitäten von $V(J_0)$ in der Menge $V(E)$ liegen.

Hilfssatz 5.13. *Sei S die Singularitätenmenge von $V(J_0)$ und E das Ideal aus 5.12. Dann gilt: $S \subseteq V(E)$.*

Beweis. Die Jacobi–Matrix von J_0 hat folgende Gestalt:

$$\begin{pmatrix}
1 & & & & & & \\
0 & 1 & & & & & \\
0 & 0 & 1 & & & & \\
0 & 0 & 0 & x_1(a,a_0,b) & & & \\
\vdots & & \vdots & \vdots & & & \\
0 & 0 & 0 & x_{131}(a,a_0,b) & & & \\
0 & 0 & 0 & 0 & y_1(a,a_0,b) & & \\
\vdots & & & \vdots & \vdots & & \\
0 & 0 & 0 & 0 & y_{125}(a,a_0,b) & & \\
0 & 0 & 0 & 0 & 0 & \frac{\partial h(a,a_0,b)}{\partial a} & \frac{\partial h(a,a_0,b)}{\partial a_0} \quad \frac{\partial h(a,a_0,b)}{\partial b} \\
\multicolumn{7}{c}{\text{... Ableitungen weiterer Erzeugenden ...}}
\end{pmatrix}$$

Sei $s \in S$. Falls $s \notin V(E_c) \cup V(E_{b_0}) \cup V(E_h) = V(E)$, so hat die Jacobi–Matrix in s mindestens $6 = 8 - \dim V(J_0)$ linear unabhängige Zeilen, also s ist nichtsingulär. Daraus folgt $S \subseteq V(E)$. □

Bemerkung 5.14. Die Menge $V_0 \setminus V(E)$ ist nicht α–invariant.

Wir werden eine Hyperfläche $V(f)$ finden, die $V(E)$ enthält, so dass $V_0 \setminus V(f) \subseteq V_0 \setminus V(E)$ nicht nur nichtsingulär, sondern auch α–invariant ist.

Wir suchen das Polynom f in $E \cap \mathbb{F}_2[a, a_0]$. Da wir nur an der Nullstellenmenge von f interessiert sind, berechnen wir das Radikalideal von $E \cap \mathbb{F}_2[a, a_0]$. Dieses wird von einem nicht α–invarianten Polynom $\tilde{f}$ erzeugt,

$$\mathrm{Rad}(E \cap \mathbb{F}_2[a, a_0]) = \langle \tilde{f} \rangle$$

und setzen

$$f := \tilde{f} \cdot \pi(\tilde{f}),$$

dabei war π definiert durch: $a \mapsto a_0$, $a_0 \mapsto a^2$.

Das Polynom $\tilde{f}(a, a_0)$ hat den Grad 38, es ist im Anhang C wiedergegeben. $f(a, a_0)$ ist ein Polynom vom Grad 95 in $\mathbb{F}_2[a, a_0]$. Wir können das nicht im Anhang angeben, aber man kann es mit dem folgenden SINGULAR Programm ausrechnen.

```
LIB"primdec.lib";
ideal F = eliminate(E,b);
ideal RF = radical(F);

map pi = R, d^2,d0,c^2,c0,b^2,b0,a^2,a0;
poly f = RF[1]*pi(RF[1]);
```

Bemerkung 5.15. Es gilt $V(E) \subseteq V(f)$, weil

$$V(E) \subseteq V(E \cap \mathbb{F}_2[a, a_0]) = V(\mathrm{Rad}(E \cap \mathbb{F}_2[a, a_0])) = V(\tilde{f}) \subseteq V(\tilde{f} \cdot \pi(\tilde{f})) = V(f).$$

Damit ist $V_0 \setminus V(f) \subseteq V_0 \setminus V(E)$.

Hilfssatz 5.16. *Die Menge*

$$U := V_0 \setminus V(f) \subseteq \mathbb{A}^8$$

ist nicht leer, α–invariant, nichtsingulär und irreduzibel.

Beweis. Für den Beweis von $U \neq \emptyset$ müssen wir zeigen, dass $f \notin J_0$ ist. Das berechnen wir mit SINGULAR:

```
reduce(f,J0);
```

Das ergibt nicht 0, also gilt $f \notin J_0$.

U ist irreduzibel nach Hilfssatz 5.7, nichtsingulär nach Hilfssatz 5.13.

Zu zeigen bleibt, dass U α–invariant ist. Da V_0 nach Bemerkung 5.10 α–invariant ist, reicht es die α–Invarianz von $\mathbb{A}^8 \setminus V(f)$ zu zeigen.

Wir zeigen: Falls $v \notin V(f)$, so gilt $\alpha(v) \notin V(f)$. Sei $v = (v_1, \ldots, v_8) \in \mathbb{A}^8 \setminus V(f)$, also $\tilde{f}(v) \neq 0$ und $\pi(\tilde{f}(v)) \neq 0$. Angenommen, $\alpha(v) \in V(f)$. Dann ist $\tilde{f}(\alpha(v)) = 0$ oder $\pi(\tilde{f}(\alpha(v))) = 0$.

Die erste Bedingung $0 = \tilde{f}(\alpha(v)) = \pi(\tilde{f}(v))$ steht im Widerspruch zur Voraussetzung.

Die zweite Bedingung ergibt $0 = \pi(\tilde{f}(\alpha(v))) = \tilde{f}(\alpha^2(v)) = \tilde{f}(v_1^2, \ldots, v_8^2)$. Da die Charakteristik des Koeffizientenkörpers 2 ist, gilt $\tilde{f}(v_1^2, \ldots, v_8^2) = \tilde{f}^2(v)$. Daraus folgt $\tilde{f}(v) = 0$, was ebenfalls ein Widerspruch ist.

Also gilt $\alpha(\mathbb{A}^8 \setminus V(f)) \subseteq \mathbb{A}^8 \setminus V(f)$. □

Die Menge $U \subseteq V(J)$ erfüllt die Voraussetzungen des Satzes 5.5. Um die Abschätzungen der Betti–Zahlen zu vereinfachen, zeigen wir im nächsten Hilfssatz, dass U biregulär zu einer Fläche in $\mathbb{A}^3$ ist.

Hilfssatz 5.17. *Sei h das Polynom aus 5.11 und*

$$W := V(h) \setminus V(f).$$

Dann sind W und $U = V_0 \setminus V(f)$ biregulär über die Projektion $\sigma : U \longrightarrow W$.

Beweis. Als Erstes bemerken wir, dass nach Konstruktion

$$\sigma(V_0) = V(h)$$

gilt.

Da $\overline{\mathbb{F}}_2$ algebraisch abgeschlossen ist, ist die Hyperfläche $V(h) \subseteq \mathbb{A}^3$ eine Vereinigung von 2–dimensionalen Komponenten. In 5.7 haben wir gezeigt, dass V_0 die einzige 2–dimensionale Komponente von $V(J_0)$ ist. Damit ist $V(h)$ als Bild von V_0 irreduzibel.

Ferner gilt:

$$\sigma(V_0 \setminus V(f)) = V(h) \setminus V(f),$$

weil $\sigma^{-1}(V(f) \subseteq \mathbb{A}^3) = V(f) \subseteq \mathbb{A}^8$ wegen $f \in \mathbb{F}_2[a, a_0]$ ist. Mit den Bezeichnungen W und U heißt das

$$\sigma(U) = W.$$

Sei nun $v \in W$. Aus $v \notin V(f)$ und $V(E) \subseteq V(f)$ folgt, dass

$$v \notin V(E) = V(x_1, \ldots, x_{131}) \cup V(y_1, \ldots, y_{125}) \cup V(h)$$

ist. Dann gibt es mindestens ein x_i und mindestens ein y_j, so dass $x_i(v) \neq 0$ und $y_i(v) \neq 0$. Damit können wir die zu σ inverse Abbildung δ definieren:

$$\begin{array}{rccc} & W & & U \\ & \shortparallel & & \shortparallel \\ \delta: & V(h) \setminus V(f) & \longrightarrow & V(J_0) \setminus V(f) \\ & (a, a_0, b) & \longmapsto & (a, b, c, d, a_0, b_0, c_0, d_0) \end{array}$$

mit

$$\begin{aligned} b_0 &= \tfrac{p_{4,j}(a,a_0,b)}{y_j(a,a_0,b)}, \\ c &= \tfrac{p_{3,i}(a,a_0,b)}{x_i(a,a_0,b)}, \\ c_0 &= p_2(a, a_0, b, b_0, c), \\ d &= p_1(a, a_0, b, b_0, c, c_0), \\ d_0 &= p_0(a, a_0, b, b_0, c, c_0, d), \end{aligned}$$

dabei benutzen wir die Bezeichnung aus 5.11. Zu jedem (a, a_0, b) aus $V(h) \setminus V(f)$ existiert mindestens ein $(a, b, c, d, a_0, b_0, c_0, d_0) \in V(J_0) \setminus V(f)$, weil $V(h) \setminus V(f)$ die Projektion von $V(J_0) \setminus V(f)$ ist. Da b_0, c, c_0, d, d_0 durch Brüche von Polynomen bestimmt werden, sind diese eindeutig. Das definiert eine reguläre Abbildung $W \to U$.

Nach der Konstruktion von σ und δ gilt $\sigma \circ \delta = Id_W$ und $\delta \circ \sigma = Id_U$. □

Bemerkung 5.18. Wir fassen nochmal die Konstruktion von U zusammen:

$$\begin{array}{lccccccccc} \mathbb{A}^3 & \supseteq & & & & & & & V(h) \setminus V(f) & =: W \\ & & & & & & & & \updownarrow \text{biregulär} & \\ \mathbb{A}^8 & \supseteq & V(J_0) & \supseteq & V_0 & \supseteq & V_0 \setminus V(E) & \supseteq & V_0 \setminus V(f) & =: U \\ & & \alpha\text{–invariant} & & \alpha\text{–invariant} & & & & \alpha\text{–invariant} & \\ & & & & \text{irred.} & & \text{irred.} & & \text{irred.} & \\ & & & & & & \text{nichtsing.} & & \text{nichtsing.} & \end{array}$$

5.3 Eine Abschätzung von $|\operatorname{Fix}(U, n)|$

Hilfssatz 5.19. *Für U aus Hilfssatz 5.16 ist $b^1(U) \leq 4482 \leq 2^{12}$, wobei $b^1(U) = \dim H^1_{et}(U, \mathbb{Q}_\ell)$ ist.*

Beweis. Nach 5.17 sind U und W biregulär. Da die Struktur von W verständlicher ist, schätzen wir die erste Betti Zahl von W ab.

Sei $H := V(\lambda_1 a + \lambda_2 a_0 + \lambda_3 b)$ eine Hyperebene in $\mathbb{A}^3$.

Nach dem Hyperebenen Schnittsatz von Lefschetz ist die Abbildung

$$H^1_{et}(W, \mathbb{Q}_p) \to H^1_{et}(W \cap H, \mathbb{Q}_p)$$

für eine 2–dimensionale Fläche W injektiv [M80], daraus folgt, dass

$$b^1(W) \leq b^1(W \cap H).$$

Sei $\overline{W \cap H}$ der projektive Abschluss von $W \cap H$ in $\overline{H} \simeq \mathbb{P}^2$. Die Fläche W ist nach Hilfssatz 5.7 irreduzibel, also ist $W \cap H$ eine irreduzible Kurve in $H \simeq \mathbb{A}^2$ und $\overline{W \cap H}$ eine irreduzible Kurve in $\overline{H} \simeq \mathbb{P}^2$.

Dann gilt nach [GL02, 7.4]:

$$b^1(\overline{W \cap H}) \leq (d-1)(d-2),$$

wobei d der Grad von $\overline{W \cap H} \subseteq \mathbb{P}^2$ ist.

Dafür müssen wir den Grad von $\overline{W \cap H}$ bestimmen. Aus der Konstruktion von W folgt:

$$\overline{W \cap H} = \overline{W} \cap \overline{H} = \overline{V(h) \setminus V(f)} \cap \overline{H} = \overline{V(h)} \cap \overline{H}.$$

Da $\overline{W \cap H}$ irreduzibel ist, folgt nach dem Satz von Bezout [Ha77, I.7.7], dass

$$\deg \overline{W \cap H} \leq \deg V(h) \cdot \deg H = 35 \cdot 1 = 35 \text{ ist, also gilt}$$

$$b^1(\overline{W \cap H}) \leq (35-1)(35-2) = 1122.$$

Wir wollen $b^1(W \cap H)$ abschätzen. Nach [M89, 9.3] ist die Sequenz

$$H^1_{et}(\overline{W \cap H}, \mathbb{Q}_l) \to H^1_{et}(W \cap H, \mathbb{Q}_l) \to H^0_{et}(\overline{W \cap H} \setminus (W \cap H), \mathbb{Q}_l)$$

exakt, also ist

$$\dim H^1_{et}(W \cap H, \mathbb{Q}_l) \leq \dim H^1_{et}(\overline{W \cap H}, \mathbb{Q}_l) + \dim H^0_{et}(\overline{W \cap H} \setminus (W \cap H), \mathbb{Q}_l).$$

Damit können wir die erste Betti–Zahl von $W \cap H$ abschätzen als:

$$\begin{aligned} b^1(W \cap H) &\leq b^1(\overline{W \cap H}) &+ \dim H^0_{et}(\overline{W \cap H} \setminus W \cap H, \mathbb{Q}_l) \\ &\leq 1122 &+ \dim H^0_{et}(\overline{W \cap H} \setminus W \cap H, \mathbb{Q}_l). \end{aligned}$$

Die Menge $\overline{W \cap H} \setminus W \cap H$ besteht aus endlich vielen Punkten, insbesondere ist

$$\dim H^0_{et}(\overline{W \cap H} \setminus W \cap H, \mathbb{Q}_l) \leq \deg \overline{W \cap H} \setminus W \cap H.$$

Also reicht es, den Grad von $\overline{W \cap H} \setminus W \cap H$ abzuschätzen. Aus der Konstruktion von W sehen wir, dass

$$\overline{W \cap H} \setminus W \cap H = (\overline{W \cap H}) \cap (V(f) \cup H_\infty).$$

Dann folgt mit dem Satz von Bezout:

$$\begin{aligned} \deg \overline{W \cap H} \setminus W \cap H &\leq \deg \overline{W \cap H} &\cdot \deg(V(f) \cup H_\infty) \\ &\leq 35 &\cdot (95+1). \end{aligned}$$

Insgesamt haben wir die Abschätzung:

$$b^1(W) \leq b^1(W \cap H) \leq 1122 + 35 \cdot 96 = 4482.$$

□

Für die Abschätzung der zweiten Betti–Zahl benötigen wir weitere Hilfssätze.

