Universität des Saarlandes
Naturwissenschaftlich-Technische Fakultät I
Mathematik

Bachelorarbeit

Punktkonfigurationen über endlichen Körpern

vorgelegt von
Marius Bohn

im Dezember 2012

Betreuer

Prof. Dr. Ernst-Ulrich Gekeler

Erklärung

Hiermit versichere ich, die Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel durchgeführt zu haben.

Saarbrücken, im Dezember 2012

Vorwort

Die vorliegende Arbeit mit dem Titel „Punktkonfigurationen über endlichen Körpern“ zur Erlangung des Bachelorabschlusses in Mathematik ist in der Zeit vom 1.Oktober 2012 bis zum 31. Dezember 2012 unter Betreuung von Prof. Dr. Ernst-Ulrich Gekeler entstanden. Über diesen Zeitraum hinweg habe ich mich mit einem speziellen, von G. Pólya in den 1930er Jahren entwickelten, Zählverfahren für die Operation von Gruppen auf Mengen auseinandergesetzt, mit dessen Hilfe es möglich ist die Anzahl an l-Punktkonfigurationen der projektiven Gerade $\mathbb{P}^1(\mathbb{F}_q)$ über dem endlichen Körper $\mathbb{F}_q$ mit q Elementen, die durch Operation der Gruppe $PGL(2,\mathbb{F}_q)$ ineinander überführt werden können, zu bestimmen. Dabei kann man eine $l-$ Punktkonfiguration als eine Zweifärbung in $\mathbb{P}^1(\mathbb{F}_q)$ interpretieren, wobei etwa l Punkte grün gefärbt sind. Dann stellt sich die Frage nach der Anzahl an solchen Färbungen, wobei wir zwei Färbungen als gleich identifizieren, wenn sie durch ein Element aus $PGL(2,\mathbb{F}_q)$ aufeinander abgebildet werden können.
Für drei Punkte liefert ein bekannter Satz aus der projektiven Geometrie unmittelbar die Antwort auf diese Frage. Bei vier Punkten ist es möglich die Anzahl an solchen Färbungen, einerseits mittels einer projektiven Invarianten (Doppelverhältnis von vier Punkten) durch direktes Ausrechnen der Bahnen zu bestimmen und andererseits die Stabilisatorgruppe von vier Punkten in Abhängigkeit von q anzugeben. Diese klassische Vorgehensweise ist bei der Bestimmung der Zahl an Fünfpunktkonfigurationen schon deutlich schwieriger und wird bei steigendem l nahezu unmöglich.
Dagegen liefert uns die durch Pólya begründete Abzähltheorie eine elegante Möglichkeit die Zahl an $l-$ Punktkonfigurationen mit verhältnismäßig geringem Rechenaufwand durch Auswertung eines speziellen Polynoms in $q+1$ Unbestimmten (Zykelzeiger), welches die Zykelstruktur von $PGL(2,\mathbb{F}_q)$ auf $\mathbb{P}^1(\mathbb{F}_q)$ in abstrakter Weise kodiert, zu bestimmen. Dies soll in der Arbeit explizit für $l \in \{3,4,5\}$ durchgeführt, und für höhere Werte von l angedeutet werden. Dabei werde ich das Ergebnis für $l = 3,4$ mit der „von Hand“ ausgerechneten Zahl abgleichen. Abschließend gehe ich auch kurz auf spezielle Drei- und Vierfärbungen auf $\mathbb{P}^1(\mathbb{F}_q)$ ein, denn der Satz von Polya gibt uns prinzipiell auch die Möglichkeit die Frage nach der Zahl an k- Färbungen auf l- Punkten anzugeben, wenngleich die Komplexität der Auswertung hierbei stark abhängig ist von der Art der speziellen Färbung.
Beginnen werde ich jedoch mit den für das Verständnis notwendigen Grundlagen. Hierbei wird insbesondere eine Einteilung der Gruppe $GL(2,\mathbb{F}_q)$ in Konjugationsklassen vorgenommen, da man sich üblicherweise bei der Bestimmung des Zykelzeigers zunutze macht, dass die Zykelstruktur invariant unter Konjugation ist.
Die Arbeit richtet sich an Leser, die das Grundvokabular der Gruppentheorie verinnerlicht haben und mit endlichen Körpern vertraut sind. Einige Grundkenntnisse der Algebra und Zahlentheorie sind ebenfalls hilfreich, aber nicht essentiell für das Verständnis der Arbeit, zumal die wichtigsten Begriffe nochmals zusammengestellt werden. Auf den Beweis des für diese Arbeit zentralen Satzes von Pólya will ich verzichten, da dieser in jedem weiterführenden Werk zur Kombinatorik zu finden ist. Eine entsprechende Referenz ist angegeben.
In Anhang A findet der historisch interessierte Leser allerdings eine Würdigung der Originalarbeit von G.Pólya und einige Anmerkung zur Entstehungsgeschichte des Satzes von Pólya.
Außerdem kann man den Zykelzeiger für l- Punktkonfigurationen relativ leicht mit Unterstützung des Computers auswerten. Dazu habe ich am Ende der Arbeit in Anhang B einige Tabellen angefügt, wo der entsprechende Koeffizient im Zykelzeiger in Körpern bestimmter Charakteristik für kleine Werte von l numerisch bestimmt wurde.

Die Berechnungen, die zur Erstellung der Tabellen nötig waren wurden mit Hilfe des Computeralgebrasystems *GAP Groups Algorithms Programming* durchgeführt. Ein entsprechender Programmcode ist beigefügt und das Programm kann beispielsweise an den Rechnern der Universität ausgeführt werden.

Saarbrücken, im Dezember 2012
Marius Bohn

Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich über mein gesamtes Studium hinweg, und insbesondere bei der Anfertigung meiner Bachelorarbeit, unterstützt haben.
Mein besonderer Dank gilt Prof. Dr. Ernst-Ulrich Gekeler, zum einen für die interessante Thematik und zum anderen für die stete und intensive Betreuung während der Anfertigung dieser Arbeit.
Außerdem geht ein Dank an Sebastian Hahn, der mir wertvolle Hinweise bei stilistischen Fragen bezüglich des Umgangs mit TeX gab.
Darüber hinaus danke ich meinen Eltern für die nötige finanzielle Rückendeckung und häusliche Unterstützung während meines Mathematikstudiums.

Notation

Die folgende allgemein übliche Notation ist für die gesamt Arbeit gültig:

- $\mathbb{N} = \{1, 2, 3, ...\}$,
- $\mathbb{N}_0 = \{0, 1, 2, ...\}$,
- $\mathbb{Q}$ = Körper der rationalen Zahlen,
- $\mathbb{F}_q$ = Körper mit q Elementen, wobei $q = p^n, n \in \mathbb{N}$ stets eine Primzahlpotenz ist,
- $\mathbb{F}_q^*$ = Einheitengruppe des Körpers $\mathbb{F}_q$,
- $p = \text{char}(\mathbb{F}_q)$ die Charakteristik des endlichen Körpers $\mathbb{F}_q$.

Die übrigen Bezeichnungen werden im Verlaufe der Arbeit eingeführt. Insbesondere verwenden wir neben den üblichen Konventionen zur besseren Übersicht ab Abschnitt 3 einige Abkürzungen, was an der entsprechenden Stelle vermerkt wird.

Inhaltsverzeichnis

1 Grundlagen

1.1 Die Gruppe $GL(2, \mathbb{F}_q)$

1.1.1 Definition.

Zentraler Bestandteil der gesamten Arbeit ist die allgemeine lineare Gruppe (für 2×2 Matrizen) über einem endlichen Körper mit q Elementen:

$$GL(2, \mathbb{F}_q) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0\}$$

$$\cup$$

$$SL(2, \mathbb{F}_q) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1\}$$

1.1.2 Satz

1. Für die Kardinalität der Gruppen ergibt sich:

$$|GL(2, \mathbb{F}_q)| = (q^2 - 1)(q^2 - q)$$

$$|SL(2, \mathbb{F}_q)| = q(q^2 - 1)$$

2. Die so genannten Transvektionen erzeugen die Gruppe $SL(2, \mathbb{F}_q)$, d.h. es gilt:

$$SL(2, \mathbb{F}_q) =< \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \mid x, y \in \mathbb{F}_q >$$

$$GL(2, \mathbb{F}_q) =< \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, \begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix} \mid x, y \in \mathbb{F}_q,\ w \in \mathbb{F}_q \setminus \{0\} >$$

Beweis. 1. Gesucht sind alle invertierbaren Matrizen mit Einträgen aus $\mathbb{F}_q$, d.h. insbesondere alle über $\mathbb{F}_q$ linear unabhängigen Vektoren

$$\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}$$

Hiervon gibt es offenbar $(q^2 - 1)(q^2 - q) = q(q - 1)(q^2 - 1)$.

Die Determinantenabbildung

$$\det :\ GL(2, \mathbb{F}_q) \to \mathbb{F}_q \setminus \{0\}$$

ist ein Gruppenepimorphismus.
Surjektivität: Sei $x \in \mathbb{F}_q \setminus \{0\}$. Dann ist ein mögliches Urbild gegeben durch:

$$A = \begin{pmatrix} 1 & y \\ 0 & x \end{pmatrix},\ y \in \mathbb{F}_q$$

Die Abbildung ist ein Gruppenhomomorphismus gemäß dem Determinantenmultiplikationssatz mit Kern(det) $= SL(2, \mathbb{F}_q)$. Der Homomorphiesatz für Gruppen liefert:

$$GL(2, \mathbb{F}_q)/SL(2, \mathbb{F}_q) \cong (\mathbb{F}_q^*, \cdot)$$

Somit gilt:

$$|SL(2, \mathbb{F}_q)| = \frac{|GL(2, \mathbb{F}_q)|}{|(\mathbb{F}_q^*, \cdot)|} = \frac{q(q-1)(q^2-1)}{q-1} = q(q^2-1)$$

2. Zunächst rechnet man leicht nach, dass die unteren und oberen Dreiecksmatrizen mit dem Eintrag 1 auf der Hauptdiagonalen (Transvektionen) eine Gruppe bilden, d.h. das inverse Element einer Transvektion ist wiederum eine Transvektion. Wir haben folgende Situation:

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} = \begin{pmatrix} 1+yz & y \\ x+xyz+z & xy+1 \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{F}_q)$$

Wir nehmen zunächst $O.B.d.A$ an, dass gilt: $b \neq 0$.
In diesem Fall erhalten wir also mit den Einträgen $y = b, z = \frac{a-1}{b}, x = \frac{d-1}{b}$ eine Darstellung wie gewünscht für A.
Nun sei $b = 0$. Also hat A die Form:

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

mit $d = a^{-1} \neq 0$. Damit stellen wir fest, dass gilt:

$$\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a \\ c & c+a^{-1} \end{pmatrix} \in SL(2, \mathbb{F}_q)$$

Demnach folgern wir:

$$A = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

wie gewünscht. Ist nun allgemeiner $A \in GL(2, \mathbb{F}_q)$ mit $\det(A) = w \neq 0$ gegeben, so können wir A darstellen in der Form:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix}$$

mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{F}_q)$ wie zuvor konstruiert.