Hilfssatz 5.20. *Für die Euler–Charakteristik von U gilt: $|\chi(U)| \leq 2486105$.*

Beweis. Da U und W biregulär sind, reicht es, wenn wir $\chi(W)$ abschätzen. Nach der Definition von W ist

$$V(h) = (V(h) \setminus V(f)) \cup (V(h) \cap V(f)) = W \cup V(h, f).$$

Da die Mengen W und $V(h, f)$ disjunkt sind, folgt

$$\chi(W) = \chi(V(h)) - \chi(V(h, f)).$$

Für die Abschätzung von $\chi(V(h))$ und $\chi(V(h, f))$ benutzen wir wie in [BGGKPP] den folgenden Satz.

Hilfssatz 5.21. *[AS88][Ka01] Sei $V \in \mathbb{A}^N$ eine affine Varietät, erzeugt von r Polynomen vom Grad $\leq d$. Dann gilt:*

$$|\chi(V)| \leq 2^r D_{N,r} \underbrace{(1, 1+d, \ldots, 1+d)}_{r+1},$$

wobei $D_{N,r}(x_0, \ldots, x_r) = \sum_{|W|=N} X^W$ die Summe der homogenen Monome vom Grad N mit den Koeffizienten 1 ist.

In unserem Fall benötigen wir:

$D_{3,1}(x_0, x_1) = x_0^3 + x_0^2 x_1 + x_0 x_1^2 + x_1^3$ und

$D_{3,2}(x_0, x_1, x_2) = x_0^3 + x_0^2 x_1 + x_0^2 x_2 + x_0 x_1^2 + x_0 x_1 x_2 + x_0 x_2^2 + x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3$.

Jetzt können wir $\chi(V(h))$ und $\chi(V(h, f))$ abschätzen.

$$\begin{aligned} \chi(V(h)) &\leq 2 \cdot D_{3,1}(1, 35+1) &&= 2 \cdot (1 + 36 + 36^2 + 36^3) = 95978, \\ \chi(V(h,f)) &\leq 2^2 \cdot D_{3,2}(1, 95+1, 95+1) &&= 4 \cdot (1 + 2 \cdot 96 + 3 \cdot 96^2 + 3 \cdot 96^3) \\ & &&= 10728196. \end{aligned}$$

Also ist

$$|\chi(W)| \leq 95978 + 10728196 = 10824174.$$

□

Hilfssatz 5.22. *Es gilt:* $b^2(U) \leq 10828655 \leq 2^{24}$.

Beweis. Ist $\chi(U) \leq 0$, dann gilt $1 - b^1(U) + b^2(U) \leq 0$ und damit

$$b^2(U) \leq b^1(U) \leq 4482 \leq 2^{12}.$$

Falls $\chi(U) > 0$, dann ist $b^2(U) = -1 + \chi(U) + b^1(U) \leq 10824173 + 4482 = 10828655 \leq 2^{24}$. □

Wir bezeichnen mit $\mathrm{Fix}(M, n)$ die Menge der Fixpunkte von α^n auf einer Menge M.

Hilfssatz 5.23. *Ist* $\mathrm{Fix}(V_0 \cap V(f), n) = \emptyset$*, so gilt:* $|\mathrm{Fix}(U, n)| > 1$*, wenn* $n > 50$ *und ungerade.*

Beweis. Zuerst zeigen wir: Wenn α^n keinen nichttrivialen Fixpunkt auf der Menge $V_0 \cap V(f)$ hat, so ist $\overline{\mathrm{Fix}(U, n)} \setminus \mathrm{Fix}(U, n)$ leer. Das ist eine der Voraussetzungen des Satzes 5.5. Wir werden dann den Satz 5.5 auf U anwenden.

Wir bezeichnen mit

$$H_\infty = \{(0 : a : b : c : d : a_0 : b_0 : c_0 : d_0)\} \subseteq \mathbb{P}^8$$

die unendlich ferne Hyperebene in $\mathbb{P}^8$. Da

$$\overline{U} \setminus U = (\overline{V_0} \cap H_\infty) \cup (V_0 \cap V(f)),$$

so ist

$$\overline{\mathrm{Fix}(U, n)} \setminus \mathrm{Fix}(U, n) = (\overline{\mathrm{Fix}(V_0, n)} \cap H_\infty) \cup (\mathrm{Fix}(V_0, n) \cap V(f)).$$

Aus der Voraussetzung $\mathrm{Fix}(V_0 \cap V(f), n) = \emptyset$ folgt, dass $\mathrm{Fix}(V_0, n) \cap V(f) = \emptyset$.

Behauptung. Die Menge $\overline{\mathrm{Fix}(V_0, n)} \cap H_\infty$ ist leer.

Beweis. Betrachten wir zunächst die Operation von $\alpha^n = \alpha^{2m+1}$ auf $\mathbb{A}^8$:

$$\alpha^{2m+1}(a, b, c, d, a_0, b_0, c_0, d_0) = (a_0^{2^m}, b_0^{2^m}, c_0^{2^m}, d_0^{2^m}, a^{2^{m+1}}, b^{2^{m+1}}, c^{2^{m+1}}, d^{2^{m+1}}).$$

Die Fixpunkte sind hier gegeben durch die Gleichungen:

$$a = a_0^{2^m}, b = b_0^{2^m}, c = c_0^{2^m}, d = d_0^{2^m}, a_0 = a^{2^{m+1}}, b_0 = b^{2^{m+1}}, c_0 = c^{2^{m+1}}, d_0 = d^{2^{m+1}},$$

insbesondere werden die Gleichungen

$$a = (a^{2^{m+1}})^{2^m} = a^{2^{m+1} \cdot 2^m} = a^{2^{2m+1}} = a^{2^n},$$

$$a_0 = (a_0^{2^m})^{2^{m+1}} = a_0^{2^m \cdot 2^{m+1}} = a_0^{2^{2m+1}} = a_0^{2^n},$$

und analog für b, c und d erfüllt. Schließen wir $\mathbb{A}^8$ in $\mathbb{P}^8$ durch Einführung der variable t ab, so enthält das Verschwindungsideal von $\overline{\mathrm{Fix}(V_0, n)}$ also die Gleichungen

$$at^{2^n-1} - a^{2^n},\ bt^{2^n-1} - b^{2^n},\ ct^{2^n-1} - c^{2^n},\ dt^{2^n-1} - d^{2^n},$$

$$at^{2^n-1} - a_0^{2^n},\ bt^{2^n-1} - b_0^{2^n},\ ct^{2^n-1} - c_0^{2^n},\ dt^{2^n-1} - d_0^{2^n}.$$

In H_∞ ist $t = 0$, also

$$a^{2^n} = b^{2^n} = c^{2^n} = d^{2^n} = a_0^{2^n} = b_0^{2^n} = c_0^{2^n} = d_0^{2^n} = 0$$

und damit

$$a = b = c = d = a_0 = b_0 = c_0 = d_0 = 0$$

in für alle $(t : a : b : c : d : a_0 : b_0 : c_0 : d_0) \in \overline{\mathrm{Fix}(V_0, n)}$. Also ist $\overline{\mathrm{Fix}(V_0, n)} \cap H_\infty = \emptyset$, womit die Behauptung gezeigt ist.

Wir haben gezeigt, dass $\overline{\mathrm{Fix}(U, n)} = \mathrm{Fix}(U, n)$ erfüllt ist. Aus Hilfssatz 5.16 wissen wir, dass die Menge U nicht leer, irreduzibel, nichtsingulär und α–invariant ist. Damit können wir Satz 5.5 anwenden, der besagt, dass

$$|\mathrm{Fix}(U, n)| \geq 2^n - b^1(U)2^{3n/4} - b^2(U)2^{n/2}.$$

Nach Hilfssatz 5.19 ist $b^1(U) \leq 4482$, und nach Hilfssatz 5.22 gilt $b^2(U) \leq 10828656$. Insgesamt ist

$$|\mathrm{Fix}(U, n)| \geq 2^n - 4482 \cdot 2^{3n/4} - 10828656 \cdot 2^{n/2}.$$

Durch Einsetzen von $n = 51$ erhalten wir, dass $|\mathrm{Fix}(U, 50)| > 1$, aus der Monotonie von $2^n - 4482 \cdot 2^{3n/4} - 10828656 \cdot 2^{n/2}$ folgt, dass $|\mathrm{Fix}(U, n)| > 1$ für alle $n > 50$. □

Hilfssatz 5.24. *Für jedes ungerade* $3 \leq n \leq 50$ *gibt es* $x, y \in \mathrm{Sz}(2^n)$*, die* $v_1(x,y) \neq 1$ *und* $v_1(x,y) = v_2(x,y)$ *erfüllen.*

Beweis. Für $n \leq 50$ suchen wir Beispiele für $(a,b,c,d,a_0,b_0,c_0,d_0) \in \mathbb{F}_{2^n}^8$ so dass $x(a,b,a_0,b_0), y(c,d,c_0,d_0) \in \mathrm{Sz}(2^n)$ sowohl $v_1(x,y) \neq 1$ als auch $v_1(x,y) = v_2(x,y)$ gilt.

Weil nur endlich viele verschiedene n zu betrachten sind, können wir die Beispiele für x und y mit MAGMA finden.

Da $\mathbb{F}_{2^k}$ für $k|l$ ein Unterkörper von $\mathbb{F}_{2^l}$ ist, reicht es, die x und y aus $\mathrm{Sz}(2^p)$ für Primzahlen $3 \leq p \leq 50$ zu bestimmen. Man kann diese Werte nicht durch einfaches Einsetzen finden, weil zum Beispiel im Fall $p = 47$ ungefähr $(2^{47})^4 \approx 10^{57}$ Fälle zu testen sind.

Wir versuchen die Lösungen systematisch zu erraten. Zum Glück gab es auch genügend von denen. Wir schreiben den Körper $\mathbb{F}_{2^p}$ als $\mathbb{F}_2[t]/(r)$ für ein irreduzibles Polynom r vom Grad p.

Zuerst wählen wir $a \in \{0, 1, t, t+1, t^2, t^2+1, t^2+t, t^2+t+1, t^3, t^3+1, t^3+t, t^3+t+1, t^3+t^2, t^3+t^2+1, t^3+t^2+t, t^3+t^2+t+1, \dots\}$ und setzen $a_0 := a^{2^{m+1}}$ nach Definition von $\theta(a)$, dabei ist $p = 2m+1$.

Als Nächstes wählen wir einige Gleichungen aus J_0, die wir in 5.11 berechnet haben:

$d_0 + p_0(a, a_0, b, b_0, c, c_0, d)$,

$d + p_1(a, a_0, b, b_0, c, c_0)$,

$c_0 + p_2(a, a_0, b, b_0, c)$,

$c \cdot x_1(a, a_0, b) + p_{3,1}(a, a_0, b)$,

$b_0 \cdot y_1(a, a_0, b) + p_{4,1}(a, a_0, b)$,

$h(a, a_0, b)$.

Es muss gelten $h(a, a_0, b) = 0$. Da der Grad von $h(a, a_0, b)$ bezüglich b gleich 18 ist, gibt es für feste a und a_0 höchstens 18 Möglichkeiten für b. Die berechnen wir mit dem MAGMA Befehl

```
Variety( );
```

Falls $y_1(a, a_0, b) \neq 0$ und $x_1(a, a_0, b) \neq 0$ gilt, so setzen wir

$$b_0 := \frac{p_{4,1}(a, a_0, b)}{y_1(a, a_0, b)} \quad \text{und} \quad c := \frac{p_{3,1}(a, a_0, b)}{x_1(a, a_0, b)}.$$

Weiter setzen wir:

$$c_0 := p_2(a, a_0, b, b_0, c),\ d := p_1(a, a_0, b, b_0, c, c_0),\ d_0 := p_0(a, a_0, b, b_0, c, c_0, d).$$

Falls zusätzlich

$$b_0 = b^{2^{m+1}},\ c_0 = c^{2^{m+1}},\ d_0 = d^{2^{m+1}}$$

und

$$y^{-2}x^{-2}yx = x^2y^{-1}x^{-1}y$$

für $x = x(a, b, a_0, b_0)$ und $y = y(c, d, c_0, d_0)$ erfüllt ist, so haben wir einen Punkt $(a, b, c, d, a_0, b_0, c_0, d_0) \in \mathbb{F}_{2^{2^{m+1}}}$ mit

$$v_2(x(a, b, a_0, b_0), y(c, d, c_0, d_0)) = v_1(x(a, b, a_0, b_0), y(c, d, c_0, d_0)),$$

$$v_1(x(a, b, a_0, b_0), y(c, d, c_0, d_0)) \neq 1$$

und $x(a, b, a_0, b_0), y(c, d, c_0, d_0) \in Sz(2^n)$ gefunden. Wir geben die Punkte mit dieser Eigenschaft aus $\mathbb{F}_{2^p}$ für $3 \leq p \leq 50$ im Anhang D an.

□

Beweis von Satz 5.1

Hat die Abbildung α^n einen nichttrivialen Fixpunkt auf der Menge $V_0 \cap V(f)$, dann hat α^n einen nichttrivialen Fixpunkt auf $V(J)$, weil $V_0 \subseteq V(J)$ ist. Nach dem Satz 5.4 gibt es $x, y \in \mathrm{Sz}(2^n)$ mit $v_1(x, y) \neq 1$ und $v_1(x, y) = v_2(x, y)$.

Hat α^n keinen nichttrivialen Fixpunkt auf der Menge $V_0 \cap V(f)$. Dann hat α^n nach Satz 5.23 einen nichttrivialen Fixpunkt auf $U \subseteq V(J)$, wenn $n > 50$. Mit dem Satz 5.4 folgt das Gleiche für $n > 50$.

Nach Satz 5.24 gibt es für $3 \leq n \leq 50$ Elemente $x, y \in \mathrm{Sz}(2^n)$, die $v_1(x, y) \neq 1$ und $v_1(x, y) = v_2(x, y)$ erfüllen. □

Kapitel 6

Eine Aussage über Engelgruppen

Wir erinnern an den Satz von Zorn:

Satz 6.1 (Zorn). *G sei eine endliche Gruppe und die Sequenz $e = (e_1, e_2, \dots)$ definiert durch $e_1 = [x, y]$ und $e_n = [e_{n-1}, y]$. Dann gilt: Es gibt ein $k \in \mathbb{N}$ so dass für alle $x, y \in G$ gilt $e_k(x, y) = 1 \Leftrightarrow G$ ist nilpotent.*

Definition 6.2. G sei eine Gruppe.

G erfüllt die *n–te Engelbedingung,* falls $e_n(x, y) = 1$ für alle $x, y \in G$. Eine Gruppe, die die n–te Engelbedingung erfüllt, nennen wir *n–Engel Gruppe.*

Wir nennen G eine *n–Engel p–Gruppe,* wenn G eine p–Gruppe und auch eine n–Engel Gruppe ist.

Diese Bezeichnung stammt aus der Theorie der Lie–Algebren, benannt nach dem deutschen Mathematiker Friedrich Engel, der die zum Satz von Zorn analoge Aussage für Lie–Algebren bewies.

Bemerkung 6.3. Ist G eine Gruppe von der Nilpotenzklasse k, ist so gilt nach der Definition $[\, x_0, x_1, \dots, x_k \,] = 1$ für alle $x_0, x_1, \dots, x_k$ aus G, insbesondere auch $e_k(x, y) = [\, x, \underbrace{y, y, \dots, y}_{k} \,] = 1$ für alle $x, y \in G$. Damit ist G eine k–Engel Gruppe.

Nun stellt sich die Frage, inwiefern die "Umkehrung" gilt, d.h. ob man die Nilpotenzklasse einer k–Engel Gruppe nach oben abschätzen kann.

Die 1–Engel Gruppen sind Gruppen von der Nilpotenzklasse 1 und Auflösungslänge 1, also genau die abelschen Gruppen.

Für die 2–Engel Gruppen zeigte F. W. Levi den folgenden Satz:

Satz 6.4. *[Le42] Ist G eine 2–Engel Gruppe, dann ist G von der Nilpotenzklasse höchstens 3. Hat G zusätzlich kein Element der Ordnung 3, so ist G höchstens von der Nilpotenzklasse 2.*

In dieser sowie in den weiteren Abschätzungen wird nicht verlangt, dass die Gruppen endlich sind.

Für die 3–Engel Gruppen ist der folgende Satz von Heineken bekannt:

Satz 6.5. *[He61] Sei G eine 3–Engel Gruppe, die kein Element der Ordnungen 2 und 5 hat, dann ist G höchstens von der Nilpotenzklasse 4.*

Auf die Einschränkung für die Ordnungen der Elemente von G kann nicht verzichtet werden. Gruenberg zeigte [Gr59], dass eine 3–Engel 2–Gruppe existiert, die nicht nilpotent ist. Ein weiteres interessantes Resultat stammt von N. Gupta, und besagt, dass 3–Engel 2–Gruppen auflösbar sind [Gu72]. Für 3–Engel 5–Gruppen ist dies nicht erfüllt. Bachmut und Mochizuki haben eine 3–Engel 5–Gruppe konstruiert, die nicht auflösbar ist [BM71].

Für die 4–Engel Gruppen ist ebenfalls eine Abschätzung bekannt.

Satz 6.6. *[Tr95] [HVL05] Ist G eine 4–Engel Gruppe, die kein Element der Ordnungen $2, 3$ und 5 hat. Dann ist G höchstens von der Nilpotenzklasse 7.*

Die Einschränkung für die Ordnungen der Elemente von G ist ebenfalls notwendig. Nach Satz 6.5 muss man 2–Gruppen und 5–Gruppen ausschließen. Mit MAGMA kann man auch 4–Engel 3–Gruppen berechnen, die von der Nilpotenzklasse > 7 sind.

Für die 5–Engel Gruppen gibt es noch keine analoge Aussagen.

Wir fassen die Ergebnisse nochmal in einer Tabelle zusammen.

Gruppe	Nilpotenzklasse	Ausnahmefälle
1–Engel	1	–
2–Engel	≤ 3	–
3–Engel	≤ 4	2–Gruppen, 5–Gruppen
4–Engel	≤ 7	2–Gruppen, 3–Gruppen, 5–Gruppen

In diesem Kapitel zeigen wir: Wenn man die Nilpotenzklasse einer k–Engel Gruppe abschätzen möchte, muss man fordern, dass die Gruppe kein Element der Ordnung p für alle Primzahlen $p < k$ hat.

Satz 6.7. *Sei p eine Primzahl und $n \in \mathbb{N}$. Es existiert eine $(p+1)$–Engel p–Gruppe von der Nilpotenzklasse n.*

Die Nilpotenzklasse n kann also beliebig groß werden.

Für den Beweis werden wir zeigen, dass Gruppen mit bestimmten Eigenschaften den Satz für beliebige n erfüllen.

Lemma 6.8. *Sei p eine Primzahl und G eine Gruppe, die folgende Eigenschaften erfüllt:*

(1) G ist metabelsch (d. h. G hat die Auflösungslänge 2),
(2) $\exp(G^1) = p$, wobei $G^1 = [G, G]$,
(3) $g^p h = hg^p$ für alle $g \in G$ und $h \in G^1$.

Dann ist G eine $(p+1)$–Engel p–Gruppe.

Beweis. Wir werden zeigen, dass für alle $x, y \in G$ die Gleichheit

$$e_{p+1}(x, y) = 1$$

gilt. Ist $p = 2$, dann gilt:

$$e_3(x,y) = [x,y,y,y] = [x,y,y]^{-1}[x,y,y]^y = ([x,y]^{-1}[x,y]^y)^{-1}([x,y]^{-1}[x,y]^y)^y$$

$$= [x,y]^{-y}[x,y][x,y]^{-y}[x,y]^{y^2} \overset{(1)}{=} [x,y]([x,y]^{-y})^2[x,y]^{y^2} \overset{(2)}{=} [x,y][x,y]^{y^2}$$

$$= [x,y]y^{-2}[x,y]y^2 \overset{(3)}{=} [x,y][x,y]y^{-2}y^2 = [x,y]^2 \overset{(2)}{=} 1.$$

Sei nun p eine ungerade Primzahl. Zuerst zeigen wir mit Induktion, dass für ungerade Zahlen n für alle x und y aus G

$$e_{n+1}(x,y) = \prod_{i=0}^{n} ([x,y]^{(-1)^{i+1}y^i})^{\binom{n}{i}}$$

gilt.

Dabei werden wir die folgenden Eigenschaften benutzen:
$(*)$ Sind $a, b \in G$ und $z \in \mathbb{N}$, dann gilt $(a^z)^b = (a^b)^z$.
$(**)$ $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ für $0 \le k < n$.
$(***)$ Eine Primzahl p teilt $\binom{p}{k}$ wenn $0 < k < p$.

Ist $n = 1$, dann gilt

$$e_2(x,y) = [x,y,y] = [[x,y],y] = [x,y]^{-1}[x,y]^y = \prod_{i=0}^{1} ([x,y]^{(-1)^{i+1}y^i})^{\binom{1}{i}}.$$

Für den Induktionsschritt berechnen wir

$e_{n+2}(x,y) =$

$$
\begin{aligned}
&= && [e_{n+1}(x,y),y] \\
&= && e_{n+1}(x,y)^{-1}y^{-1}e_{n+1}(x,y)y \\
&= && e_{n+1}(x,y)^{-1}e_{n+1}(x,y)^{y} \\
&\overset{Ind.Ann.}{=} && \Big(\prod_{i=0}^{n}([x,y]^{(-1)^{i+1}y^i})^{\binom{n}{i}}\Big)^{-1}\Big(\prod_{i=0}^{n}([x,y]^{(-1)^{i+1}y^i})^{\binom{n}{i}}\Big)^{y} \\
&\overset{(*)}{=} && \prod_{i=0}^{n}([x,y]^{(-1)^{i}y^i})^{\binom{n}{i}}\prod_{i=0}^{n}([x,y]^{(-1)^{i+1}y^{i+1}})^{\binom{n}{i}} \\
&= && \prod_{i=0}^{n}([x,y]^{(-1)^{i}y^i})^{\binom{n}{i}}\prod_{i=1}^{n+1}([x,y]^{(-1)^{i}y^i})^{\binom{n}{i-1}} \\
&= && [x,y]\Big(\prod_{i=1}^{n}([x,y]^{(-1)^{i}y^i})^{\binom{n}{i}}\Big)\Big(\prod_{i=1}^{n}([x,y]^{(-1)^{i}y^i})^{\binom{n}{i-1}}\Big)[x,y]^{(-1)^{n+1}y^{n+1}} \\
&\overset{(1)}{=} && [x,y]\Big(\prod_{i=1}^{n}([x,y]^{(-1)^{i}y^i})^{\binom{n}{i}+\binom{n}{i-1}}\Big)[x,y]^{(-1)^{n+1}y^{n+1}} \\
&\overset{(**)}{=} && \prod_{i=0}^{n+1}([x,y]^{(-1)^{i}y^i})^{\binom{n+1}{i}}
\end{aligned}
$$

Analog beweisen wir, dass

$$e_{n+3}(x,y) = \prod_{i=0}^{n+2}([x,y]^{(-1)^{i+1}y^i})^{\binom{n+2}{i}}.$$

Damit können wir das Lemma beweisen. Ist p eine ungerade Primzahl, dann gilt:

$$
\begin{aligned}
e_{p+1}(x,y) &= && \prod_{i=0}^{p}([x,y]^{(-1)^{i+1}y^i})^{\binom{p}{i}} \\
&\overset{(***),(2)}{=} && [x,y]^{-1}[x,y]^{y^p} \\
&= && [x,y]^{-1}y^{-p}[x,y]y^p \\
&\overset{(3)}{=} && [x,y]^{-1}[x,y]y^{-p}y^p = 1
\end{aligned}
$$

für alle $x, y \in G$. □

Für den Beweis von dem Satz 6.7 müssen wir zeigen, dass für jedes $n \in \mathbb{N}$ eine Gruppe existiert, die die Voraussetzungen des Lemmas 6.8 erfüllt und von der Nilpotenzklasse n ist.

Es ist klar, dass solche Gruppen existieren, denn wir haben keine Einschränkung für die Anzahl der Erzeugenden gemacht. N. Gupta zeigte, dass die von n Elementen erzeugte freie metabelsche Gruppe vom exponent p^2 von der Nilpotenzklasse $n(p-1)+(p-1)^2$ ist [Gu69], also wachsend mit n.

Wir geben Beispiele von Gruppen an, die von n Elementen erzeugt werden, von der Nilpotenzklasse $n+1$ sind und die Voraussetzungen des Lemmas 6.8 erfüllen.

Definition 6.9. Seien p eine Primzahl, $n \in \mathbb{N}$ und $N := \{1, 2, 3, \ldots, n\}$.

Wir definieren $G_p(n)$ als eine Gruppe, die von den Elementen $a_1, \ldots, a_n$ und g_I für alle Teilmengen $I \subseteq N$ erzeugt wird, mit den Relationen:

$$\begin{array}{rcll}
a_i^p & = & 1 & \text{für } i \in \{1, 2, \ldots, n-1\}, \\
a_n^{p^2} & = & 1, & \\
g_I^p & = & 1 & \text{für alle } I \subseteq N, \\
g_{\{j\}} & = & [a_n, a_j] & \text{für } j \in \{1, 2, \ldots, n\}, \\
g_I & = & [g_{I\setminus k}, a_k] & \text{für alle } I \subseteq N \text{ mit } |I| > 1 \\
 & & & \text{und alle } k \in I, \\
[a_i, a_j] & = & 1 & \text{für } i, j \in \{1, 2, 3, \ldots, n-1\}, \\
[g_I, g_J] & = & 1 & \text{für } I, J \subseteq N, \\
[g_I, a_k] & = & 1 & \text{für } k \in I.
\end{array}$$

Beispiel 6.10. $p = 3,\ n = 2,\ N = \{1, 2\}$.

$$\begin{array}{rrrr}
G_3(2) = \langle\, a_1, a_2, g_{\{1\}}, g_{\{1,2\}} \mid & a_1^3 = 1, & [g_{\{1\}}, a_1] = 1, & g_{\{1\}} = [a_2, a_1], \\
 & a_2^9 = 1, & [g_{\{1,2\}}, a_1] = 1, & g_{\{1,2\}} = [g_{\{1\}}, a_2] \\
 & g_{\{1\}}^3 = 1, & [g_{\{1,2\}}, a_2] = 1, & = [a_2, a_1, a_2] \\
 & g_{\{1,2\}}^3 = 1, & [g_{\{1,2\}}, g_{\{1\}}] = 1, & \rangle.
\end{array}$$

Die Gruppe $G_p(n)$ hat folgende Eigenschaften:

Seien $n \in \mathbb{N}$, p Primzahl.