□

(vgl. [Lan79], Seite 188, Lemma 3)

1.2 Die projektive Gerade $\mathbb{P}^1(\mathbb{F}_q)$

1.2.1 Definition.
Sei V ein $K-$Vektorraum. Dann bezeichnet $\mathbb{P}(V) = \{\text{1-dim Untervektorräume von V}\}$. $\mathbb{P}(V)$ heißt der zu V gehörige projektive Raum. Die Elemente von $\mathbb{P}(V)$ bezeichnen wir als Punkte, obwohl es sich formal um Ursprungsgeraden handelt. Für $\dim(V) < \infty$ setzen wir $\dim(\mathbb{P}(V)) := \dim(V) - 1$. Weiter sei $\mathbb{P}^n(K) = \mathbb{P}(K^{n+1})$ der kanonische n-dimensionale projektive Raum über K.
(siehe auch [Fis01], Seite 134, Definition 3.1.1)

1.2.2 Bemerkung.

- Alternativ können wir den n-dimensionalen kanonischen projektiven Raum auch über eine Äquivalenzrelation einführen: Auf $K^{n+1} \setminus \{0\}$ gelte:

$$x \sim y :\Leftrightarrow \exists \lambda \in K \setminus \{0\} : y = \lambda x.$$

  Wir definieren dann

$$\mathbb{P}^n(K) := (K^{n+1} \setminus \{0\})/\sim$$

  als Menge der Äquivalenzklassen. Wir erhalten als kanonische Abbildung:

$$\begin{aligned} \rho : \quad & K^{n+1} \setminus \{0\} \to \mathbb{P}^n(K) \\ & (x_0, ..., x_n) \mapsto [(x_0, ..., x_n)] \\ & \qquad = \{\lambda(x_0, ..., x_n) \mid \lambda \in K\} =: (x_0 : ... : x_n) \end{aligned}$$

  Man nennt dieses $n+1$-Tupel auch die homogenen Koordinaten eines Punktes in $\mathbb{P}^n(K)$. Es gilt offenbar:

$$(x_0 : ... : x_n) = (x_0' : ... : x_n') \Leftrightarrow \exists \lambda \in K^*$$

  mit $x_0' = \lambda x_0, \cdots, x_n' = \lambda x_n$, d.h. die homogenen Koordinaten sind nur bis auf einen gemeinsamen, von Null verschiedenen, Faktor festgelegt.
  Für einen beliebigen Körper K nennen wir $\mathbb{P}^1(K)$ die *projektive Gerade*.

- Wir identifizieren diesen Raum mit dem Körper durch Hinzunahme eines unendlich fernen Punktes $\mathbb{P}^1(K) = K \cup \{\infty\}$ vermöge der wohldefinierten Bijektion:

$$\begin{aligned} \pi : \quad & \mathbb{P}^1(K) \to K \cup \{\infty\} \\ & (x_0 : x_1) \mapsto \frac{x_0}{x_1} \end{aligned}$$

  i) Wohldefiniertheit
  Seien hierzu $(x_0 : x_1)$ und $(x_0' : x_0')$ zwei Elemente der gleichen Äquivalenzklasse. Dann gilt offenbar: $\exists\ 0 \neq \lambda \in K$ mit $x_0' = \lambda x_0$ und $x_1' = \lambda x_1$. Demnach gilt aber auch:
  $\pi(x_0 : x_1) = \frac{x_0}{x_1} = \frac{\lambda x_0}{\lambda x_1} = \frac{x_0'}{x_1'} = \pi(x_0' : x_1')$
  ii) Surjektivität
  Klar $\forall x_0, x_1 \neq 0$. Insbesondere gilt:

$$\pi^{-1}(\infty) = (1 : 0)$$

iii) Injektivität
Es gilt offenbar $\pi(x_0 : x_1) = \pi(x_0' : x_1') \Leftrightarrow \exists \lambda \in \mathbb{F}_q^*$ mit $x_0' = \lambda x_0,\ x_1' = \lambda x_1$. Also gilt schon $(x_0 : x_1) = (x_0' : x_1')$.
Außerdem können unbestimmte Ausdrücke der Form „$\frac{0}{0}$“ nicht auftreten, weil die der Äquivalenzrelation zugrundeliegende Menge gerade der zweidimensionale Raum $K^2 \setminus \{(0,0)\}$ ohne den Ursprung ist.

- Im Nachfolgenden betrachten wir den projektiven Raum über dem endlichen Körper $\mathbb{F}_q$. Damit ergibt sich für die Anzahl der Elemente des projektiven Raumes $\mathbb{P}(\mathbb{F}_q^{n+1} \setminus \{0\}) = \mathbb{P}^n(\mathbb{F}_q)$ der Dimension n über einem endlichen Körper:

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^{n+1} \setminus \{0\}|}{|\mathbb{F}_q \setminus \{0\}|} = \frac{q^{n+1} - 1}{q - 1}$$

Für die weiteren Überlegungen interessieren wir uns insbesondere für die projektive Gerade $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ über dem endlichen Körper $\mathbb{F}_q$ mit

$$|\mathbb{P}^1(\mathbb{F}_q)| = \frac{q^2 - 1}{q - 1} = q + 1.$$

1.3 Die Gruppe $PGL(2, \mathbb{F}_q)$

1.3.1 Definition.

Wir betrachten die kanonische Abbildung $\rho :\ A \mapsto \{\lambda A \mid \lambda \in \mathbb{F}_q^*\} =: [A]$ mit $A \in GL(2, \mathbb{F}_q)$. Das Zentrum von $GL(2, \mathbb{F}_q)$ ist Kern der Abbildung ρ, d.h.

$$\text{Kern}(\rho) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^*\} = Z(GL(2, \mathbb{F}_q))$$

Damit definieren wir nun
$GL(2, \mathbb{F}_q)/Z(GL(2, \mathbb{F}_q)) = GL(2, \mathbb{F}_q)/\text{Kern}(\rho) =: PGL(2, \mathbb{F}_q)$
als allgemeine projektive lineare Gruppe über dem endlichen Körper $\mathbb{F}_q$. Es gilt somit offensichtlich:

$$|PGL(2, \mathbb{F}_q)| = \frac{|GL(2, \mathbb{F}_q)|}{|Z(GL(2, \mathbb{F}_q))|} = \frac{(q^2 - 1)q(q - 1)}{q - 1} = q(q^2 - 1)$$

1.3.2 Definition und Bemerkung.

Eine Abbildung $f_A : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ der Gestalt $z \mapsto \frac{az+b}{cz+d}$ mit einer Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{F}_q)$ nennen wir *Möbiustransformation*. Dabei gelten die üblichen Rechenregeln mit dem Symbol „∞“:

$$f_A(\infty) = \frac{a}{c} \quad \text{für} \quad c \neq 0$$
$$f_A(\infty) = \infty \quad \text{für} \quad c = 0$$

Wir erhalten insgesamt die folgenden Korrespondenzen:

$$\mathbb{P}^1(\mathbb{F}_q) \quad \overset{1:1}{\longleftrightarrow} \quad \mathbb{F}_q \cup \{\infty\}$$
$$A \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \frac{ax_0 + bx_1}{cx_0 + dx_1} \overset{1:1}{\longleftrightarrow} \quad f_A(z) = \frac{az + b}{cz + d}$$

2 Die Konjugationsklassen der Gruppe $GL(2, \mathbb{F}_q)$

2.1 Vorbemerkungen

2.1.1 Beobachtung.
Etwas tiefgehender ist die Frage nach Anzahl und Größe der Konjugationsklassen der Gruppen $GL(2, \mathbb{F}_q)$. Es sei hierzu

$$A \in GL(2, \mathbb{F}_q) \quad \text{mit} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

und $\chi_A(x) = x^2 - a_1 x + a_0$ das charakteristische Polynom von A mit $a_1 = \text{Spur}(A) = a + d$,
$a_0 = \det(A) = ad - bc \neq 0$. Aus der linearen Algebra ist bekannt:
A, B konjugiert $\Longrightarrow \chi_A = \chi_B$, aber
A, B konjugiert $\not\Longleftarrow \chi_A = \chi_B$
d.h. die Konjugationsklassen sind a priori nicht eindeutig durch das charakteristische Polynom beschreibbar. Allerdings liefert uns das charakteristische Polynom zusammen mit dem folgenden Lemma und Kenntnissen der Gruppentheorie, alle Informationen um die Konjugationsklassen von $GL(2, \mathbb{F}_q)$ vollständig zu charakterisieren.

2.1.2 Lemma.
Sei $p(x) = \sum_{k=0}^{n} a_k x^k$ mit $a_n = 1 \in K[x]$ ein beliebiges normiertes Polynom und A die so genannte Begleitmatrix von p der Gestalt

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Dann gilt: $\chi_A(x) = p(x)$, d.h. jedes normierte Polynom tritt als charakteristisches Polynom eines geeigneten Endomorphismus auf.

Beweis. (Induktion nach $n = \deg(p)$)
Induktionsanfang: $n = 1$ Klar!
Induktionsschritt: $(n-1) \to n$
Gemäß Induktionsvoraussetzung (I.V.) ist die Behauptung gezeigt für Polynome vom Grad $n - 1$:

$$\chi_A(x) = \det(xE - A) = \det \begin{pmatrix} x & \cdots & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & -1 & x + a_{n-1} \end{pmatrix}$$

Entwicklung nach der ersten Zeile liefert:

$$\chi_A(x) = (-1)^{1+1}\, x \det \begin{pmatrix} x & \cdots & \cdots & 0 & a_1 \\ -1 & x & \cdots & 0 & a_2 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & -1 & x + a_{n-1} \end{pmatrix} + (-1)^{n+1} a_0 \det \begin{pmatrix} -1 & x & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & x \\ 0 & \cdots & \cdots & 0 & -1 \end{pmatrix}$$

$$\chi_A(x) \overset{I.V.}{=} x(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1) + (-1)^{n+1}(-1)^{n-1}a_0 = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = p(x)$$

Der für unsere nachfolgenden Betrachtungen interessante Fall $n = 2$ mit $K = \mathbb{F}_q$ ergibt:

$$p(x) = x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$$

ist das charakteristische Polynom zur Matrix

$$A = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \qquad A \in GL(2, \mathbb{F}_q)$$

□

(siehe [BE08], Seite 126).