(1) Jedes $g \in G_p(n)$ hat eine (bis auf die Reihenfolge der g_{I_j}) eindeutige Darstellung als

$$g = a_1^{e_1} a_2^{e_2} \ldots a_{n-1}^{e_{n-1}} a_n^{e_n} g_{I_1}^{i_1} \ldots g_{I_t}^{i_t}$$

für Teilmengen $I_1, \ldots, I_t \subseteq N$, mit $I_{i+1} \not\subseteq I_i$, wobei $e_1, \ldots, e_{n-1}, i_1, \ldots, i_t \in \{0, \ldots, p\}$ und $e_n \in \{0, \ldots, p^2\}$.

(2) Die Gruppe $G_p(n)$ hat n Erzeugende $\{a_1, a_2, a_3, \ldots, a_{n-1}, a_n\}$ und $p^{2n+\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{n-1}+\binom{n}{n}}$ Elemente.

(3) Es gilt: $g_N = [a_n, a_1, a_2, a_3, \ldots, a_{n-1}, a_n] \neq 1$, daher ist $G_p(n)$ mindestens von der Nilpotenzklasse $n+1$.

(4) Die Kommutatoruntergruppe $G_p(n)^1 = \langle g_{\{1\}}, \ldots, g_{\{n-1\}} \rangle$ ist abelsch, also ist $G_p(n)$ metabelsch.

(5) $\exp(G_p(n)^1) = p$.

(6) Es gilt $g^p h = hg^p$ für alle $g \in G_p(n)$ und $h \in G_p(n)'$.

Beweis. Es reicht zu zeigen, dass $a_n^p g_I = g_I a_n^p$ für alle Teilmengen $I \subseteq N$. Ist $n \in I$, dann gilt $g_I = a_n^{-1} g_I a_n$. Daraus folgt, dass

$$[g_I, a_n^p] = g_I^{-1} a_n^{-p} g_I a_n^p = g_I^{-1} g_I = 1,$$

und damit $a_n^p g_I = g_I a_n^p$.

Ist $n \notin I$, so gilt $g_I g_{I\cup\{n\}} = a_n^{-1} g_I a_n$. Dann ist

$$[g_I, a_n^p] = g_I^{-1} a_n^{-p} g_I a_n^p = g_I^{-1} g_I (g_{I\cup\{n\}})^p = 1.$$

Beweis von dem Satz 6.7. Aus den Bemerkungen (4), (5) und (6) sehen wir, dass die Gruppe $G_p(n)$ die Voraussetzungen des Lemmas 6.8 erfüllt. Also ist $G_p(n)$ eine $(p+1)$–Engel p–Gruppe von der Nilpotenzklasse mindestens $n+1$.

□

Mit Hilfe der Gruppen $G_p(n)$ können wir einen weiteren Satz beweisen.

Satz 6.11. *Sei p eine Primzahl. Dann existiert eine unendliche $(p+1)$–Engel p–Gruppe, die nicht nilpotent ist. Für alle $n \in \mathbb{N}$ enthält diese Gruppe eine von n Elementen erzeugte Untergruppe von der Nilpotenzklasse mindestens $n+1$.*

Beweis. Für festes p und alle $n \in \mathbb{N}$ ist $G_p(n)$ eine Untergruppe von $G_p(n+1)$. Wir erhalten eine Kette von Gruppen $G_p(2) \leqslant G_p(3) \leqslant G_p(4) \leqslant \ldots$

Sei $G_p(\infty) := \lim_{n\to\infty} G_p(n)$. G_∞ ist eine unendliche $(p+1)$–Engel Gruppe, die nicht nilpotent ist. Ferner ist die Gruppe $G_p(\infty)$ metabelsch und nicht endlich erzeugt. Die Gruppen $G_p(n)$ sind Untergruppen von $G_p(\infty)$ von der Nilpotenzklasse mindestens $n+1$. □

Anhang A

Programme

A.1 Berechnung der Menge S_1

```
G<x,y>:=FreeGroup(2);
x1:=x^-1;
y1:=y^-1;

F3:=[* x, x^-1, y, y^-1, x^2, x*y, x*y^-1, x^-2, x^-1*y, x^-1*y^-1,
y*x, y*x^-1, y^2, y^-1*x, y^-1*x^-1, y^-2, x^3, x^2*y, x^2*y^-1,
x*y*x, x*y*x^-1, x*y^2, x*y^-1*x, x*y^-1*x^-1, x*y^-2, x^-3, x^-2*y,
x^-2*y^-1, y^x, x^-1*y*x^-1, x^-1*y^2, x^-1*y^-1*x, x^-1*y^-1*x^-1,
x^-1*y^-2, y*x^2, y*x*y, y*x*y^-1, y*x^-2, y*x^-1*y, y*x^-1*y^-1,
y^2*x, y^2*x^-1, y^3, y^-1*x^2, x^y, y^-1*x*y^-1, y^-1*x^-2,
y^-1*x^-1*y, y^-1*x^-1*y^-1, y^-2*x, y^-2*x^-1, y^-3 *];

S:=[* *];
for l1 in F3 do
 for l2 in F3 do
  for l3 in F3 do
    Append(~S,<l1,l2,l3>);
  end for;
 end for;
end for;

for N in [1..#S] do
print  S[N];
end for;
```

A.2 Berechnung der Dimensionen von $V(I), V(I_0)$

```
R<t,a,b> := PolynomialRing(Rationals(), 3);
```

```
x := Matrix(2, [t,-1,1,0]);
y := Matrix(2, [1,a,b,1+a*b]);
Id := Matrix(2, [1,0,0,1]);

F3:=[* x, x^-1, y, y^-1, x^2, x*y, x*y^-1, x^-2, x^-1*y, x^-1*y^-1,
y*x, y*x^-1, y^2, y^-1*x, y^-1*x^-1, y^-2, x^3, x^2*y, x^2*y^-1,
x*y*x, x*y*x^-1, x*y^2, x*y^-1*x, x*y^-1*x^-1, x*y^-2, x^-3, x^-2*y,
x^-2*y^-1, y^x, x^-1*y*x^-1, x^-1*y^2, x^-1*y^-1*x, x^-1*y^-1*x^-1,
x^-1*y^-2, y*x^2, y*x*y, y*x*y^-1, y*x^-2, y*x^-1*y, y*x^-1*y^-1,
y^2*x, y^2*x^-1, y^3, y^-1*x^2, x^y, y^-1*x*y^-1, y^-1*x^-2,
y^-1*x^-1*y, y^-1*x^-1*y^-1, y^-2*x, y^-2*x^-1, y^-3 *];

S:=[* *];
for l1 in F3 do
 for l2 in F3 do
  for l3 in F3 do
    Append(~S,<l1,l2,l3>);
  end for;
 end for;
end for;

for i in [1..#S] do
 f:=S[i][1];
 g:=S[i][2];
 h:=S[i][3];
    M:= g^-1*f^-1*g*   h^-1*f^-1*h* g^-1*f*g* h^-1*f*h  - f;
    N:= f - Id;
        I:=ideal< R |{ M[i1,i2] : i1 in [1..2], i2 in [1..2]} > ;
        I0:=ideal< R |{ N[i1,i2] : i1 in [1..2], i2 in [1..2]}> ;
    print i, Dimension(I), Dimension(I0);
end for;
```

A.3 Berechnung von $x, y \in PSL(3, \mathbb{F}_3)$ mit $v_1(x, y) = v_2(x, y)$ und $v_1(x, y) \neq 1$

```
G:=PSL(3,3);
function f(x,y)
return x*y;
end function;

function g(x,y)
return y*x^-1*y^-1;
end function;

function h(x,y)
return x*y*x; // die erste Sequenz
end function;

J:=0;
```

```
N:=0;
C:=ConjugacyClasses(G);
 for w in [1..#C] do
 x:=C[w][3];
 for y in G do
   if (f(x,y)^g(x,y), f(x,y)^h(x,y)) eq f(x,y) eq true
   and f(x,y) ne G!1 eq true then J:=J+1;
   else N:=N+1;
   end if;
 J,N;
 end for;
 end for;
```

Anhang B

Die Menge S_3

$f(x,y)$	$g(x,y)$	$h(x,y)$
xy	x	$x^{-2}y^{-1}$
xy	x	$yx^{-1}y^{-1}$
xy	y^{-1}	$x^{-2}y^{-1}$
xy	y^{-1}	$yx^{-1}y^{-1}$
xy	xyx	$x^{-2}y^{-1}$
xy	xyx	$yx^{-1}y^{-1}$
xy	$x^{-2}y^{-1}$	x
xy	$x^{-2}y^{-1}$	y^{-1}
xy	$x^{-2}y^{-1}$	$x^{-1}y^{-1}$
xy	$x^{-2}y^{-1}$	xyx
xy	$x^{-2}y^{-1}$	$y^{-1}x^{-1}y^{-1}$
xy	$x^{-1}yx$	yx
xy	yxy^{-1}	$x^{-2}y^{-1}$
xy	$yx^{-1}y^{-1}$	x
xy	$yx^{-1}y^{-1}$	y^{-1}
xy	$yx^{-1}y^{-1}$	$x^{-1}y^{-1}$
xy	$yx^{-1}y^{-1}$	xyx
xy	$yx^{-1}y^{-1}$	$y^{-1}x^{-1}y^{-1}$
xy	y^2x	yx
xy	$y^{-1}x^{-1}y^{-1}$	$x^{-2}y^{-1}$
xy	$y^{-1}x^{-1}y^{-1}$	$yx^{-1}y^{-1}$
$x^{-1}y^{-1}$	x^{-1}	x^2y
$x^{-1}y^{-1}$	x^{-1}	$y^{-1}xy$
$x^{-1}y^{-1}$	y	x^2y
$x^{-1}y^{-1}$	y	$y^{-1}xy$
$x^{-1}y^{-1}$	x^2y	x^{-1}
$x^{-1}y^{-1}$	x^2y	y
$x^{-1}y^{-1}$	x^2y	xy
$x^{-1}y^{-1}$	x^2y	$x^{-1}y^{-1}x^{-1}$
$x^{-1}y^{-1}$	x^2y	yxy

$f(x,y)$	$g(x,y)$	$h(x,y)$
$x^{-1}y^{-1}$	$xy^{-1}x^{-1}$	$y^{-1}x^{-1}$
$x^{-1}y^{-1}$	$x^{-1}y^{-1}x^{-1}$	x^2y
$x^{-1}y^{-1}$	$x^{-1}y^{-1}x^{-1}$	$y^{-1}xy$
$x^{-1}y^{-1}$	yxy	x^2y
$x^{-1}y^{-1}$	yxy	$y^{-1}xy$
$x^{-1}y^{-1}$	$y^{-1}xy$	x^{-1}
$x^{-1}y^{-1}$	$y^{-1}xy$	y
$x^{-1}y^{-1}$	$y^{-1}xy$	xy
$x^{-1}y^{-1}$	$y^{-1}xy$	$x^{-1}y^{-1}x^{-1}$
$x^{-1}y^{-1}$	$y^{-1}xy$	yxy
$x^{-1}y^{-1}$	$y^{-1}x^{-1}y$	x^2y
$x^{-1}y^{-1}$	$y^{-2}x^{-1}$	$y^{-1}x^{-1}$
yx	x^{-1}	$xy^{-1}x^{-1}$
yx	x^{-1}	$y^{-2}x^{-1}$
yx	y	$xy^{-1}x^{-1}$
yx	y	$y^{-2}x^{-1}$
yx	x^2y	xy
yx	xyx^{-1}	$y^{-2}x^{-1}$
yx	$xy^{-1}x^{-1}$	x^{-1}
yx	$xy^{-1}x^{-1}$	y
yx	$xy^{-1}x^{-1}$	$y^{-1}x^{-1}$
yx	$xy^{-1}x^{-1}$	$x^{-1}y^{-1}x^{-1}$
yx	$xy^{-1}x^{-1}$	yxy
yx	$x^{-1}y^{-1}x^{-1}$	$xy^{-1}x^{-1}$
yx	$x^{-1}y^{-1}x^{-1}$	$y^{-2}x^{-1}$
yx	yxy	$xy^{-1}x^{-1}$
yx	yxy	$y^{-2}x^{-1}$
yx	$y^{-1}xy$	xy
yx	$y^{-2}x^{-1}$	x^{-1}
yx	$y^{-2}x^{-1}$	y

$f(x,y)$	$g(x,y)$	$h(x,y)$
yx	$y^{-2}x^{-1}$	$y^{-1}x^{-1}$
yx	$y^{-2}x^{-1}$	$x^{-1}y^{-1}x^{-1}$
yx	$y^{-2}x^{-1}$	yxy
$y^{-1}x^{-1}$	x	$x^{-1}yx$
$y^{-1}x^{-1}$	x	y^2x
$y^{-1}x^{-1}$	y^{-1}	$x^{-1}yx$
$y^{-1}x^{-1}$	y^{-1}	y^2x
$y^{-1}x^{-1}$	xyx	$x^{-1}yx$
$y^{-1}x^{-1}$	xyx	y^2x
$y^{-1}x^{-1}$	$x^{-2}y^{-1}$	$x^{-1}y^{-1}$
$y^{-1}x^{-1}$	$x^{-1}yx$	x
$y^{-1}x^{-1}$	$x^{-1}yx$	y^{-1}
$y^{-1}x^{-1}$	$x^{-1}yx$	yx
$y^{-1}x^{-1}$	$x^{-1}yx$	xyx
$y^{-1}x^{-1}$	$x^{-1}yx$	$y^{-1}x^{-1}y^{-1}$
$y^{-1}x^{-1}$	$x^{-1}y^{-1}x$	y^2x
$y^{-1}x^{-1}$	$yx^{-1}y^{-1}$	$x^{-1}y^{-1}$
$y^{-1}x^{-1}$	y^2x	x
$y^{-1}x^{-1}$	y^2x	y^{-1}
$y^{-1}x^{-1}$	y^2x	yx
$y^{-1}x^{-1}$	y^2x	xyx
$y^{-1}x^{-1}$	y^2x	$y^{-1}x^{-1}y^{-1}$
$y^{-1}x^{-1}$	$y^{-1}x^{-1}y^{-1}$	$x^{-1}yx$
$y^{-1}x^{-1}$	$y^{-1}x^{-1}y^{-1}$	y^2x
x^2y	x^{-1}	yx^2
x^2y	yx	xyx
x^2y	yx	yx^2
xyx	x	$yx^{-1}y^{-1}$
xyx	$x^{-1}y^{-1}$	$yx^{-1}y^{-1}$
xyx	$yx^{-1}y^{-1}$	x
xyx	$yx^{-1}y^{-1}$	$x^{-1}y^{-1}$
xyx	$yx^{-1}y^{-1}$	$x^{-2}y^{-1}$
xyx	$y^{-1}xy$	x^2y
$x^{-2}y^{-1}$	x	$y^{-1}x^{-2}$
$x^{-2}y^{-1}$	$y^{-1}x^{-1}$	$x^{-1}y^{-1}x^{-1}$
$x^{-2}y^{-1}$	$y^{-1}x^{-1}$	$y^{-1}x^{-2}$
$x^{-1}y^{-1}x^{-1}$	x^{-1}	$y^{-1}xy$
$x^{-1}y^{-1}x^{-1}$	xy	$y^{-1}xy$
$x^{-1}y^{-1}x^{-1}$	$yx^{-1}y^{-1}$	$x^{-2}y^{-1}$
$x^{-1}y^{-1}x^{-1}$	$y^{-1}xy$	x^{-1}
$x^{-1}y^{-1}x^{-1}$	$y^{-1}xy$	xy
$x^{-1}y^{-1}x^{-1}$	$y^{-1}xy$	x^2y
yx^2	x	x^2y
yx^2	x^{-1}	$y^{-1}x^{-1}$
yx^2	yx	$y^{-1}x^{-1}$

$f(x,y)$	$g(x,y)$	$h(x,y)$
yx^2	$y^{-1}x^{-1}$	x^{-1}
yx^2	$y^{-1}x^{-1}$	yx
yx^2	$y^{-1}x^{-1}$	$x^{-1}y^{-1}x^{-1}$
yxy^{-1}	y	$y^{-1}x^{-1}$
yxy^{-1}	y	$xy^{-1}x^{-1}$
yxy^{-1}	y	$x^{-1}y^{-1}x^{-1}$
yxy^{-1}	y^{-1}	$y^{-1}xy$
yxy^{-1}	xy	$x^{-1}y^{-1}x^{-1}$
yxy^{-1}	yx	$y^{-1}x^{-1}$
yxy^{-1}	yx	$xy^{-1}x^{-1}$
yxy^{-1}	yx	$x^{-1}y^{-1}x^{-1}$
yxy^{-1}	yx^{-1}	$y^{-1}x^{-1}$
yxy^{-1}	yx^{-1}	$xy^{-1}x^{-1}$
yxy^{-1}	yx^{-1}	$x^{-1}y^{-1}x^{-1}$
yxy^{-1}	$y^{-1}x$	x
yxy^{-1}	$y^{-1}x$	$y^{-1}xy$
yxy^{-1}	$y^{-1}x^{-1}$	x^{-1}
yxy^{-1}	$y^{-1}x^{-1}$	y
yxy^{-1}	$y^{-1}x^{-1}$	yx
yxy^{-1}	$y^{-1}x^{-1}$	yx^{-1}
yxy^{-1}	$y^{-1}x^{-1}$	yx^2
yxy^{-1}	$y^{-1}x^{-1}$	yx^{-2}
yxy^{-1}	xyx^{-1}	$y^{-1}x^{-1}$
yxy^{-1}	$xy^{-1}x$	x
yxy^{-1}	$xy^{-1}x^{-1}$	x^{-1}
yxy^{-1}	$xy^{-1}x^{-1}$	y
yxy^{-1}	$xy^{-1}x^{-1}$	yx
yxy^{-1}	$xy^{-1}x^{-1}$	yx^{-1}
yxy^{-1}	$xy^{-1}x^{-1}$	yx^2
yxy^{-1}	$xy^{-1}x^{-1}$	yx^{-2}
yxy^{-1}	$x^{-1}y^{-1}x$	x
yxy^{-1}	$x^{-1}y^{-1}x^{-1}$	x^{-1}
yxy^{-1}	$x^{-1}y^{-1}x^{-1}$	y
yxy^{-1}	$x^{-1}y^{-1}x^{-1}$	yx
yxy^{-1}	$x^{-1}y^{-1}x^{-1}$	yx^{-1}
yxy^{-1}	$x^{-1}y^{-1}x^{-1}$	yx^2
yxy^{-1}	$x^{-1}y^{-1}x^{-1}$	yx^{-2}
yxy^{-1}	yx^2	$y^{-1}x^{-1}$
yxy^{-1}	yx^2	$xy^{-1}x^{-1}$
yxy^{-1}	yx^2	$x^{-1}y^{-1}x^{-1}$
yxy^{-1}	yx^{-2}	$y^{-1}x^{-1}$
yxy^{-1}	yx^{-2}	$xy^{-1}x^{-1}$
yxy^{-1}	yx^{-2}	$x^{-1}y^{-1}x^{-1}$
$yx^{-1}y^{-1}$	y	$y^{-1}x$
$yx^{-1}y^{-1}$	y	$xy^{-1}x$

$f(x,y)$	$g(x,y)$	$h(x,y)$
$yx^{-1}y^{-1}$	y	$x^{-1}y^{-1}x$
$yx^{-1}y^{-1}$	y^{-1}	$y^{-1}x^{-1}y$
$yx^{-1}y^{-1}$	$x^{-1}y$	$xy^{-1}x$
$yx^{-1}y^{-1}$	yx	$y^{-1}x$
$yx^{-1}y^{-1}$	yx	$xy^{-1}x$
$yx^{-1}y^{-1}$	yx	$x^{-1}y^{-1}x$
$yx^{-1}y^{-1}$	yx^{-1}	$y^{-1}x$
$yx^{-1}y^{-1}$	yx^{-1}	$xy^{-1}x$
$yx^{-1}y^{-1}$	yx^{-1}	$x^{-1}y^{-1}x$
$yx^{-1}y^{-1}$	$y^{-1}x$	x
$yx^{-1}y^{-1}$	$y^{-1}x$	y
$yx^{-1}y^{-1}$	$y^{-1}x$	yx
$yx^{-1}y^{-1}$	$y^{-1}x$	yx^{-1}
$yx^{-1}y^{-1}$	$y^{-1}x$	yx^{2}
$yx^{-1}y^{-1}$	$y^{-1}x$	yx^{-2}
$yx^{-1}y^{-1}$	$y^{-1}x^{-1}$	x^{-1}
$yx^{-1}y^{-1}$	$y^{-1}x^{-1}$	$y^{-1}x^{-1}y$
$yx^{-1}y^{-1}$	$xy^{-1}x$	x
$yx^{-1}y^{-1}$	$xy^{-1}x$	y
$yx^{-1}y^{-1}$	$xy^{-1}x$	yx
$yx^{-1}y^{-1}$	$xy^{-1}x$	yx^{-1}
$yx^{-1}y^{-1}$	$xy^{-1}x$	yx^{2}
$yx^{-1}y^{-1}$	$xy^{-1}x$	yx^{-2}
$yx^{-1}y^{-1}$	$xy^{-1}x^{-1}$	x^{-1}
$yx^{-1}y^{-1}$	$x^{-1}yx$	$y^{-1}x$
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x$	x
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x$	y
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x$	yx
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x$	yx^{-1}
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x$	yx^{2}
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x$	yx^{-2}
$yx^{-1}y^{-1}$	$x^{-1}y^{-1}x^{-1}$	x^{-1}
$yx^{-1}y^{-1}$	yx^{2}	$y^{-1}x$
$yx^{-1}y^{-1}$	yx^{2}	$xy^{-1}x$
$yx^{-1}y^{-1}$	yx^{2}	$x^{-1}y^{-1}x$
$yx^{-1}y^{-1}$	yx^{-2}	$y^{-1}x$
$yx^{-1}y^{-1}$	yx^{-2}	$xy^{-1}x$
$yx^{-1}y^{-1}$	yx^{-2}	$x^{-1}y^{-1}x$
$y^{-1}xy$	y	yxy^{-1}
$y^{-1}xy$	y^{-1}	yx^{-1}
$y^{-1}xy$	y^{-1}	xyx^{-1}
$y^{-1}xy$	y^{-1}	$x^{-1}yx^{-1}$
$y^{-1}xy$	xy^{-1}	$x^{-1}yx^{-1}$
$y^{-1}xy$	yx	x
$y^{-1}xy$	yx	yxy^{-1}

$f(x,y)$	$g(x,y)$	$h(x,y)$
$y^{-1}xy$	yx^{-1}	x^{-1}
$y^{-1}xy$	yx^{-1}	y^{-1}
$y^{-1}xy$	yx^{-1}	$y^{-1}x$
$y^{-1}xy$	yx^{-1}	$y^{-1}x^{-1}$
$y^{-1}xy$	yx^{-1}	$y^{-1}x^{2}$
$y^{-1}xy$	yx^{-1}	$y^{-1}x^{-2}$
$y^{-1}xy$	$y^{-1}x$	yx^{-1}
$y^{-1}xy$	$y^{-1}x$	yxx^{-1}
$y^{-1}xy$	$y^{-1}x$	xyx^{-1}
$y^{-1}xy$	$y^{-1}x$	$x^{-1}yx^{-1}$
$y^{-1}xy$	$y^{-1}x^{-1}$	yx^{-1}
$y^{-1}xy$	$y^{-1}x^{-1}$	xyx^{-1}
$y^{-1}xy$	$y^{-1}x^{-1}$	$x^{-1}yx^{-1}$
$y^{-1}xy$	xyx	x
$y^{-1}xy$	xyx^{-1}	x^{-1}
$y^{-1}xy$	xyx^{-1}	y^{-1}
$y^{-1}xy$	xyx^{-1}	$y^{-1}x$
$y^{-1}xy$	xyx^{-1}	$y^{-1}x^{-1}$
$y^{-1}xy$	xyx^{-1}	$y^{-1}x^{2}$
$y^{-1}xy$	xyx^{-1}	$y^{-1}x^{-2}$
$y^{-1}xy$	$xy^{-1}x^{-1}$	yx^{-1}
$y^{-1}xy$	$x^{-1}yx$	x
$y^{-1}xy$	$x^{-1}yx^{-1}$	x^{-1}
$y^{-1}xy$	$x^{-1}yx^{-1}$	y^{-1}
$y^{-1}xy$	$x^{-1}yx^{-1}$	$y^{-1}x$
$y^{-1}xy$	$x^{-1}yx^{-1}$	$y^{-1}x^{-1}$
$y^{-1}xy$	$x^{-1}yx^{-1}$	$y^{-1}x^{2}$
$y^{-1}xy$	$x^{-1}yx^{-1}$	$y^{-1}x^{-2}$
$y^{-1}xy$	$y^{-1}x^{2}$	yx^{-1}
$y^{-1}xy$	$y^{-1}x^{2}$	xyx^{-1}
$y^{-1}xy$	$y^{-1}x^{2}$	$x^{-1}yx^{-1}$
$y^{-1}xy$	$y^{-1}x^{-2}$	yx^{-1}
$y^{-1}xy$	$y^{-1}x^{-2}$	xyx^{-1}
$y^{-1}xy$	$y^{-1}x^{-2}$	$x^{-1}yx^{-1}$
$y^{-1}x^{-2}$	x	yx
$y^{-1}x^{-2}$	x^{-1}	$x^{-2}y^{-1}$
$y^{-1}x^{-2}$	yx	x
$y^{-1}x^{-2}$	yx	$y^{-1}x^{-1}$
$y^{-1}x^{-2}$	yx	xyx
$y^{-1}x^{-2}$	$y^{-1}x^{-1}$	yx
$y^{-1}x^{-1}y$	y	$yx^{-1}y^{-1}$
$y^{-1}x^{-1}y$	y^{-1}	yx
$y^{-1}x^{-1}y$	y^{-1}	xyx
$y^{-1}x^{-1}y$	y^{-1}	$x^{-1}yx$
$y^{-1}x^{-1}y$	$x^{-1}y^{-1}$	xyx
$y^{-1}x^{-1}y$	yx	x