2.1.3 Bemerkung.

Zur vollständigen Klassifizierung der Konjugationsklassen, wie sie für die Bestimmung des Zyklenzeigers notwendig ist, müssen wir zu $A \in GL(2, \mathbb{F}_q)$ die folgenden Parameter bestimmen:

- charakteristisches Polynom
- Repräsentant
- Anzahl der Klassen
- Anzahl der Elemente pro Klasse

Wir führen die Fallunterscheidung für Matrizen in $GL(2, \mathbb{F}_q)$ also anhand der Gestalt des charakteristischen Polynoms durch. Bei der Bestimmung der Größe der Konjugationsklassen von $GL(2, \mathbb{F}_q)$ verwenden wir im Nachfolgenden zur Vereinfachung die Kurzschreibweise: $G := GL(2, \mathbb{F}_q)$.

2.2 Klassifikation der Konjugationsklassen

2.2.1 Matrizen vom Typ 1.

Das charakteristische Polynom $\chi_A(x) = x^2 + a_1x + a_0$ ist irreduzibel.
Die Konjugationsklasse von A ist eindeutig durch χ_A bestimmt. Ein jeweiliger Repräsentant in Normalform ist gemäß Lemma 2.1.2 gegeben durch:

$$\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}$$

i) Anzahl
Die irreduziblen Polynome liefern uns $\frac{q(q-1)}{2}$ Konjugationsklassen von $GL(2,\mathbb{F}_q)$.
Offensichtlich gibt es gibt es gerade q^2 Polynome der Gestalt $p(x) = x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$. Außerdem haben wir gerade q mögliche Linearfaktoren vom Grad 1. Daher gibt es q Polynome vom Grad 2, die Quadrat eines solchen Faktors sind. Es bleiben noch $\frac{q(q-1)}{2}$ normierte Polynome zweiten Grades, die Produkt von zwei paarweise verschiedenen Linearfaktoren sind. Also gibt es

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

irreduzible normierte Polynome vom Grad 2.

ii) Größe
Den Schlüssel zur Bestimmung der jeweiligen Größe der Konjugationsklasse liefert uns die Bahnformel für Konjugation. Hierzu müssen wir den entsprechenden Zentralisator für den Standardrepräsentanten bestimmen.

$$Z_G(\begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}) = \left\{ A \in G \mid A \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} A \right\}$$

Dazu müssen wir die folgende Matrixgleichung lösen:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Dies ergibt:

$$\begin{aligned} b &= -a_0c \\ -a_0a - a_1b &= -a_0c - a_0d \\ d &= a - a_1c \\ -a_0c - a_1d &= b - a_1d \end{aligned}$$

Auflösen des Gleichungssystems liefert:

$$Z_G(\text{„“}) = \left\{ \begin{pmatrix} a & b \\ -\frac{b}{a_0}a & a + a_1\frac{b}{a_0} \end{pmatrix} \mid (a,b) \neq (0,0) \right\}$$

Also ergibt sich für die Größe des Zentralisators (wegen a, b nicht beide null) und somit für die Größe der Klasse:

$$|Z_G(\text{„“})| = q^2 - 1, \quad \text{also} \quad |K_1| = \frac{|G|}{|Z_G(\text{„“})|} = \frac{q(q-1)(q^2-1)}{q^2-1} = q(q-1).$$

2.2.2 Matrizen vom Typ 2.
Das charakteristische Polynom zerfällt in paarweise verschiedene Linearfaktoren.
$\chi_A(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$ mit $\alpha \neq \beta$, wobei $\alpha, \beta \in \mathbb{F}_q^*$.
Für die zugehörigen Eigenräume gilt:

$$\text{Eig}(A,\alpha) = \ < \begin{pmatrix} -\beta \\ 1 \end{pmatrix} >, \qquad \text{Eig}(A,\beta) = \ < \begin{pmatrix} -\alpha \\ 1 \end{pmatrix} >,$$

also

$$\dim(\mathrm{Eig}(A,\alpha)) = \dim(\mathrm{Eig}(A,\beta)) = \mu_A(\alpha) = \mu_A(\beta) = 1.$$

Das charakteristische Polynom zerfällt vollständig in Linearfaktoren und geometrische und algebraische Vielfachheit stimmen überein. Demnach ist A diagonalisierbar. Somit ergibt sich:

$$\begin{pmatrix} 0 & -\alpha\beta \\ 1 & \alpha+\beta \end{pmatrix} \sim \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

i) Anzahl
Es gibt offenbar $\frac{(q-1)(q-2)}{2}$ Konjugationsklassen der obigen Form, denn:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}$$

vermöge der Operation $S \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} S^{-1}$ mit

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = S^{-1}$$

ii) Größe
Wir bestimmen wieder den Zentralisator für den Standardrepräsentanten.

$$Z_G(\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}) = \left\{ A \in G \mid A \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} A \right\}$$

Dies ergibt:

$$\begin{aligned} \alpha a &= \alpha a \\ \beta b &= \alpha a \\ \alpha c &= \beta c \\ \beta d &= \beta d \end{aligned}$$

$$\text{Wegen } \alpha \neq \beta \text{ ist } b = c = 0$$

Also folgt:

$$Z_G(\text{„“}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, b \in \mathbb{F}_q \setminus \{0\} \right\}$$

Demnach erhalten wir:

$$|Z_G(\text{„“})| = (q-1)^2, \quad \text{also} \quad |K_2| = \frac{|G|}{|Z_G(\text{„“})|} = \frac{q(q-1)(q^2-1)}{(q-1)^2} = q(q+1).$$

2.2.3 Matrizen vom Typ 3.
Das charakteristische Polynom ist Quadrat eines Linearfaktors.
$\chi_A(x) = (x-\alpha)^2 = x^2 - 2\alpha x + \alpha^2$ mit $\alpha \in \mathbb{F}_q \setminus \{0\}$.

Hier müssen wir wiederum zwei Fälle unterscheiden.
a)

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \quad \dim(\mathrm{Eig}(A, \alpha)) = \mu_A(\alpha) = 2$$

$x = \alpha$ ist doppelter Eigenwert und A hat schon Diagonalgestalt.
i) Anzahl
Es gibt offenbar $q - 1$ Konjugationsklassen dieser Sorte.
ii) Größe
Trivialerweise gibt es nur ein Element pro Klasse.
b)

$$A = \begin{pmatrix} 0 & -\alpha^2 \\ 1 & 2\alpha \end{pmatrix} \quad \dim(\mathrm{Eig}(A, \alpha)) = 1 \neq \mu_A(\alpha)$$

also A ist nicht diagonalisierbar, aber es gilt:

$$A \sim \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

i) Anzahl
Hiervon haben wir offensichtlich wiederum $q - 1$ Konjugationsklassen.
ii) Größe
Wir bestimmen den Zentralisator für den Standardrepräsentanten.

$$Z_G(\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}) = \left\{ A \in G \mid A \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} A \right\}$$

Dies ergibt:

$$\begin{aligned} \alpha a &= \alpha a + c \\ a + b &= \alpha b + d \\ \alpha c &= c \\ c + d &= d, \end{aligned}$$

$$\text{d.h.} \quad a = d, \quad \alpha = 1, \quad c = 0.$$

Also folgt:

$$Z_G(\text{„“}) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q \setminus \{0\}, b \in \mathbb{F}_q \right\}$$

Demnach erhalten wir:

$$|Z_G(\text{„“})| = (q-1)q, \quad \text{also} \quad |K_4| = \frac{|G|}{|Z_G(\text{„“})|} = \frac{q(q-1)(q^2-1)}{q(q-1)} = q^2 - 1.$$

2.2.4 Bemerkung.
Insgesamt zerfällt $G = GL(2, \mathbb{F}_q)$ also in $q^2 - 1$ Konjugationsklassen, denn:

$$\frac{q(q-1)}{2} + \frac{(q-1)(q-2)}{2} + (q-1) + (q-1) = q^2 - 1$$

Die Klassengleichung bestätigt nun die Richtigkeit unserer Überlegungen:

$$|G| \stackrel{!}{=} \frac{q(q-1)}{2}q(q-1) + \frac{(q-1)(q-2)}{2}q(q+1) + (q-1)1 + (q-1)(q^2-1) = q(q-1)(q^2-1)$$

Damit erhalten wir die nachfolgende tabellarische Übersicht für die Konjugationsklassen der Gruppe $GL(2, \mathbb{F}_q)$.

Typ	$\chi_A(x)$	Repräsentant	Größe	Anzahl
1	$x^2 - bx - a \in \mathbb{F}_q[x]$ irreduzibel	$\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$	$q(q-1)$	$\frac{q(q-1)}{2}$
2	$(x-\alpha)(x-\beta) \quad \alpha \neq \beta \in \mathbb{F}_q \setminus \{0\}$	$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$	$q(q+1)$	$\frac{(q-1)(q-2)}{2}$
3 a)	$(x-\alpha)^2$ $\alpha \in \mathbb{F}_q \setminus \{0\} \quad \dim(\mathrm{Eig}(A,\alpha)) = \mu_A(\alpha) = 2$	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$	1	$q-1$
3 b)	$(x-\alpha)^2$ $\alpha \in \mathbb{F}_q \setminus \{0\} \quad \dim(\mathrm{Eig}(A,\alpha)) = 1 \neq \mu_A(\alpha) = 2$	$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$	q^2-1	$q-1$

3 Drei- und Vierpunktkonfigurationen in $\mathbb{P}^1(\mathbb{F}_q)$

Notation

Für den restlichen Teil der Arbeit (vermehrt ab Abschnitt 3.3) werden gegebenenfalls zur besseren Übersicht die folgenden Abkürzungen verwendet.

- $K := \mathbb{F}_q$
- $L := \mathbb{F}_{q^2}$
- $G := GL(2, \mathbb{F}_q)$
- $\overline{G} := PGL(2, \mathbb{F}_q)$
- $X := \mathbb{P}^1(\mathbb{F}_q)$

3.1 Dreipunktkonfigurationen

Im nachfolgenden Abschnitt wollen wir Punktkonfigurationen der projektiven Gerade über einem endlichen Körper mit q Elementen untersuchen. Unser Ziel ist es Invarianten von Projektivitäten zu definieren, um hiermit die Anzahl der Äquivalenzklassen von Anordnungen von drei und vier Punkten zu bestimmen.

3.1.1 Definition.
Seien $Z, Z' \subset \mathbb{P}^1(\mathbb{F}_q)$ zwei Teilmengen. Z, Z' heißen projektiv äquivalent, wenn eine Möbiustransformation f_A existiert, sodass $f_A(Z) = Z'$.

3.1.2 Satz (Dreipunktesatz)
Sind $\{z_0, z_1, z_2\}$ und $\{z_0', z_1', z_2'\}$ jeweils drei paarweise verschiedene Punkte in $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$, dann gibt es genau eine Möbiustransformation f_A mit $f_A(z_i) = z_i' \ \ \forall i = 0, 1, 2$.