$f(x,y)$	$g(x,y)$	$h(x,y)$
$y^{-1}x^{-1}y$	yx	y^{-1}
$y^{-1}x^{-1}y$	yx	$y^{-1}x$
$y^{-1}x^{-1}y$	yx	$y^{-1}x^{-1}$
$y^{-1}x^{-1}y$	yx	$y^{-1}x^{2}$
$y^{-1}x^{-1}y$	yx	$y^{-1}x^{-2}$
$y^{-1}x^{-1}y$	yx^{-1}	x^{-1}
$y^{-1}x^{-1}y$	yx^{-1}	$yx^{-1}y^{-1}$
$y^{-1}x^{-1}y$	$y^{-1}x$	yx
$y^{-1}x^{-1}y$	$y^{-1}x$	xyx
$y^{-1}x^{-1}y$	$y^{-1}x$	$x^{-1}yx$
$y^{-1}x^{-1}y$	$y^{-1}x^{-1}$	yx
$y^{-1}x^{-1}y$	$y^{-1}x^{-1}$	xyx
$y^{-1}x^{-1}y$	$y^{-1}x^{-1}$	$x^{-1}yx$
$y^{-1}x^{-1}y$	xyx	x
$y^{-1}x^{-1}y$	xyx	y^{-1}
$y^{-1}x^{-1}y$	xyx	$y^{-1}x$
$y^{-1}x^{-1}y$	xyx	$y^{-1}x^{-1}$

$f(x,y)$	$g(x,y)$	$h(x,y)$
$y^{-1}x^{-1}y$	xyx	$y^{-1}x^{2}$
$y^{-1}x^{-1}y$	xyx	$y^{-1}x^{-2}$
$y^{-1}x^{-1}y$	xyx^{-1}	x^{-1}
$y^{-1}x^{-1}y$	$x^{-1}yx$	x
$y^{-1}x^{-1}y$	$x^{-1}yx$	y^{-1}
$y^{-1}x^{-1}y$	$x^{-1}yx$	$y^{-1}x$
$y^{-1}x^{-1}y$	$x^{-1}yx$	$y^{-1}x^{-1}$
$y^{-1}x^{-1}y$	$x^{-1}yx$	$y^{-1}x^{2}$
$y^{-1}x^{-1}y$	$x^{-1}yx$	$y^{-1}x^{-2}$
$y^{-1}x^{-1}y$	$x^{-1}yx^{-1}$	x^{-1}
$y^{-1}x^{-1}y$	$x^{-1}y^{-1}x$	yx
$y^{-1}x^{-1}y$	$y^{-1}x^{2}$	yx
$y^{-1}x^{-1}y$	$y^{-1}x^{2}$	xyx
$y^{-1}x^{-1}y$	$y^{-1}x^{2}$	$x^{-1}yx$
$y^{-1}x^{-1}y$	$y^{-1}x^{-2}$	yx
$y^{-1}x^{-1}y$	$y^{-1}x^{-2}$	xyx
$y^{-1}x^{-1}y$	$y^{-1}x^{-2}$	$x^{-1}yx$

Anhang C

Polynome

$$h(a,a_0,b) = b^9a_0^{11}a^{15}+b^{10}a_0^{10}a^{14}+b^7a_0^{13}a^{13}+b^7a_0^9a^{17}+b^8a_0^{12}a^{12}+b^6a_0^{12}a^{14}+b^8a_0^8a^{16}+b^5a_0^{15}a^{11}+b^9a_0^7a^{15}+b^5a_0^{11}a^{15}+b^5a_0^7a^{19}+b^6a_0^{14}a^{10}+b^6a_0^{12}a^{12}+b^{10}a_0^6a^{14}+b^6a_0^{10}a^{14}+b^4a_0^{10}a^{16}+b^6a_0^6a^{18}+b^{11}a_0^9a^9+b^7a_0^{13}a^9+b^3a_0^{17}a^9+b^7a_0^{11}a^{11}+b^{11}a_0^5a^{13}+b^3a_0^{13}a^{13}+b^3a_0^9a^{17}+b^3a_0^5a^{21}+b^{12}a_0^8a^8+b^8a_0^{12}a^8+b^4a_0^{16}a^8+b^{10}a_0^8a^{10}+b^8a_0^{10}a^{10}+b^6a_0^{12}a^{10}+b^2a_0^{16}a^{10}+b^{12}a_0^4a^{12}+b^4a_0^{12}a^{12}+b^6a_0^8a^{14}+b^4a_0^{10}a^{14}+b^4a_0^8a^{16}+b^2a_0^8a^{18}+b^4a_0^4a^{20}+b^{17}a_0^3a^7+b^{13}a_0^7a^7+b^9a_0^9a^9+b^7a_0^{11}a^9+b^{13}a_0^3a^{11}+b^9a_0^7a^{11}+ba_0^{15}a^{11}+b^9a_0^3a^{15}+b^5a_0^3a^{19}+ba_0^7a^{19}+b^{18}a_0^2a^6+b^{14}a_0^6a^6+b^{12}a_0^6a^8+b^6a_0^{12}a^8+b^2a_0^{16}a^8+b^{14}a_0^2a^{10}+b^{10}a_0^6a^{10}+b^4a_0^{12}a^{10}+b^2a_0^{14}a^{10}+b^6a_0^8a^{12}+a_0^{14}a^{12}+b^{10}a_0^2a^{14}+b^2a_0^8a^{16}+b^6a_0^2a^{18}+b^2a_0^6a^{18}+a_0^6a^{20}+b^{11}a_0^9a^5+b^3a_0^{17}a^5+b^{11}a_0^7a^7+b^9a_0^9a^7+b^3a_0^{15}a^7+b^3a_0^{13}a^9+b^5a_0^9a^{11}+b^3a_0^{11}a^{11}+b^3a_0^7a^{15}+b^{12}a_0^8a^4+b^4a_0^{16}a^4+b^8a_0^{10}a^6+b^4a_0^{14}a^6+b^2a_0^{16}a^6+b^8a_0^8a^8+b^6a_0^{10}a^8+b^2a_0^{14}a^8+b^{10}a_0^4a^{10}+b^6a_0^8a^{10}+b^4a_0^{10}a^{10}+b^2a_0^{12}a^{10}+a_0^{14}a^{10}+b^4a_0^8a^{12}+b^4a_0^6a^{14}+b^2a_0^4a^{18}+a_0^6a^{18}+b^{17}a_0^3a^3+b^{13}a_0^7a^3+b^9a_0^{11}a^3+b^5a_0^{15}a^3+b^{13}a_0^5a^5+b^{11}a_0^7a^5+b^5a_0^{13}a^5+b^3a_0^{15}a^5+b^9a_0^7a^7+b^5a_0^{11}a^7+ba_0^{13}a^9+b^9a_0^3a^{11}+b^5a_0^7a^{11}+b^5a_0^5a^{13}+ba_0^9a^{13}+b^{18}a_0^2a^2+b^{14}a_0^6a^2+b^{10}a_0^{10}a^2+b^6a_0^{14}a^2+b^{16}a_0^2a^4+b^{14}a_0^4a^4+b^{10}a_0^8a^4+b^8a_0^{10}a^4+b^6a_0^{12}a^4+b^2a_0^{16}a^4+b^{10}a_0^6a^6+b^4a_0^{12}a^6+b^2a_0^{14}a^6+b^{12}a_0^2a^8+b^{10}a_0^4a^8+b^4a_0^{10}a^8+b^{10}a_0^2a^{10}+b^2a_0^{10}a^{10}+a_0^{12}a^{10}+b^8a_0^2a^{12}+b^6a_0^4a^{12}+b^2a_0^8a^{12}+a_0^{10}a^{12}+a_0^8a^{14}+b^4a_0^2a^{16}+b^2a_0^4a^{16}+a_0^6a^{16}+b^{13}a_0^5a^3+b^5a_0^{13}a^3+b^3a_0^{13}a^5+b^9a_0^5a^7+b^5a_0^9a^7+b^3a_0^{11}a^7+ba_0^{13}a^7+b^3a_0^9a^9+b^3a_0^7a^{11}+ba_0^9a^{11}+b^3a_0^5a^{13}+b^{16}a_0^2a^2+b^{14}a_0^4a^2+b^{12}a_0^6a^2+b^8a_0^{10}a^2+b^6a_0^{12}a^2+b^4a_0^{14}a^2+b^{10}a_0^6a^4+b^4a_0^{12}a^4+b^2a_0^{14}a^4+b^{12}a_0^2a^6+b^{10}a_0^4a^6+b^6a_0^8a^6+b^2a_0^{10}a^8+a_0^{12}a^8+b^8a_0^2a^{10}+b^4a_0^6a^{10}+b^2a_0^8a^{10}+a_0^{10}a^{10}+b^2a_0^6a^{12}+b^4a_0^2a^{14}+a_0^6a^{14}+a_0^4a^{16}+b^5a_0^{11}a^3+ba_0^{15}a^3+b^9a_0^5a^5+b^5a_0^9a^5+b^3a_0^{11}a^5+ba_0^{13}a^5+b^9a_0^3a^7+b^5a_0^7a^7+b^5a_0^5a^9+b^3a_0^7a^9+b^5a_0^3a^{11}+b^{12}a_0^4a^2+b^{10}a_0^6a^2+b^6a_0^{10}a^2+b^4a_0^{12}a^2+b^{10}a_0^4a^4+b^6a_0^8a^4+a_0^{14}a^4+b^6a_0^6a^6+b^2a_0^{10}a^6+b^6a_0^4a^8+b^4a_0^6a^8+b^6a_0^2a^{10}+b^4a_0^4a^{10}+b^2a_0^6a^{10}+a_0^6a^{12}+b^2a_0^2a^{14}+b^9a_0^5a^3+b^5a_0^9a^3+ba_0^{13}a^3+b^3a_0^9a^5+b^5a_0^5a^7+b^3a_0^7a^7+ba_0^5a^{11}+b^{16}+b^{12}a_0^4+b^8a_0^8+b^4a_0^{12}+b^{10}a_0^4a^2+b^6a_0^8a^2+b^4a_0^{10}a^2+b^2a_0^{12}a^2+a_0^{14}a^2+b^{12}a^4+b^4a_0^8a^4+b^2a_0^{10}a^4+a_0^{12}a^4+b^6a_0^4a^6+b^4a_0^6a^6+b^2a_0^8a^6+b^8a^8+b^4a_0^4a^8+b^2a_0^6a^8+a_0^6a^{10}+b^4a^{12}+a_0^4a^{12}+b^5a_0^7a^3+b^5a_0^5a^5+b^3a_0^7a^5+ba_0^9a^5+ba_0^7a^7+ba_0^5a^9+ba_0^3a^{11}+b^8a_0^4a^2+b^6a_0^6a^2+b^4a_0^8a^2+b^2a_0^{10}a^2+a_0^{12}a^2+b^6a_0^4a^4+b^4a_0^4a^6+b^2a_0^6a^6+a_0^8a^6+b^4a_0^2a^8+a_0^6a^8+b^2a_0^2a^{10}+a_0^2a^{12}+b^5a_0^5a^3+ba_0^9a^3+b^8a_0^4+b^4a_0^8+b^6a_0^4a^2+b^4a_0^6a^2+b^2a_0^8a^2+b^2a_0^6a^4+a_0^8a^4+b^4a_0^2a^6+a_0^6a^6+a_0^4a^8+a_0^2a^{10}+ba_0^5a^5+b^4a_0^4a^2+b^2a_0^6a^2+a_0^8a^2+b^2a_0^4a^4+b^2a_0^2a^6+a_0^4a^6+ba_0^5a^3+b^4a_0^4+a_0^8+b^2a_0^4a^2+b^4a^4+a_0^4a^4+a^8+ba_0^3a^3+b^2a_0^2a^2+a_0^4a^2+a_0^2a^4+a_0^4+a_0^2a^2+1.$$

$$\tilde{f}(a,a_0) = a_0^{19}a^{19}+a_0^{16}a^{22}+a_0^{15}a^{23}+a_0^{12}a^{26}+a_0^{11}a^{27}+a_0^8a^{30}+a_0^{20}a^{17}+a_0^{19}a^{18}+a_0^{18}a^{19}+a_0^{16}a^{21}+a_0^{14}a^{23}+a_0^{12}a^{25}+a_0^{10}a^{27}+a_0^7a^{30}+a_0^{21}a^{15}+a_0^{19}a^{17}+a_0^{18}a^{18}+a_0^{17}a^{19}+a_0^{15}a^{21}+a_0^{13}a^{23}+a_0^{11}a^{25}+a_0^6a^{30}+a_0^{22}a^{13}+a_0^{21}a^{14}+a_0^{19}a^{16}+a_0^{18}a^{17}+a_0^{16}a^{19}+a_0^{15}a^{20}+a_0^{12}a^{23}+a_0^9a^{26}+a_0^5a^{30}+a_0^{19}a^{15}+a_0^{17}a^{17}+a_0^{14}a^{20}+a_0^{11}a^{23}+a_0^{10}a^{24}+a_0^9a^{25}+a_0^8a^{26}+a_0^6a^{28}+a_0^{19}a^{14}+a_0^{16}a^{17}+a_0^{13}a^{20}+a_0^{12}a^{21}+a_0^{10}a^{23}+a_0^8a^{25}+a_0^{21}a^{11}+a_0^{20}a^{12}+a_0^{16}a^{16}+a_0^{14}a^{18}+a_0^{13}a^{19}+a_0^{12}a^{20}+a_0^{10}a^{22}+a_0^7a^{25}+a_0^5a^{27}+a_0^4a^{28}+a_0^{22}a^9+a_0^{21}a^{10}+a_0^{18}a^{13}+a_0^{16}a^{15}+a_0^{15}a^{16}+a_0^{11}a^{20}+a_0^{10}a^{21}+a_0^9a^{22}+a_0^8a^{23}+a_0^7a^{24}+a_0^5a^{26}+a_0^4a^{27}+a_0^{20}a^{10}+a_0^{19}a^{11}+a_0^{16}a^{14}+a_0^{14}a^{16}+a_0^{13}a^{17}+a_0^{11}a^{19}+a_0^9a^{21}+a_0^6a^{24}+a_0^5a^{25}+$$

$$a_0^4a^{26}+a_0^{19}a^{10}+a_0^{15}a^{14}+a_0^{13}a^{16}+a_0^{12}a^{17}+a_0^{10}a^{19}+a_0^9a^{20}+a_0^8a^{21}+a_0^6a^{23}+a_0^5a^{24}+a_0^3a^{26}+a_0^{21}a^7+a_0^{19}a^9+a_0^{17}a^{11}+a_0^{14}a^{14}+a_0^{13}a^{15}+a_0^{12}a^{16}+a_0^{11}a^{17}+a_0^{10}a^{18}+a_0^7a^{21}+a_0^6a^{22}+a_0^{22}a^5+a_0^{21}a^6+a_0^{19}a^8+a_0^{18}a^9+a_0^{17}a^{10}+a_0^{13}a^{14}+a_0^{10}a^{17}+a_0^6a^{21}+a_0^5a^{22}+a_0^3a^{24}+a_0^{19}a^7+a_0^{17}a^9+a_0^{15}a^{11}+a_0^{14}a^{12}+a_0^{13}a^{13}+a_0^{10}a^{16}+a_0^9a^{17}+a_0^7a^{19}+a_0^4a^{22}+a_0^3a^{23}+a_0^2a^{24}+a_0^{19}a^6+a_0^{17}a^8+a_0^{16}a^9+a_0^{15}a^{10}+a_0^{13}a^{12}+a_0^{12}a^{13}+a_0^9a^{16}+a_0^7a^{18}+a_0^6a^{19}+a_0^5a^{20}+a_0^4a^{21}+a_0^3a^{22}+a_0^2a^{23}+a_0^{21}a^3+a_0^{20}a^4+a_0^{17}a^7+a_0^{16}a^8+a_0^{15}a^9+a_0^{13}a^{11}+a_0^{12}a^{12}+a_0^{10}a^{14}+a_0^9a^{15}+a_0^7a^{17}+a_0^2a^{22}+a_0^{22}a+a_0^{21}a^2+a_0^{18}a^5+a_0^{17}a^6+a_0^{15}a^8+a_0^{14}a^9+a_0^{13}a^{10}+a_0^{12}a^{11}+a_0^{10}a^{13}+a_0^9a^{14}+a_0^8a^{15}+a_0^7a^{16}+a_0^5a^{18}+a_0^2a^{21}+a_0^{20}a^2+a_0^{17}a^5+a_0^{15}a^7+a_0^{14}a^8+a_0^{12}a^{10}+a_0^{11}a^{11}+a_0^{10}a^{12}+a_0^9a^{13}+a_0^8a^{14}+a_0^2a^{20}+a_0^{20}a+a_0^{18}a^3+a_0^{17}a^4+a_0^{15}a^6+a_0^{13}a^8+a_0^{12}a^9+a_0^{11}a^{10}+a_0^{10}a^{11}+a_0^8a^{13}+a_0^7a^{14}+a_0^6a^{15}+a_0^4a^{17}+a_0^3a^{18}+a_0^2a^{19}+a_0^{18}a^2+a_0^{17}a^3+a_0^{15}a^5+a_0^{12}a^8+a_0^8a^{12}+a_0^7a^{13}+a_0^6a^{14}+a_0^5a^{15}+a_0^2a^{18}+a_0^{15}a^4+a_0^{14}a^5+a_0^{13}a^6+a_0^6a^{13}+a_0^5a^{14}+a_0^4a^{15}+a_0^{17}a+a_0^{15}a^3+a_0^9a^9+a_0^5a^{13}+a_0^4a^{14}+a_0^{16}a+a_0^{15}a^2+a_0^{14}a^3+a_0^{13}a^4+a_0^{12}a^5+a_0^{11}a^6+a_0^{10}a^7+a_0^9a^8+a_0^8a^9+a_0^6a^{11}+a_0^4a^{13}+a_0^2a^{15}+a_0a^{16}+a_0^{15}a+a_0^{13}a^3+a_0^{11}a^5+a_0^9a^7+a_0^6a^{10}+a_0^3a^{13}+a_0^3a^{12}+a_0^2a^{13}+a_0a^{14}+a_0^{13}a+a_0^9a^5+a_0^5a^9+a_0^3a^{11}+a_0a^{13}+a_0^4a^9+a_0^3a^{10}+a_0^2a^{11}+a_0a^{12}+a_0^3a^9+a_0a^{11}+a_0a^9.$$

Anhang D

Beispiele für x und y in $\mathrm{Sz}(2^p)$ für $3 \leq p \leq 50$

Mit MP bezeichnen wir das Minimalpolynom.

$p = 3,\ MP = t^5 + t^2 + 1$

$$
\begin{array}{lcl}
a & = & t, \\
a_0 & = & t^2 + t, \\
b & = & t^2, \\
b_0 & = & t, \\
c & = & t^2 + t, \\
c_0 & = & t^2, \\
d & = & t^2 + 1, \\
d_0 & = & t + 1.
\end{array}
$$

$p = 5,\ MP = t^5 + t^2 + 1$

$$
\begin{array}{lcl}
a & = & t + 1, \\
a_0 & = & t^3 + t^2, \\
b & = & 0, \\
b_0 & = & 0, \\
c & = & t^4 + t^2 + t + 1, \\
c_0 & = & t^4 + t^2 + 1, \\
d & = & t^4 + t^3 + t^2 + t, \\
d_0 & = & t^3 + t.
\end{array}
$$

$p = 7,\ MP = t^7 + t + 1$

$$
\begin{array}{lcl}
a & = & t^3 + t, \\
a_0 & = & t^5 + t^3 + t, \\
b & = & t^5 + t^2 + t + 1, \\
b_0 & = & t^6 + t^5 + t^3 + t^2 + 1, \\
c & = & t^5 + t^2 + 1, \\
c_0 & = & t^6 + t^5 + t^4 + t^3 + 1, \\
d & = & t^6 + t^4 + t^3 + 1, \\
d_0 & = & t^6 + t^5 + t^2 + t + 1.
\end{array}
$$

$p = 11,\ MP = t^{11} + t^2 + 1$

$$
\begin{array}{lcl}
a & = & t^2 + t, \\
a_0 & = & t^{10} + t^9 + t^7 + t^6 + t^4 + t^3 + t + 1, \\
b & = & t^7 + t^5 + t^4 + t^2 + t + 1, \\
b_0 & = & t^6 + t^5 + t^2 + 1, \\
c & = & t^{10} + t^9 + t^8 + t^7 + t^5 + t + 1, \\
c_0 & = & t^8 + t^7 + t^3 + t, \\
d & = & t^{10} + t^9 + t^7 + t^5 + t^3 + t^2 + t + 1, \\
d_0 & = & t^{10} + t^6 + t^4 + t^2.
\end{array}
$$

$p = 13,\ MP = t^{13} + t^4 + t^3 + t + 1$

$$
\begin{array}{lcl}
a & = & t^2 + t, \\
a_0 & = & t^9 + t^8 + t^6 + 1, \\
b & = & t^8 + t^3 + t, \\
b_0 & = & t^{11} + t^9 + t^8 + t^7 + t^5 + t^4 + t^2 + t + 1, \\
c & = & t^{12} + t^{10} + t^9 + t^8 + t^7 + t^6 + 1, \\
c_0 & = & t^{12} + t^{11} + t^9 + t^7 + t^6 + t^4 + t^2 + 1, \\
d & = & t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^4 + t^3 + t^2, \\
d_0 & = & t^9 + t^8 + t^2.
\end{array}
$$

$p = 17,\ MP = t^{17} + t^3 + 1$

$$
\begin{aligned}
a &= t^2 + t + 1,\\
a_0 &= t^{12} + t^{11} + t^{10} + t^7 + t^3 + t^2 + t + 1,\\
b &= t^{15} + t^{14} + t^{11} + t^{10} + t^6 + t^4,\\
b_0 &= t^{12} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^4 + t^3,\\
c &= t^{15} + t^{12} + t^{10} + t^9 + t^4 + t^3 + t^2 + 1,\\
c_0 &= t^{16} + t^{14} + t^{10} + t^9 + t^7 + t^6 + t^4 + t^3 + t + 1,\\
d &= t^{15} + t^{13} + t^{11} + t^{10} + t^9 + t^8 + t^5 + t^4 + t^3,\\
d_0 &= t^{13} + t^{10} + t^8 + t.
\end{aligned}
$$

$p = 19,\ MP = t^{19} + t^5 + t^2 + t + 1$

$$
\begin{aligned}
a &= t,\\
a_0 &= t^{18} + t^{17} + t^{12} + t^{11} + t^7 + t^6 + t^5 + t^2 + 1,\\
b &= t^{16} + t^{15} + t^{14} + t^{12} + t^8 + t^6 + t^5 + t^2 + t + 1,\\
b_0 &= t^{18} + t^{16} + t^{15} + t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^6 + t^2 + t + 1,\\
c &= t^{16} + t^{14} + t^{12} + t^{11} + t^{10} + t^8 + t^7 + t^6 + t^4 + t^3 + 1,\\
c_0 &= t^{18} + t^{17} + t^{16} + t^5 + t^4 + t^2,\\
d &= t^{18} + t^{16} + t^{15} + t^{11} + t^{10} + t^8 + t^7 + t^5 + 1,\\
d_0 &= t^{18} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^{12} + t^{11} + t^8 + t^7 + t^6 + t^5 + t^3 + t^2 + t.
\end{aligned}
$$

$p = 23,\ MP = t^{23} + t^5 + 1$

$$
\begin{aligned}
a &= t,\\
a_0 &= t^{22} + t^{21} + t^{20} + t^{19} + t^{17} + t^{15} + t^{13} + t^{12} + t^{10} + t^7 + t^5 + t^4,\\
b &= t^{20} + t^{19} + t^{18} + t^{15} + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^8 + t^7 + t^6 + t^4 + t + 1,\\
b_0 &= t^{21} + t^{19} + t^{18} + t^{17} + t^{14} + t^{13} + t^9 + t^8 + 1,\\
c &= t^{21} + t^{20} + t^{17} + t^{16} + t^{13} + t^{12} + t^{11} + t^{10} + t^6 + t^5 + t^3,\\
c_0 &= t^{22} + t^{20} + t^{18} + t^{17} + t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 + t^2,\\
d &= t^{22} + t^{21} + t^{19} + t^{18} + t^{16} + t^{15} + t^{14} + t^{13} + t^9 + t^7 + t^6 + t^4 + t + 1,\\
d_0 &= t^{17} + t^{15} + t^{14} + t^9 + t^7 + t^6 + t^4 + t^3 + 1.
\end{aligned}
$$

$p = 29,\ MP = t^{29} + t^2 + 1$

$$
\begin{aligned}
a &= t^2 + t,\\
a_0 &= t^{28} + t^{26} + t^{20} + t^{18} + t^{17} + t^{11} + t^{10} + t^8 + t^4 + t^3 + t,\\
b &= t^{26} + t^{25} + t^{24} + t^{23} + t^{21} + t^{20} + t^{19} + t^{18} + t^{16} + t^{12} + t^{11} + t^{10} + t^8 + t^7 + t^5 + t,\\
b_0 &= t^{28} + t^{24} + t^{23} + t^{21} + t^{20} + t^{17} + t^{16} + t^{12} + t^{11} + t^{10} + t^7 + t^5 + t^3 + t^2,\\
c &= t^{25} + t^{23} + t^{20} + t^{19} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^9 + t^2 + 1,\\
c_0 &= t^{28} + t^{25} + t^{20} + t^{19} + t^{18} + t^{17} + t^{16} + t^{13} + t^{10} + t^9 + t^7 + t^6 + t^3 + t + 1,\\
d &= t^{27} + t^{25} + t^{23} + t^{21} + t^{20} + t^{19} + t^{18} + t^{17} + t^{16} + t^{13} + t^{12} + t^{10} + t^8 + t^6 + t^4 + t^3 + t + 1,\\
d_0 &= t^{28} + t^{27} + t^{26} + t^{21} + t^{18} + t^{15} + t^{13} + t^{11} + t^9 + t^8 + t^5 + t + 1.
\end{aligned}
$$

$p = 31,\ MP = t^{31} + t^3 + 1$

$$
\begin{aligned}
a &= t^3,\\
a_0 &= t^{24} + t^{10} + t^9 + t^2 + t,\\
b &= t^{30} + t^{25} + t^{23} + t^{21} + t^{20} + t^{18} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^{11} + t^9 + t^8 + t^4 + t^3 + t,\\
b_0 &= t^{30} + t^{29} + t^{24} + t^{23} + t^{21} + t^{20} + t^{17} + t^{11} + t^9 + t^8 + t^7 + t^4 + t^3 + t^2 + t,\\
c &= t^{27} + t^{24} + t^{20} + t^{19} + t^{18} + t^{16} + t^{14} + t^{12} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^4 + t^3,\\
c_0 &= t^{30} + t^{28} + t^{26} + t^{25} + t^{20} + t^{18} + t^{17} + t^{16} + t^{15} + t^{11} + t^{10} + t^8 + t^7 + t^5 + t^2,\\
d &= t^{29} + t^{28} + t^{27} + t^{26} + t^{23} + t^{22} + t^{16} + t^{15} + t^{14} + t^{13} + t^7 + t^6 + t^3 + t^2 + 1,\\
d_0 &= t^{29} + t^{28} + t^{25} + t^{24} + t^{23} + t^{21} + t^{20} + t^{17} + t^{14} + t^{10} + t^8 + t^7 + t^4 + t^2 + t + 1.
\end{aligned}
$$