Beweis. i) Es genügt dies für $z_0 = 0, z_1 = 1, z_2 = \infty$ zu zeigen. Ist nämlich $f_A(z) = \frac{az+b}{cz+d}$ gegeben, so ist:

$$\begin{aligned} f_A(0) &= \frac{b}{d} \\ f_A(1) &= \frac{a+b}{c+d} \\ f_A(\infty) &= \frac{a}{c} \end{aligned}$$

Da $A \in GL(2, \mathbb{F}_q)$ gilt $ad - bc \neq 0$, also ist $c = 0 \ \wedge \ d = 0$ nicht möglich.
Nun führen wir eine Fallunterscheidung durch:
a) $\quad c = 0 \ \wedge \ d \neq 0$

$$\begin{aligned} f_A(1) &= \frac{a+b}{d} = \frac{a}{d} + \frac{b}{d} \\ f_A(z) &= (f_A(1) - f_A(0))z + f_A(0) \end{aligned}$$

b) $c \neq 0 \wedge d = 0$

$$\begin{aligned} f_A(1) &= \frac{a+b}{c} = \frac{a}{c} + \frac{b}{c} \\ f_A(z) &= \frac{az}{c} + \frac{b}{c}\frac{1}{z} \\ &= f_A(\infty)z + (f_A(1) - f_A(\infty))\frac{1}{z} \end{aligned}$$

c) $c \neq 0 \wedge d \neq 0$

$$\begin{aligned} f_A(z) &= \frac{\frac{a}{c}z + \frac{b}{c}}{z + \frac{d}{c}} \\ &= \frac{f_A(\infty)z + f_A(0)\frac{d}{c}}{z + \frac{d}{c}} \end{aligned}$$

Damit erhalten wir

$$f_A(1) = \frac{f_A(\infty) + f_A(0)\frac{d}{c}}{1 + \frac{d}{c}},$$

wobei dann offenbar wegen $f_A(0) \neq f_A(\infty)$ der Ausdruck $\frac{d}{c}$ eindeutig durch den Wert von $f_A(1)$ bestimmt wird.
(ii) Wir zeigen die Existenz einer solchen Möbiustransformation nun für die Punkte $\{0, 1, \infty\}$:
Hierzu wählen wir $a, b, c, d \in \mathbb{F}_q \cup \{\infty\}$ so, dass

$$\begin{aligned} f_A(0) &= \frac{b}{d} = z_0' \\ f_A(\infty) &= \frac{a}{c} = z_2' \end{aligned}$$

Da nach Voraussetzung gilt $z_0' \neq z_2'$, erhalten wir mit den so gewählten Einträgen für die Matrix der Möbiustransformation gerade:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{F}_q)$$

wie gewünscht. Wir wählen nun weiter $\lambda \in \mathbb{F}_q \setminus \{0\}$ so, dass $f_A(1) = \frac{\lambda a + b}{\lambda c + d} = z_1'$. Dies ist möglich, da

$$\frac{\lambda a + b}{\lambda c + d} = z_1' \Leftrightarrow \lambda(a - cz_1') = dz_1' - b$$

wobei $z_2' = \frac{a}{c} \neq z_1' \Leftrightarrow a - cz_1' \neq 0$, also ist die Gleichung nach λ auflösbar, d.h. $\lambda = \frac{dz_1' - b}{a - cz_1'}$. Insbesondere bleibt das Bild von ∞ unverändert, da $z_2' = \frac{\lambda a}{\lambda c} = \frac{a}{c} = f_A(\infty) = f_A(z_2)$.
(iii) Die Eindeutigkeit von $f_A(0), f_A(\infty)$ ist klar. Sei nun $\lambda' \in \mathbb{F}_q \setminus \{0\}$ ein weiterer geeigneter Faktor. Dann gilt:

$$z_1' = f_A(1) = \frac{\lambda a + b}{\lambda c + d} = \frac{\lambda' a + b}{\lambda' c + d}$$

Damit haben wir:

$$\begin{aligned}\lambda a + b &= z_1'(\lambda c + d)\\ \lambda' a + b &= z_1'(\lambda' c + d)\end{aligned}$$

Demnach ergibt sich durch Auflösen nach b und Gleichsetzen:

$$\begin{aligned} b &= z_1'(\lambda c + d) - \lambda a\\ b &= z_1'(\lambda' c + d) - \lambda' a\\ \Leftrightarrow \lambda(z_1' c - a) &= \lambda'(z_1' c - a)\end{aligned}$$

Dabei ist $z_2' = \frac{a}{c} \neq z_1'$, also folgt nach Division durch $z_1' c - a \neq 0$ gerade:

$$\lambda = \lambda'$$

Damit sind die Werte a, b, c, d bis auf einen gemeinsamen, von Null verschiedenen, Faktor eindeutig bestimmt. □

3.1.3 Korollar.
Für die Operation der Gruppe $PGL(2, \mathbb{F}_q)$ auf der Menge $\mathbb{P}^1(\mathbb{F}_q)$ vermöge Möbiustransformation gilt: Zu je zwei dreielementigen Teilmengen $\{z_0, z_1, z_2\}$ und $\{z_0', z_1', z_2'\}$ mit paarweise verschiedenen Elementen gilt:

$$\exists!\ [A] \in PGL(2, \mathbb{F}_q): \quad ([A], z_i) \mapsto z_i' \quad \forall i = 0, 1, 2$$

Also je zwei dreielementige Teilmengen mit paarweise verschiedenen Elementen sind projektiv äquivalent.

Beweis. Die Abbildung: $\phi : PGL(2, \mathbb{F}_q) \to \{\text{Möbiustransformationen}\}$ der Gestalt:

$$\phi([A]) = f_A$$

ist ein Gruppenisomorphismus. Demnach entspricht eine Operation von $[A]$ auf $\mathbb{P}^1(\mathbb{F}_q)$ einer Abbildung der Form: $f_A(z) = \frac{az+b}{cz+d}$. Damit greift der zuvor bewiesene Dreipunktesatz. □

3.1.4 Bemerkung.
Der hier bewiesene Dreipunktesatz kann auch wesentlich allgemeiner für projektive Räume höherer Dimension über einem beliebigen Körper bewiesen werden. Dies erfordert allerdings die Entwicklung einer, für unsere weiteren Betrachtungen nicht weiter benötigten, Begriffsmaschinerie, sodass wir uns mit dem für uns relevanten Speziallfall begnügen wollen (siehe hierzu etwa [Fis01], Seite 146 Satz 3.2.5).

3.2 Vierpunktkonfigurationen

3.2.1 Definition.
In $\mathbb{P}^1(\mathbb{F}_q)$ seien vier Punkte (durch ihre homogenen Koordinaten gegeben), also

$$z_0 = (x_0 : y_0), \quad z_1 = (x_1 : y_1), \quad z_2 = (x_2 : y_2), \quad z_3 = (x_3 : y_3)$$

derart, dass mindestens drei Punkte z_i, z_j, z_k mit $i, j, k \in \{0, 1, 2, 3\}$ paarweise verschieden sind. Dann ist

$$DV(z_0, z_1, z_2, z_3) := \frac{z_3 - z_1}{z_3 - z_0} : \frac{z_2 - z_1}{z_2 - z_0}$$

$$= \frac{\begin{vmatrix} x_3 & x_1 \\ y_3 & y_1 \end{vmatrix}}{\begin{vmatrix} x_3 & x_0 \\ y_3 & y_0 \end{vmatrix}} : \frac{\begin{vmatrix} x_2 & x_1 \\ y_2 & y_1 \end{vmatrix}}{\begin{vmatrix} x_2 & x_0 \\ y_2 & y_0 \end{vmatrix}} = \frac{x_3y_1 - y_3x_1}{x_3y_0 - y_3x_0} : \frac{x_2y_1 - x_1y_2}{x_2y_0 - y_2x_0}$$

das Doppelverhältnis der Punkte z_0, z_1, z_2, z_3.

3.2.2 Satz.
Das Doppelverhältnis von vier Punkten, gewählt wie in obiger Definition, ist invariant unter Möbiustransformationen.

Beweis. Ist $f_A : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ eine Möbiustransformation, so lässt sich die Abbildung durch eine 2×2- Matrix aus $GL(2, \mathbb{F}_q)$ beschreiben. Sei also

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{F}_q)$$

die Darstellungsmatrix von f_A. Dann erhalten wir:

$$\begin{aligned} z_0' &= (ax_0 + by_0 : cx_0 + dy_0) = (x_0' : y_0') \\ z_1' &= (ax_1 + by_1 : cx_1 + dy_1) = (x_1' : y_1') \\ z_2' &= (ax_2 + by_2 : cx_2 + dy_2) = (x_2' : y_2') \\ z_3' &= (ax_3 + by_3 : cx_3 + dy_3) = (x_3' : y_3') \end{aligned}$$

Damit ergibt sich:

$$DV(z_0', z_1', z_2', z_3') = \frac{\begin{vmatrix} x_3' & x_1' \\ y_3' & y_1' \end{vmatrix}}{\begin{vmatrix} x_3' & x_0' \\ y_3' & y_0' \end{vmatrix}} : \frac{\begin{vmatrix} x_2' & x_1' \\ y_2' & y_1' \end{vmatrix}}{\begin{vmatrix} x_2' & x_0' \\ y_2' & y_0' \end{vmatrix}} = \frac{x_3'y_1' - y_3'x_1'}{x_3'y_0' - y_3'x_0'} : \frac{x_2'y_1' - x_1'y_2'}{x_2'y_0' - y_2'x_0'}$$

$$= \frac{(ax_3 + by_3)(cx_1 + dy_1) - (cx_3 + dy_3)(ax_1 + by_1)}{(ax_3 + by_3)(cx_0 + dy_0) - (cx_3 + dy_3)(ax_0 + by_0)} : \frac{(ax_2 + by_2)(cx_1 + dy_1) - (cx_2 + dy_2)(ax_1 + by_1)}{(ax_2 + by_2)(cx_0 + dy_0) - (cx_2 + dy_2)(ax_0 + by_0)}$$

$$= \left(\frac{acx_3x_1 + adx_3y_1 + bcx_1y_3 + bdy_3y_1 - acx_3x_1 - bcx_3x_1 - adx_1y_3 - bdy_3y_1}{acx_3x_0 + adx_3y_0 + bcx_0y_3 + bdy_3y_0 - acx_3x_0 - bdx_3y_0 - adx_0y_3 - bdy_3y_0} \right)$$

$$: \left(\frac{acx_1x_2 + adx_2y_1 + bcx_1y_2 + bdy_1y_2 - acx_1x_2 - bcx_2y_1 - ady_2x_1 - bdy_1y_2}{acx_0x_2 + adx_2y_0 + bcx_0y_2 + bdy_0y_2 - acx_0x_2 - bcy_0x_2 - adx_0y_2 - bdy_0y_2} \right)$$

$$= \frac{(ad - bc)x_3y_1 + (bc - ad)y_3x_1}{(ad - bc)x_3y_0 + (bc - ad)y_3x_0} : \frac{(ad - bc)x_2y_1 + (bc - ad)x_1y_2}{(ad - bc)x_2y_0 + (bc - ad)y_2x_0}$$

$$= \frac{(ad - bc)(x_3y_1 - y_3x_1)}{(ad - bc)(x_3y_3 - y_3x_0)} : \frac{(ad - bc)(x_2y_1 - x_1y_2)}{(ad - bc)(x_2y_0 - y_2x_0)}$$

$$\overset{ad-bc=\det(A)\neq 0}{=} \frac{x_3y_1 - y_3x_1}{x_3y_0 - y_3x_0} : \frac{x_2y_1 - x_1y_2}{x_2y_0 - y_2x_0} = DV(z_0, z_1, z_2, z_3)$$

□

3.2.3 Lemma.
Sind $\{z_0, z_1, z_2, z_3\}$ vier paarweise verschiedene Punkte, so gibt es genau eine Möbiustransformation f_A, d.h. mit Darstellungsmatrix aus $A \in GL(2, \mathbb{F}_q)$, sodass

$$\begin{aligned} f_A(z_0) &= \infty \\ f_A(z_1) &= 0 \\ f_A(z_2) &= 1 \\ f_A(z_3) &= z \end{aligned}$$

mit $z = DV(z_0, z_1, z_2, z_3)$. Wir sagen auch die Punkte $\{z_0, z_1, z_2, z_3\}$ können auf die *Normalform* $\{\infty, 0, 1, z\}$ gebracht werden.