$p = 37,\ MP = t^{37} + t^5 + t^4 + t^3 + t^2 + t + 1$

$$
\begin{aligned}
a &= t^2 + t, \\
a_0 &= t^{34} + t^{33} + t^{31} + t^{30} + t^{29} + t^{28} + t^{27} + t^{26} + t^{19} + t^{18} + t^{17} + t^{16} + t^{14} + t^{13} + \\
&\quad t^{10} + t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1, \\
b &= t^{33} + t^{30} + t^{29} + t^{28} + t^{26} + t^{25} + t^{23} + t^{16} + t^{12} + t^7 + t^4 + t^3 + t^2 + 1, \\
b_0 &= t^{35} + t^{33} + t^{32} + t^{28} + t^{26} + t^{25} + t^{23} + t^{22} + t^{20} + t^{18} + t^{16} + t^{12} + t^{11} + t^{10} + \\
&\quad t^8 + t^7 + t^5 + t^4 + t^3 + t, \\
c &= t^{36} + t^{35} + t^{33} + t^{32} + t^{31} + t^{29} + t^{19} + t^{14} + t^{11} + t^{10} + t^9 + t^7 + t, \\
c_0 &= t^{36} + t^{34} + t^{33} + t^{30} + t^{26} + t^{24} + t^{21} + t^{17} + t^{15} + t^{13} + t^{12} + t^9 + t^7 + t^6 + t^5 + t^4 + 1, \\
d &= t^{36} + t^{35} + t^{34} + t^{33} + t^{30} + t^{26} + t^{24} + t^{22} + t^{21} + t^{16} + t^{14} + t^{12} + t^{10} + t^9 + \\
&\quad t^8 + t^7 + t^6 + t^4 + t^3 + 1, \\
d_0 &= t^{35} + t^{32} + t^{31} + t^{30} + t^{29} + t^{27} + t^{26} + t^{25} + t^{24} + t^{22} + t^{19} + t^{17} + t^{14} + t^{10} + \\
&\quad t^8 + t^6 + t^5 + t^3 + t^2.
\end{aligned}
$$

$p = 41,\ MP = t^{41} + t^3 + 1$

$$
\begin{aligned}
a &= t, \\
a_0 &= t^{38} + t^{37} + t^{36} + t^{35} + t^{34} + t^{32} + t^{31} + t^{29} + t^{26} + t^{23} + t^{21} + t^{20} + t^{18} + t^{17} + \\
&\quad t^{15} + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^7 + t^6 + t^4 + t^3 + t^2 + t, \\
b &= t^{38} + t^{34} + t^{32} + t^{28} + t^{27} + t^{26} + t^{23} + t^{22} + t^{21} + t^{20} + t^{17} + t^{14} + t^{12} + t^{10} + \\
&\quad t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t + 1, \\
b_0 &= t^{39} + t^{38} + t^{36} + t^{35} + t^{34} + t^{32} + t^{30} + t^{29} + t^{27} + t^{26} + t^{24} + t^{23} + t^{22} + t^{18} + \\
&\quad t^{17} + t^{15} + t^{12} + t^7 + t^5 + t^3 + t^2 + 1, \\
c &= t^{40} + t^{38} + t^{36} + t^{33} + t^{32} + t^{31} + t^{29} + t^{28} + t^{27} + t^{26} + t^{24} + t^{23} + t^{22} + t^{19} + \\
&\quad t^{18} + t^{14} + t^{12} + t^{10} + t^7 + t^3 + t + 1, \\
c_0 &= t^{37} + t^{35} + t^{33} + t^{31} + t^{26} + t^{23} + t^{17} + t^{15} + t^{14} + t^{11} + t^{10} + t^4 + t^3 + 1, \\
d &= t^{40} + t^{37} + t^{35} + t^{34} + t^{33} + t^{32} + t^{30} + t^{28} + t^{25} + t^{24} + t^{23} + t^{19} + t^{18} + t^{17} + \\
&\quad t^{11} + t^{10} + t^9 + t^6 + t^5 + 1, \\
d_0 &= t^{40} + t^{39} + t^{37} + t^{32} + t^{26} + t^{23} + t^{20} + t^{19} + t^{14} + t^{13} + t^{11} + t^{10} + t^7 + t^3 + t^2 + t + 1.
\end{aligned}
$$

$p = 43,\ MP = t^{43} + t^6 + t^4 + t^3 + 1$

$$
\begin{aligned}
a &= t^2 + t + 1, \\
a_0 &= t^{44} + t^{41} + t^{40} + t^{38} + t^{37} + t^{34} + t^{33} + t^{32} + t^{31} + t^{28} + t^{27} + t^{26} + t^{25} + t^{23} + \\
&\quad t^{22} + t^{18} + t^{17} + t^{16} + t^{12} + t^{10} + t^9 + t^7 + t^6 + t^5 + t^2 + t + 1, \\
b &= t^{45} + t^{41} + t^{40} + t^{39} + t^{35} + t^{33} + t^{31} + t^{30} + t^{28} + t^{25} + t^{24} + t^{23} + t^{19} + t^{18} + \\
&\quad t^{17} + t^{12} + t^{11} + t^9 + t^8 + t^6 + t^4 + 1, \\
b_0 &= t^{46} + t^{42} + t^{41} + t^{38} + t^{36} + t^{35} + t^{34} + t^{32} + t^{30} + t^{27} + t^{20} + t^{19} + t^{17} + t^{16} + \\
&\quad t^{13} + t^{12} + t^8 + t^6 + t^5 + t^4 + t^2 + t + 1, \\
c &= t^{40} + t^{33} + t^{31} + t^{30} + t^{29} + t^{26} + t^{25} + t^{24} + t^{23} + t^{21} + t^{19} + t^{16} + t^{15} + t^{14} + \\
&\quad t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^2 + t + 1, \\
c_0 &= t^{46} + t^{45} + t^{40} + t^{39} + t^{38} + t^{35} + t^{34} + t^{32} + t^{30} + t^{29} + t^{28} + t^{23} + t^{22} + t^{21} + \\
&\quad t^{20} + t^{16} + t^{12} + t^{11} + t^{10} + t^8 + t^3 + t + 1, \\
d &= t^{45} + t^{44} + t^{37} + t^{35} + t^{34} + t^{33} + t^{28} + t^{26} + t^{24} + t^{22} + t^{20} + t^{18} + t^{17} + t^{16} + \\
&\quad t^{15} + t^{14} + t^{10} + t^9 + t^7 + t^6 + t^4 + 1, \\
d_0 &= t^{46} + t^{45} + t^{44} + t^{43} + t^{41} + t^{40} + t^{38} + t^{33} + t^{32} + t^{26} + t^{24} + t^{23} + t^{19} + t^{17} + \\
&\quad t^{16} + t^{15} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^4 + 1.
\end{aligned}
$$

$p = 47,\ MP = t^{47} + t^5 + 1$

$$
\begin{aligned}
a &= t^2 + t + 1, \\
a_0 &= t^{44} + t^{41} + t^{40} + t^{38} + t^{37} + t^{34} + t^{33} + t^{32} + t^{31} + t^{28} + t^{27} + t^{26} + t^{25} + t^{23} + \\
&\quad t^{22} + t^{18} + t^{17} + t^{16} + t^{12} + t^{10} + t^9 + t^7 + t^6 + t^5 + t^2 + t + 1, \\
b &= t^{45} + t^{41} + t^{40} + t^{39} + t^{35} + t^{33} + t^{31} + t^{30} + t^{28} + t^{25} + t^{24} + t^{23} + t^{19} + t^{18} + \\
&\quad t^{17} + t^{12} + t^{11} + t^9 + t^8 + t^6 + t^4 + 1, \\
b_0 &= t^{46} + t^{42} + t^{41} + t^{38} + t^{36} + t^{35} + t^{34} + t^{32} + t^{30} + t^{27} + t^{20} + t^{19} + t^{17} + t^{16} + \\
&\quad t^{13} + t^{12} + t^8 + t^6 + t^5 + t^4 + t^2 + t + 1, \\
c &= t^{40} + t^{33} + t^{31} + t^{30} + t^{29} + t^{26} + t^{25} + t^{24} + t^{23} + t^{21} + t^{19} + t^{16} + t^{15} + t^{14} + \\
&\quad t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^2 + t + 1, \\
c_0 &= t^{46} + t^{45} + t^{40} + t^{39} + t^{38} + t^{35} + t^{34} + t^{32} + t^{30} + t^{29} + t^{28} + t^{23} + t^{22} + t^{21} + \\
&\quad t^{20} + t^{16} + t^{12} + t^{11} + t^{10} + t^8 + t^3 + t + 1, \\
d &= t^{45} + t^{44} + t^{37} + t^{35} + t^{34} + t^{33} + t^{28} + t^{26} + t^{24} + t^{22} + t^{20} + t^{18} + t^{17} + t^{16} + \\
&\quad t^{15} + t^{14} + t^{10} + t^9 + t^7 + t^6 + t^4 + 1, \\
d_0 &= t^{46} + t^{45} + t^{44} + t^{43} + t^{41} + t^{40} + t^{38} + t^{33} + t^{32} + t^{26} + t^{24} + t^{23} + t^{19} + t^{17} + \\
&\quad t^{16} + t^{15} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^4 + 1.
\end{aligned}
$$

Literaturverzeichnis

[AS88] A. Adolphson, S. Sperber, *On the degree of the L–function associated with an exponential sum*, Composito Math. **68** (1988) 125–159.

[BM71] S. Bachmuth and H.Y. Mochizuki, *Third Engel groups and the Macdonald–Neumann conjecture*, Bull. Austral. Math. Soc. **5** (1971) 379–386.

[DSW] G. Davidoff, P. Sarnak, A. Valette *Elementary Number Theory, Group Theory and Ramanujan Graphs*, Cambridge University Press, 2003.

[BGGKPP] T.Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskii, G. Pfister and E. Plotkin, *Engel-like identities charakterising finite solvable groups*, Max-Planck-Institut für Mathematik. Preprint Series (2003) **87.**

[He61] H. Heineken, *Engelsche Elemente der Länge drei*, Illinois J. Math. **5** (1961) 681–707.

[dJP00] T. de Jong, G. Pfister *Local analytic geometry*, Vieweg–Verlag, Braunschweig/Wiesbaden, 2000.

[FJ86] M. Fried, M. Jarden, *Field Arithmetic*, Springer–Verlag, Berlin, 1986.

[Fu69] W. Fulton, *Algebraic curves*, W. A. BEBJAMIN, INC, New York, 1969.

[Fu98] W. Fulton, *Intersection Theory*, Springer–Verlag, Berlin–Heidelberg, 1998.

[GL02] S. R. Ghorpade, G. Lachlaud, *Etale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Moscow Math. J. **2** (2002) 589–631.

[GP02] G. M. Greuel, G. Pfister, *A SINGULAR Introduction to Commutative Algebra*, Springer–Verlag, Berlin–Heidelberg, 2002.

[Gr59] K.W. Gruenberg, *The Engel elements of a soluble group*, Illinois J. Math. **3** (1959) 151–168.

[Gu72] N. Gupta, *Third–Engel 2–groups are soluble*, Canad. Math. Bull. **15** (1972) 523–524.

[Gu69] N. Gupta, *The free metabelian group of exponent p^2*, Proc. Amer. Math. Soc. **22** (1969) 375–376.

[Ha77] R. Hartshorne, *Algebraic Geometry*, Springer–Verlag, New York–Heidelberg–Berlin, 1977.

[H67] B.Huppert *Endliche Gruppen* I, Springer-Verlag Berlin Heidelberg New York, 1967.

[HB82] B. Huppert, N. Blackburn, *Finite Groups*, III, Springer–Verlag, Berlin–Heidelberg–New York, 1982.

[Ka01] N. M. Katz, *Sums of Betti numbers in arbitrary charakteristics*, Finite Fields and Their Applications **7** (2001) 29–44.

[Le42] F. W. Levi, *Groups in which the commutator operations satisfy certain algebraic conditions*, J. Indian Math. Soc. **6** (1942) 87–97.

[M80] J. S. Milne, *Etale Cohomology*, Princeton University Press, Princeton, New Jersey, 1980.

[M89] J. S. Milne, *Lectures on Etale Cohomology*, `www.math.lsa.umich.edu/ milne/`

[Sh94] I. R. Shafarevich, *Basic Algebraic Geometry*, 2nd ed., Springer–Verlag, New York–Berlin–Heidelberg, 1994.

[S62] M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962) 105–145.

[Th68] J. Thompson, *Non–solvable finite groups all of whose subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968) 383–437.

[Tr95] G. Traustason *On 4–Engel groups*, J. Algebra. (2) **178** (1995) 414-429.

[HVL05] G. Havas and M. R. Vaughan-Lee *4–Engel groups are locally nilpotent*, International Journal of Algebra and Computation **15** (2005) 649-682.

[BWW05] J. N. Bray, J. S. Wilson, R. A. Wilson, *A charakterisation of finite soluble groups by laws in two variables*, Bull. London Math. Soc. **37** (2005) 179–186.

[Z63] M. Zorn, *Nilpotency of finite groups*, Bull. Amer. Math. Soc. **42** (1936) 485–486.

Die hier vorgelegte Dissertation habe ich eigenständig und ohne unerlaubte Hilfe angefertigt. Die Dissertation wurde in der vorgelegten oder in ähnlicher Form noch bei keiner anderen Institution eingereicht. Ich habe bisher keine erfolglosen Promotionsversuche unternommen.

Düsseldorf, den 15. Februar 2007