Beweis. Der Dreipunktesatz liefert eine eindeutig bestimmte Möbiustransformation f_A mit

$$\begin{aligned} f_A(z_0) &= \infty \\ f_A(z_1) &= 0 \\ f_A(z_2) &= 1 \end{aligned}$$

Dann erhalten wir mit den Bildern der drei Punkte z_0, z_1, z_2 folgende Situation:

$$f_A(z_0) = \infty \Leftrightarrow cz_0 + d = 0 \tag{1}$$
$$f_A(z_1) = 0 \Leftrightarrow az_1 + b = 0 \tag{2}$$
$$f_A(z_2) = 1 \Leftrightarrow az_2 + b = cz_2 + d \tag{3}$$

Also durch Einsetzen von (1) und (2) in (3) gerade:

$$\frac{a}{c} = \frac{z_2 - z_0}{z_2 - z_1} \tag{4}$$

Damit ergibt sich für den vierten Punkt:

$$f_A(z_3) = \frac{az_3 + b}{cz_3 + d}$$

Also unter Verwendung von (1), (2) und (4) erhalten wir schon

$$f_A(z_3) = \frac{z_3 - z_1}{z_3 - z_0} \cdot \frac{z_2 - z_0}{z_2 - z_1} = \frac{z_3 - z_1}{z_3 - z_0} : \frac{z_2 - z_1}{z_2 - z_0} = DV(z_0, z_1, z_2, z_3)$$

wie gewünscht. □

3.2.4 Bemerkung.
Betrachten wir im Speziellen die Vierpunktkonfiguration $\{\infty, 0, 1, z\}$, wobei $z \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{0, 1, \infty\}$ mit $z = (x : y)$ so gilt:

$$DV(\infty, 0, 1, z) = \frac{\begin{vmatrix} x & 0 \\ y & 1 \end{vmatrix}}{\begin{vmatrix} x & 1 \\ y & 0 \end{vmatrix}} : \frac{\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}} = (x : y) = z \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{0, 1, \infty\}$$

3.2.5 Satz.
Es seien $\{z_0, z_1, z_2, z_3\}$ und $\{z_0', z_1', z_2', z_3'\}$ zwei Mal vier paarweise verschiedene Punkte aus $\mathbb{P}^1(\mathbb{F}_q)$. Es existiert eine Möbiustransformation f_A mit

$$f_A(z_i) = z_i' \quad \forall i \in \{0, 1, 2, 3\}$$

genau dann wenn das Doppelverhältnis übereinstimmt, d.h. wenn gilt

$$DV(z_0, z_1, z_2, z_3) = DV(z_0', z_1', z_2', z_3').$$

Beweis. „⇒“ Die Bedingung ist notwendig wegen der Invarianz des Doppelverhältnisses unter Möbiustransformationen, wie in Satz 3.2.2 gezeigt wurde.
„⇐“ Stimmt das Doppelverhältnis der Punkte überein, so finden wir gemäß Lemma 3.2.3 eine Möbiustransformation f_B mit Darstellungsmatrix $B \in GL(2, \mathbb{F}_q)$, welche die Punkte auf Normalform bringt.

$$\begin{aligned} f_B(z_0) &= \infty \\ f_B(z_1) &= 0 \\ f_B(z_2) &= 1 \\ f_B(z_3) &= z \end{aligned}$$

wobei $z \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{0, 1, \infty\}$. Weiterhin exisitert gemäß Lemma 3.2.3 eine Möbiustransformation f_C mit Darstellungsmatrix $C \in GL(2, \mathbb{F}_q)$, sodass

$$\begin{aligned} f_C(z_0') &= \infty \\ f_C(z_1') &= 0 \\ f_C(z_2') &= 1 \\ f_C(z_3') &= DV(z_0', z_1', z_2', z_3') = DV(z_0, z_1, z_2, z_3) = z \end{aligned}$$

sodass wir mit $f_A := f_C^{-1} \circ f_B$ eine Möbiustransformation der gewünschten Form erhalten mit der Darstellungsmatrix $A := C^{-1} \cdot B$.

$$\begin{array}{ccc} \{z_0, z_1, z_2, z_3\} & \xrightarrow{f_A := f_C^{-1} \circ f_B} & \{z_0', z_1', z_2', z_3'\} \\ \Big\downarrow f_B & & \Big\downarrow f_C \\ \{\infty, 0, 1, DV(z_0, z_1, z_2, z_3)\} & = & \{\infty, 0, 1, DV(z_0', z_1', z_2', z_3')\} \end{array}$$

Dies zeigt, dass die Bedingung auch hinreichend ist. □

3.2.6 Definition.
Die endliche Gruppe G operiere auf der endlichen Menge $\mathcal{X}$ mit $|\mathcal{X}| = n$. Für $g \in G$ nennen wir das n-Tupel $\underline{c}(g) = (c_1(g), ..., c_n(g))$ den *Zykeltyp* von g auf $\mathcal{X}$, wobei $c_k(g)$ die Zahl der Zykel der Länge k bei Operation von g auf $\mathcal{X}$ bezeichnet.
Der Zykeltyp liefert die folgende Zerlegung von $n = |\mathcal{X}|$:

$$1 + ... + 1 + 2 + ... + 2 + ... + k + ... + k = n$$

Diese, nach der Zykellänge geordnete, Partition von n nennen wir im Nachfolgenden die *Zykelstruktur* von G auf $\mathcal{X}$.

3.2.7 Bemerkung.
Der Satz beantwortet die Frage, ob zwei Vierpunktkonfigurationen $\{z_0, z_1, z_2, z_3\}$ und $\{z_0', z_1', z_2', z_3'\}$ projektiv äquivalent sind noch nicht. Wir können die Punkte permutieren. Bei bestimmten Permutationen ändert sich das Doppelverhältnis der Punkte. Die Permutationsgruppe S_4 operiert also auf der Vierpunktkonfiguration $\{z_0, z_1, z_2, z_3\}$, sodass die folgende Situation vorliegt:

$$S_4 \times \{z_0, z_1, z_2, z_3\} \to \{z_0, z_1, z_2, z_3\}$$
$$(\sigma, z_i) \mapsto z_{\sigma(i)} \qquad \forall i \in \{0, 1, 2, 3\}$$

Für jede der 24 möglichen Permutationen mit vier verschiedenen Punkten $\{z_0, z_1, z_2, z_3\}$ ist offenbar $DV(z_{\sigma(0)}, z_{\sigma(1)}, z_{\sigma(2)}, z_{\sigma(3)}) \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{0, 1, \infty\}$. Mit $DV(z_0, z_1, z_2, z_3) =: z$ ergibt sich Folgendes:

1. $$DV(z_0, z_1, z_2, z_3) = DV(z_1, z_0, z_3, z_2) = DV(z_2, z_3, z_0, z_1) = DV(z_3, z_2, z_1, z_0) = z,$$
   wobei alle Permuationen, die das Doppelverhältnis invariant lassen, die Kleinschen Vierergruppe V_4 bilden.
   $$V_4 := \{(z_0)(z_1)(z_2)(z_3), (z_0z_1)(z_2z_3), (z_0z_2)(z_1z_3), (z_0z_3)(z_1z_2)\}$$

2. $$DV(z_1, z_0, z_2, z_3) = DV(z_0, z_1, z_3, z_2) = DV(z_2, z_3, z_1, z_0) = DV(z_3, z_2, z_0, z_1) = z^{-1},$$
   wobei alle Permuationen, die das Doppelverhältnis invertieren die Zykelstruktur $1+2$ und 4 haben. Speziell wurden hier die folgenden Permutationen betrachtet:
   $$\{(z_0z_1)(z_2)(z_3), (z_2z_3)(z_0)(z_1), (z_0z_2z_1z_3), (z_1z_3z_0z_2)\}$$

3. $$DV(z_3, z_1, z_2, z_0) = DV(z_1, z_3, z_0, z_2) = DV(z_2, z_0, z_3, z_1) = DV(z_0, z_2, z_1, z_3) = 1 - z,$$
   wobei alle Permutationen dieser Art ebenfall die Zykelstruktur $1 + 2$ und 4 aufweisen, also:
   $$\{(z_0z_3)(z_1)(z_2), (z_0z_1z_3z_2), (z_0z_2z_3z_1), (z_1z_2)(z_0)(z_3)\}$$

4. $$DV(z_3, z_0, z_2, z_1) = DV(z_0, z_3, z_1, z_2) = DV(z_2, z_1, z_3, z_0) = DV(z_1, z_2, z_0, z_3) = 1 - z^{-1},$$
   wobei alle Permutationen dieser Art von der Zykelstruktur $1+3$ sind. Im Speziellen handelt es sich um folgende Permutationen:
   $$\{(z_0z_3z_1)(z_2), (z_1z_3z_2)(z_0), (z_0z_2z_3)(z_1), (z_0z_1z_2)(z_3)\}$$

5.

$$DV(z_1, z_3, z_2, z_0) = DV(z_3, z_1, z_0, z_2) = DV(z_2, z_0, z_1, z_3) = DV(z_0, z_2, z_3, z_1) = (1-z)^{-1},$$

wobei alle Permutationen dieser Art die verbleibenden Zykel der Struktur $1+3$ liefern:

$$\{(z_0z_2z_1)(z_3), (z_0z_1z_3)(z_2), (z_0z_2z_1)(z_3), (z_1z_2z_3)(z_0)\}$$

6.

$$DV(z_0, z_3, z_2, z_1) = DV(z_3, z_0, z_1, z_2) = DV(z_2, z_1, z_0, z_3) = DV(z_1, z_2, z_3, z_0) = 1-(1-z)^{-1} = \frac{z}{z-1},$$

wobei alle Permutationen dieser Form Zykel mit Zykelstruktur $1+2$ und 4 aufweisen:

$$\{(z_1z_3)(z_0)(z_2), (z_0z_3z_2z_1), (z_0z_2)(z_1)(z_3), (z_0z_1z_2z_3)\}$$

Von der Richtigkeit der Doppelverhältnisse unter veränderter Reihenfolge der Punkte überzeugt man sich leicht mit der Berechnungsformel aus Definition 3.2.1. (siehe auch [Fis01], Seite 156, Rechenregel 3.3.3). Demnach stellen wir fest:
Die Quotientengruppe S_4/V_4 operiert auf der Menge $\mathbb{P}^1(\mathbb{F}_q) \setminus \{0, 1, \infty\}$ mit den folgenden Bahnen:
$\{z, z^{-1}, 1-z, 1-z^{-1}, (1-z)^{-1}, 1-(1-z)^{-1}\}$. Für allgemeines z sind diese sechs Werte paarweise verschieden. Jedoch verkleinert sich für spezielle Werte von z die Bahn. In diesem Fall nehmen die vier Punkte eine spezielle Konfiguration im projektiven Raum $\mathbb{P}^1(\mathbb{F}_q)$ an. Dies wollen wir nun näher untersuchen.

3.2.8 Beobachtung.
Um die veränderten Bahnlängen zu bestimmen, müssen wir zunächst fünf Fälle unterscheiden, wobei wir feststellen werden, dass einige der Bestimmungsgleichungen die gleiche Bahn ergeben.
(i) $z = z^{-1} \Leftrightarrow z^2 = 1 \overset{z \neq 1}{\Leftrightarrow} z = -1$ liefert die Bahn $\{-1, 2, \frac{1}{2}\}$
(ii) $z = 1-z \Leftrightarrow 2z = 1 \Leftrightarrow z = \frac{1}{2}$ liefert die gleiche Bahn $\{-1, 2, \frac{1}{2}\}$
(iii) $z = 1-z^{-1} \Leftrightarrow z^2 - z + 1 = 0 \Leftrightarrow z = \rho_6$, wobei ρ_6 eine primitive 6-te Einheitswurzel darstellt. Diese Bahn besteht nur aus $\{\rho_6, \rho_6^5\}$.
(iv) $z = (1-z)^{-1} \Leftrightarrow z^2 - z + 1 = 0 \Leftrightarrow z = \rho_6$, wobei ρ_6 eine primitive 6-te Einheitswurzel darstellt. Dies ergibt wiederum eine Bahn der Form $\{\rho_6, \rho_6^5\}$.
(v) $z = 1-(1-z)^{-1} \Leftrightarrow z(2-z) = 0 \Leftrightarrow z = 2$ liefert wiederum die Bahn $\{-1, 2, \frac{1}{2}\}$
Wir bemerken also, dass es nur zwei spezielle Bahnen der Form $\{\rho_6, \rho_6^5\}$ und $\{-1, 2, \frac{1}{2}\}$ mit Bahnlänge 2 und 3 gibt. Für Körper der Charakteristik $p = 3$ fallen die Elemente $-1, 2, \frac{1}{2}$ zusammen. In diesem Fall erhalten wir eine Bahn der Länge 1.
Außerdem müssen wir Körper der Charakteristik $p = 2$ gesondert behandeln.

3.2.9 Bemerkung.

- Jede geordnete Menge von vier Punkten $\{z_0, z_1, z_2, z_3\}$ in allgemeiner Lage kann in eineindeutiger Weise auf die Normalform $\{\infty, 0, 1, z\}$ gebracht werden, wobei $z = DV(z_0, z_1, z_2, z_3)$
- Das Doppelverhältnis von vier geordneten Punkten $\{z_0, z_1, z_2, z_3\}$ kann daher genau $q-2$ Werte annehmen.

- Insgesamt erhalten wir für die Anzahl an Vierpunktkonfigurationen $\mathcal{X}_4 := \{\{z_0, z_1, z_2, z_3\} \mid z_0, z_1, z_2, z_3, z_4 \in \mathbb{P}^1(\mathbb{F}_q)\}$ als Zahl aller vierelementigen Teilmengen von $\mathbb{P}^1(\mathbb{F}_q)$ gerade: $|\mathcal{X}_4| = \binom{q+1}{4} = \frac{(q+1)q(q-1)(q-2)}{4!} = \frac{q-2}{6}\frac{q(q^2-1)}{4}$
- Die Abbildung

$$\begin{aligned}\delta: \quad \mathbb{P}^1(\mathbb{F}_q) \setminus \{\infty, 0, 1\} &\to \mathcal{X}_4 \\ z &\mapsto \{\infty, 0, 1, z\}\end{aligned}$$

  induziert einen Isomorphismus

$$(S_4/V_4) \setminus (\mathbb{P}^1(\mathbb{F}_q) \setminus \{\infty, 0, 1\}) \xrightarrow{\cong} \overline{G} \setminus \mathcal{X}_4$$

  Ist also $l(B)$ die Länge einer Bahn B unter der Operation von S_4/V_4 auf $\mathbb{P}^1(\mathbb{F}_q) \setminus \{\infty, 0, 1\}$, so ist die Länge der entsprechenden Bahn B' in $\overline{G} \setminus \mathcal{X}_4$ gegeben durch: $\frac{q(q^2-1)}{4l(B)}$.
  Mit $l(B) \in \{1, 2, 3, 6\}$ gilt also für die entsprechende Bahn $B' \in \overline{G} \setminus \mathcal{X}_4$:
  $l(B') \in \{\frac{q(q^2-1)}{4}, \frac{q(q^2-1)}{8}, \frac{q(q^2-1)}{12}, \frac{q(q^2-1)}{24}\}$.

3.2.10 Zusammenfassung.
Führt man nun für die unterschiedlichen Bahnen B' in $\overline{G} \setminus \mathcal{X}_4$ eine Gewichtsfunktion der Gestalt

$$\begin{aligned}w: \quad \overline{G} \setminus \mathcal{X}_4 &\to \mathbb{Q} \\ B' &\mapsto \frac{4l(B')}{q(q^2-1)}\end{aligned}$$

$\forall B' \in \overline{G} \setminus \mathcal{X}_4$ mit $l(B') \in \{\frac{q(q^2-1)}{4}, \frac{q(q^2-1)}{8}, \frac{q(q^2-1)}{12}, \frac{q(q^2-1)}{24}\}$ ein, so gilt offenbar unter Verwendung von $l(B') = \frac{q(q^2-1)}{4l(B)}$ und $l(B) \in \{1, 2, 3, 6\}$ gemäß Beobachtung 3.2.8 und Bemerkung 3.2.9, gerade Folgendes für den Wertebereich der gewichteten Bahnen:

$$w(B') = \frac{1}{l(B)}, \text{ also } w(B') \in \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{6}\}$$

$\mathcal{X}_4$ ist disjunkte Vereinigung von Bahnen B' aus $\overline{G} \setminus \mathcal{X}_4$, d.h. $\mathcal{X}_4 = \bigcup_{B' \in \overline{G} \setminus \mathcal{X}_4} B'$. Weil die Vereinigung disjunkt ist, ergibt sich also $|\mathcal{X}_4| = \sum_{B' \in \overline{G} \setminus \mathcal{X}_4} l(B')$. Fassen wir in dieser Summe Bahnen gleicher Länge, d.h. mit gleichem Gewicht, zusammen, so erhalten wir:

$$|\mathcal{X}_4| = \frac{q-2}{6}\frac{q(q^2-1)}{4} = m_1\frac{q(q^2-1)}{4} + m_2\frac{q(q^2-1)}{8} + m_3\frac{q(q^2-1)}{12} + m_6\frac{q(q^2-1)}{24}$$

wobei $m_i = |\{\text{Bahnen der Länge } \frac{q(q^2-1)}{4i}\}|$ mit $i \in \{1, 2, 3, 6\}$. Demnach ergibt sich also:

$$m_1 + \frac{1}{2}m_2 + \frac{1}{3}m_3 + \frac{1}{6}m_6 = \frac{q-2}{6}$$

Demnach erhalten wir für die Summe der gewichteten Bahnen gerade den Wert $\frac{q-2}{6}$:

$$\sum_{B' \in \overline{G} \setminus \mathcal{X}_4} w(B') = \frac{q-2}{6}$$

3.3 Bestimmung des Stabilisators von vier Punkten in X

Wir wollen im Nachfolgenden den Stabilisator von vier Punkten in der Menge X unter Operation der Gruppe $\overline{G}$ bestimmen. Das Ziel dieses Abschnittes ist es dann hiermit einerseits die entsprechenden Ausnahmekonfigurationen näher zu charakterisieren und andererseits die, bereits in Teil 3.2, respektive Ausnahmebahnen gewichtete, Zahl an Vierpunktkonfigurationen zu bestätigen.

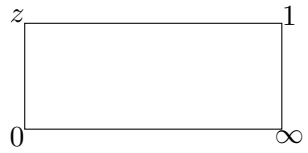
3.3.1 Bemerkung.
Wir können uns im Nachfolgenden bei der Beschreibung des Stabilisators von vier Punkten auf die Menge $\{\infty, 0, 1, z\}$ beschränken, denn wie wir bereits in Abschnitt 3.2 festgestellt haben gilt: Sind $\{z_0, z_1, z_2, z_3\}$ vier paarweise verschiedene Punkte aus X, so ist diese vierelementige Menge projektiv äquivalent zu $\{\infty, 0, 1, z\}$, wobei $z = DV(z_0, z_1, z_2, z_3)$.

1. Jedes Element im Stabilisator von $\{\infty, 0, 1, z\}$ bewirkt eine Permutation der Punkte $\{\infty, 0, 1, z\}$. Damit erhalten wir für die Kardinalität $|\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})|$:

$$|\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| \mid 24 \text{ d.h. } |\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| \in \{1, 2, 3, 4, 6, 8, 12, 24\}$$

2. Wir werden nun zeigen, dass die Kleinsche Vierergruppe $\forall z \in X$ kanonisch im Stabilisator eingebettet ist.
   Wir stellen hierzu fest, dass die Permutationen vom Zykeltyp $(2, 2)$ bewirkt werden durch:

$$\begin{aligned} V &= \{(0)(1)(\infty)(z); (0\infty)(1z); (01)(z\infty); (0z)(1\infty)\} \\ &= \left\{ [\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}], [\begin{pmatrix} 0 & z \\ 1 & 0 \end{pmatrix}], [\begin{pmatrix} -1 & 1 \\ -z^{-1} & 1 \end{pmatrix}], [\begin{pmatrix} 1 & -z \\ 1 & -1 \end{pmatrix}] \right\} \end{aligned}$$



   Diese Matrizen liefern Permutationen von $\{\infty, 0, 1, z\}$, die unabhängig von der speziellen Wahl der Parameter q, p, über allen endlichen Körpern Sinn ergeben. Also erhalten wir:
   $|\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| \in \{4, 8, 12, 24\}$.

3.3.2 Beobachtung.
Um die Möglichkeiten für die Kardinalität des Stabilisators von $\{\infty, 0, 1, z\}$ weiter einzugrenzen, bestimmen wir alle möglichen Permutationen und eliminieren dann sukzessive die Möglichkeiten für diejenigen Matrizen, die als Elemente im Stabilisator vorkommen können.

- Zykeltyp $(1, 1, 1, 1)$ und $(2, 2)$
  Wir erhalten die Kleinsche Vierergruppe, gegeben durch die Matrizen in obiger Bemerkung.

- Zykeltyp $(1, 1, 2)$

$$(01)(\infty)(z) \leftrightarrow [\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}] \Leftrightarrow z = \frac{1}{2}$$

$$(0\infty)(1)(z) \leftrightarrow [\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}] \Leftrightarrow z^2 = 1$$

$$(0z)(1)(\infty) \leftrightarrow [\begin{pmatrix} 1-z & z \\ 0 & 1 \end{pmatrix}] \Leftrightarrow z = 2$$

$$(1\infty)(0)(z) \leftrightarrow [\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}] \Leftrightarrow z = 2$$

$$(1z)(0)(\infty) \leftrightarrow [\begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix}] \Leftrightarrow z^2 = 1$$

$$(z\infty)(0)(1) \leftrightarrow [\begin{pmatrix} z & 0 \\ 1 & -z \end{pmatrix}] \Leftrightarrow z = \frac{1}{2}$$

- Zykeltyp $(1,3)$

$$(1\infty z)(0) \leftrightarrow [\begin{pmatrix} 1 & 0 \\ z^{-1} & -z^{-1} \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(1z\infty)(0) \leftrightarrow [\begin{pmatrix} 1 & 0 \\ 1 & -z \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(0z\infty)(1) \leftrightarrow [\begin{pmatrix} 0 & z \\ -z^{-1} & 1 \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(0\infty z)(1) \leftrightarrow [\begin{pmatrix} z & 1-z \\ 1 & 0 \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(01z)(\infty) \leftrightarrow [\begin{pmatrix} z-1 & 1 \\ 0 & 1 \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(0z1)(\infty) \leftrightarrow [\begin{pmatrix} -z & z \\ 0 & 1 \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(01\infty)(z) \leftrightarrow [\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

$$(0\infty 1)(z) \leftrightarrow [\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}] \Leftrightarrow z^2 - z + 1 = 0$$

- Zykeltyp (4)

$$(01\infty z) \leftrightarrow [\begin{pmatrix} -z & 1 \\ -1 & 1 \end{pmatrix}] \Leftrightarrow z^2 = 1$$

$$(01z\infty) \leftrightarrow [\begin{pmatrix} 0 & 1 \\ -z^{-1} & 1 \end{pmatrix}] \Leftrightarrow z = 2$$

$$(0\infty 1z) \leftrightarrow [\begin{pmatrix} -1 & -z \\ 1 & 0 \end{pmatrix}] \Leftrightarrow z = \frac{1}{2}$$

$$(0\infty z1) \leftrightarrow [\begin{pmatrix} 1 & -1 \\ z^{-1} & 0 \end{pmatrix}] \Leftrightarrow z = 2$$

$$(0z1\infty) \leftrightarrow [\begin{pmatrix} 0 & z \\ -1 & 1 \end{pmatrix}] \Leftrightarrow z = \frac{1}{2}$$

$$(0z\infty 1) \leftrightarrow [\begin{pmatrix} 1 & -1 \\ 1 & -z^{-1} \end{pmatrix}] \Leftrightarrow z^2 = 1$$

Wir erhalten also zunächst die folgenden Bestimmungsgleichungen für Punkte $z \in X$ bezüglich des Stabilisators von vier Punkten:

$$z^2 = 1 \tag{5}$$

$$z^2 - z + 1 = 0 \tag{6}$$

$$z = 2 \tag{7}$$

$$z = \frac{1}{2} \tag{8}$$

Dabei bemerken wir natürlich, dass Gleichung (7) und Gleichung (8) nur in Körpern der Charakteristik ungleich 2 Sinn ergeben.
Ist eine oder mehrere der Gleichungen (5), (6), (7), (8) für ein $z \in X$ erfüllt, so erhalten wir zu den kanonisch eingebetteten Elementen der Kleinschen Vierergruppe zusätzliche Elemente im Stabilisator von $\{\infty, 0, 1, z\}$, und zwar folgende:
- Gleichung (3) liefert 4 zusätzliche Elemente
- Gleichung (4) liefert 8 „ “
- Gleichung (5) liefert 4 „ “
- Gleichung (6) liefert 4 „ “

Dabei erkennen wir diese Gleichungen wieder, als die charakteristischen Gleichungen zur Bestimmung des Doppelverhältnisses einer ungeordneten (d.h. permutierten) Vierpunktekonfiguration in X (vgl. Abschnitt 3.2). Es leuchtet leicht ein, dass solche Gleichungen nur gelten können für spezielle Körperparameter q, p.
Wir wollen die Abhängigkeit der Kardinalität des Stabilsators von $\{\infty, 0, 1, z\}$ von der Arithmetik des, der Menge X zugrunde liegenden endlichen Körpers, nun genauer charakterisieren. Hierzu sei zunächst an einige wichtige Resultate aus der Algebra erinnert.

3.3.3 Definition.
Sei $n \in \mathbb{N}$ und K ein Körper. Eine Zahl ρ_n heißt $n-$ *te Einheitswurzel* in K, wenn ρ_n eine Lösung der Gleichung

$$z^n - 1 = 0$$

mit $z^n - 1 \in K[z]$ ist.
Gilt zusätzlich

$$\rho_n^k \neq 1 \ \forall \ k \in \mathbb{N}$$

mit $0 < k < n$, so heißt ρ_n *primitive* $n-$ *te Einheitswurzel.*

3.3.4 Definition.
Die Abbildung

$$\begin{aligned} \varphi : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \varphi(n) = |\{1 \leq r \leq n \mid \mathrm{ggT}(r, n) = 1\}| \end{aligned}$$

heißt eulersche Phi-Funktion. Sie ist schwach multiplikativ, d.h. für zwei teilerfremde n und m gilt: $\varphi(nm) = \varphi(n)\varphi(m)$. Im Speziellen erhalten wir für $n = p^r, r \in \mathbb{N}$ und p prim:

$$\varphi(p^r) = (p-1)p^{r-1}$$

Also ergibt sich im Fall $r = 1$ gerade:

$$\varphi(p) = p - 1$$

3.3.5 Satz.
Es sei $n \in \mathbb{N}$ und K ein Körper mit $\text{char}(K) \nmid n$. Es bezeichne U_n die Gruppe der $n-$ ten Einheitswurzeln in K.

- Eine $n-$ te Einheitswurzel ρ_n ist primitiv, wenn sie die Gruppe U_n erzeugt.
  Wir sagen: $\mathbb{F}_q$ enthält die $n-$ ten Einheitswurzeln, wenn für die Kardinalität der Gruppe U_n gilt: $|U_n| = n$.

- Die Gruppe U_n der $n-$ ten Einheitswurzeln enthält genau $\varphi(n)$ primitive $n-$ te Einheitswurzeln. Ist $\rho_n \in U_n$ primitive $n-$ te Einheitswurzel, so ist ρ_n^k für $k \in \mathbb{Z}$ genau dann primitive $n-$ te Einheitswurzel, wenn die Restklasse von k modulo n eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist, d.h. wenn $\text{ggT}(k, n) = 1$ gilt.

(siehe [Bos01], Seite 184, Korollar 6)
3.3.6 Definition.
Sei K ein Körper und $n \in \mathbb{N}$. Für $\text{char}(K) \nmid n$ seien $\rho_1, ..., \rho_{\varphi(n)}$ die primitiven $n-$ ten Einheitswurzeln in $\overline{K}$. Dann heißt

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (z - \rho_i)$$

das $n-$ te Kreisteilungspolynom über K.

3.3.7 Lemma.
$\mathbb{F}_q$ enthält die $n-$ ten Einheitswurzeln genau dann, wenn $q \equiv 1 \mod n$, für $\text{ggT}(q, n) = 1$.

Beweis. Es gelte $f(z) = z^n - 1 \in \mathbb{F}_q[z]$. Die Behauptung lautet nun:
f zerfällt über $\mathbb{F}_q$ genau dann vollständig in Linearfaktoren, wenn $q \equiv 1 \mod n$.
f zerfällt über $\mathbb{F}_q$ vollständig in Linearfaktoren.
$\Leftrightarrow$ f hat eine primitivie $n-$te Einheitswurzel $\rho \in \mathbb{F}_q$ als Nullstelle.
$\Leftrightarrow$ Es gilt: $\rho^q = \rho$, bzw. $\rho^{q-1} = 1$.
$\Leftrightarrow$ f hat eine Nullstelle ρ mit $n \mid (q-1)$.
$\Leftrightarrow q \equiv 1 \mod n$. □

3.3.8 Beobachtung.

- Die Bestimmungsgleichungen für spezielle Punktkonfigurationen mit einer größeren Stabilisatorgruppe decken sich mit Überlegungen aus der Gruppentheorie, denn der Stabilisator von vier

Punkten mit Kardinalität 8 ist als Untergruppe von S_4 mit den Sylowsätzen folgendermaßen charakterisiert: $|S_4| = 24 = 2^3 3$. Bezeichnet n_2 die Anzahl der $2-$ Sylowuntergruppen von S_4, d.h. derjenigen Untergruppen der Kardinalität $2^3 = 8$, so gilt:

$$\underbrace{n_2 \mid 3 \quad \wedge \quad n_2 \equiv 1 \mod 2}_{n_2 \in \{1,3\}}$$

Durch direktes Ausrechnen der Untergruppen von S_4 (etwa durch Veranschaulichung mittels der Stabilisatoren von Kantenmittendiagonalen im Tetraeder) ergibt sich: $n_2 = 3$. Es trägt allerdings stets nur eine $2-$ Sylowuntergruppe (nämlich diejenigen Matrizen die zur Bestimmungsgleichung $z^2 = 1$ gehören) zum Stabilisator der Punkte $\{\infty, 0, 1, z\}$ bei.
Für $z = 2 \vee z = \frac{1}{2}$ ist die jeweilige Untergruppe von $\overline{G}$ nicht abgeschlossen gegenüber Matrizenmultiplikation.

$$z = 2 \leftrightarrow (1\infty)(0)(z) \leftrightarrow [\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}] \in \mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})$$

$$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & z \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & z \\ -1 & z \end{pmatrix} \notin \overline{G}$$

$$z = \frac{1}{2} \leftrightarrow (01)(\infty)(z), (0z1\infty) \leftrightarrow [\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}], [\begin{pmatrix} 0 & z \\ -1 & 1 \end{pmatrix}] \in \mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})$$

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & z \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -z+1 \\ -1 & 1 \end{pmatrix} \notin \overline{G}$$

- In Körpern der Charakteristik $p = 2$ gilt Folgendes: Die Gleichung $z^2 = 1$ hat keine nichttriviale Lösung wegen $1 = -1$. Weiterhin müssen wir folgende Fälle unterscheiden:
  a) $q = 2^n, n$ gerade.
  Dann gilt $3 \mid 2^n - 1 \; \forall n \in \mathbb{N}$ (Beweis durch Induktion nach $n \in \mathbb{N}$). Gemäß Lemma 3.3.7 enthält $\mathbb{F}_q$ die dritten Einheitswurzeln. Damit erhalten wir:

  $$z^2 - z + 1 = (z - \rho_3)(z - \rho_3^2) \in \mathbb{F}_q[z]$$

  wobei ρ_3 eine primitive dritte Einheitswurzel ist. Die Nullstellen des Polynoms $z^2 - z + 1$ sind in diesen Körpern also gerade die Elemente $z = \rho_3$ und $z = \rho_3^2$. Damit erhalten wir einen Stabilisator der Kardinalität 12.
  b) $p = 2, q = 2^n, n$ ungerade.
  Das Polynom $z^2 - z + 1$ hat keine Nullstellen in $\mathbb{F}_q$ und ist somit irreduzibel. Damit erhalten wir also den einfachsten Fall ohne Ausnahmebahnen.

- Für Körper der Charakteristik $p = 3$ erhalten wir: $|\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| = 24$. Es gilt in diesen Körpern gemäß den Rechenregeln im Primkörper $\mathbb{F}_3$ nämlich Folgendes:

  $$z = 2 \Leftrightarrow z = \frac{1}{2} \Leftrightarrow z^2 = 1$$

  $$z^2 - z + 1 = (z + 1)^2 = (z - 2)(z - \frac{1}{2})$$

- Im Fall $p \neq 2,3$ existieren für den Stabilisator von $\{\infty, 0, 1, z\}$ der Kardinalität 12 (abgesehen von der durch die Kleinschen Vierergruppebewirkten Permutationen der Zykelstruktur $2+2$) nur 3er Zykel, also:

$$\Leftrightarrow z^2 - z + 1 = 0$$

  Diese charakteristische Gleichung für die Existenz von 3er-Zykeln besitzt in Körpern der Charakterisitik ungleich $2,3$ genau dann Nullstellen in $\mathbb{F}_q$, ist also reduzibel über $\mathbb{F}_q$, wenn $\mathbb{F}_q$ die $6-$ ten Einheitswurzeln enthält, denn wir bemerken: Bei dem Polynom $z^2 - z + 1$ handelt es sich um das $6-$ te Kreisteilungspolynom $\Phi_6 = z^2 - z + 1 = (z - \rho_6)(z - \rho_6^5)$.
  Nach Lemma 3.3.7 ist dies äquivalent zu $q \equiv 1 \mod 6$.
  Weiterhin erhalten wir in diesem Fall für die dritte Gleichung folgende Lösung:

$$z^2 = 1$$

$$\Leftrightarrow z = \rho_4^2 \quad \vee \quad z = -1$$

  wobei ρ_4 eine primitive $4-$ ten Einheitswurzel ist. Dies ist genau dann der Fall, wenn schon gilt: $\mathbb{F}_q$ enthält die $4-$ ten Einheitswurzeln: $\{1, \rho_4, \rho_4^2, \rho_4^3\}$.

$$\Leftrightarrow q \equiv 1 \mod 4$$

  Im Fall $q \equiv 3 \mod 4$ hat die Gleichung $z^2 = 1$ ebenfalls paarweise verschiedene Lösungen 1 und $-1 \neq \rho_4^2$. Für $q \equiv 1 \mod 6$ gilt stets $q \equiv 1 \mod 4 \vee q \equiv 3 \mod 4$. Damit hat die Gleichung $z^2 = 1$ also für Körper, welche dieser Kongruenzbedingung genügen, stets eine nichttriviale Lösung $z = -1$. Wir erhalten also insgesamt je eine Ausnahmekonfiguration mit einem Stabilisator von 12 Elementen und 8 Elementen.

- Ist $p \neq 2$ mit $q \equiv 5 \mod 6$, so ist das Polynom $z^2 - z + 1 \in \mathbb{F}_q[z]$ irreduzibel. Für $q \equiv 5 \mod 6$ gilt ebenfalls immer: $q \equiv 1 \mod 4 \vee q \equiv 3 \mod 4$. Demnach liefert $z = -1$ also eine Ausnahmebahn mit Stabilisator der Kardinaltität 8.

Es bezeichne $V := \{(0)(1)(\infty)(z); (0\infty)(1z); (01)(z\infty); (0z)(1\infty)\}$ die Kleinsche Vierergruppe, die für alle z im Stabilisator einer Vierpunktkonfiguration in Normalform, enthalten ist, wobei $s := |\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})|$. Damit ergibt sich also vorläufig folgendes Bild für die Stabilisatorgruppe von 4 Punkten in Normalform:

z	s	Parameter q, p	Zykel
$\rho_4, -1$	8	$q \equiv 1 \mod 4$ $q \equiv 3 \mod 4$	$V \cup \{(1z)(0)(\infty); (0\infty)(1z); (01\infty z);$ $(0z\infty 1)\}$
$2,3$	12	$p = 2, q = 2^n, n$ gerade	$V \cup \{(1\infty z)(0); (1z\infty)(0); (0z\infty)(1);$ $(0\infty z)(1); (01z)(\infty); (0z1)(\infty);$ $(01\infty)(z); (0\infty 1)(z)\}$
ρ_6, ρ_6^5	12	$q \equiv 1 \mod 6$ $p \neq 2,3$	$V \cup \{(1\infty z)(0); (1z\infty)(0); (0z\infty)(1);$ $(0\infty z)(1); (01z)(\infty); (0z1)(\infty);$ $(01\infty)(z); (0\infty 1)(z)\}$
-1	24	$p = 3$	$S(\{\infty, 0, 1, z\})$

3.3.9 Bemerkung.

- Wie in Abschnitt 3.2 festgestellt, entsprechen den Bahnen von vier verschiedenen Punkten $\{z_0, z_1, z_2, z_3\} \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{0, 1, \infty\}$ unter Operation von S_4/V_4, gerade die Bahnen einer Vierpunktkonfiguration in Normalform $\{\infty, 0, 1, z\}$ unter Operation von $\overline{G}$. Damit erhalten wir folgende Korrespondenzen zwischen Bahnlänge $l(B')$ einer Bahn $B' \in \overline{G} \setminus \mathcal{X}_4$ und Kardinalität der Stabilisatorgruppe.

$$\begin{aligned} l(B') = 1 \quad &\overset{1:1}{\longleftrightarrow} \quad |\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| = 24 \\ l(B') = 2 \quad &\overset{1:1}{\longleftrightarrow} \quad |\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| = 12 \\ l(B') = 3 \quad &\overset{1:1}{\longleftrightarrow} \quad |\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| = 8 \\ l(B') = 6 \quad &\overset{1:1}{\longleftrightarrow} \quad |\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| = 4 \end{aligned}$$

- Betrachten wir wiederum die schon in 3.2.9 untersuchte Gleichung für die Gesamtzahl an Vierpunktkonfigurationen,

$$|\mathcal{X}_4| = \binom{q+1}{4} = \frac{(q+1)q(q-1)(q-2)}{4!} = \frac{q-2}{6}\frac{q(q^2-1)}{4}$$

  so erhalten wir nun mit $s_i = |\{\text{Vierpunktkonfigurationen mit Stabilisator der Kardinalität i}\}|$, wobei $i \in \{4, 8, 12, 24\}$, eine disjunkte Zerlegung der Vierpunktkonfigurationen in Normalform unter Operation von $\overline{G}$, durch Zusammenfassen von Konfigurationen mit gleicher Kardinalität des Stabilisators.

$$\frac{q-2}{6}\frac{q(q^2-1)}{4} = \frac{q(q^2-1)}{24}s_{24} + \frac{q(q^2-1)}{12}s_{12} + \frac{q(q^2-1)}{8}s_8 + \frac{q(q^2-1)}{4}s_4$$

- In der Gewichtsfunktion drücken wir diesmal die Bahnlänge durch die Kardinalität des Stabilisators aus, d.h. mit $l(B') = \frac{|\overline{G}|}{|\mathrm{Stab}_{\overline{G}}(\{\infty,0,1,z\})|} = \frac{q(q^2-1)}{|\mathrm{Stab}_{\overline{G}}(\{\infty,0,1,z\})|}$ ergibt sich:

$$\begin{aligned} w: \qquad \overline{G} \setminus \mathcal{X}_4 &\to \mathbb{Q} \\ B' &\mapsto \frac{4}{|\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})|} \end{aligned}$$

  mit $\{\infty, 0, 1, z\} \in B'$ und $|\mathrm{Stab}_{\overline{G}}(\{\infty, 0, 1, z\})| \in \{4, 8, 12, 24\}$.

- Mit der Gewichtsfunktion liegt nun folgende Situation vor:

$$\frac{q-2}{6} = \frac{1}{6}s_{24} + \frac{1}{3}s_{12} + \frac{1}{2}s_8 + 1s_4$$

  Damit erhalten wir also insbesondere eine Bestätigung der Überlegungen aus 3.2, denn für die Summe der gewichteten Bahnen gilt offenbar wiederum:

$$\sum_{B \in \overline{G} \setminus \mathcal{X}_4} w(B') = \frac{q-2}{6}$$

3.3.10 Zusammenfassung.
Wir können also den Lösungsvektor $(s_{24}, s_{12}, s_8, s_4)$ für die obige Bahnengleichung explizit in Abhängigkeit von q angeben.

1. $$q = 2^n,\ n = 2k,\ 2 \leq k \in \mathbb{N}, \quad (s_{24}, s_{12}, s_8, s_4) = (0, 1, 0, \frac{q-4}{6})$$

2. $$q = 2^n,\ n = 2k-1,\ 2 \leq k \in \mathbb{N}, \quad (s_{24}, s_{12}, s_8, s_4) = (0, 0, 0, \frac{q-2}{6})$$

3. $$q = 3^n,\ n \in \mathbb{N}, \quad (s_{24}, s_{12}, s_8, s_4) = (1, 0, 0, \frac{q-3}{6})$$

4. $$q \equiv 1 \mod 6, \quad (s_{24}, s_{12}, s_8, s_4) = (0, 1, 1, \frac{q-7}{6})$$

5. $$q \equiv 5 \mod 6, \quad (s_{24}, s_{12}, s_8, s_4) = (0, 0, 1, \frac{q-5}{6}).$$

4 Ordnung von $A \in G$ und Zykelstruktur bei Operation auf X

4.1 Ordnungen der Elemente in G

4.1.1 Lemma.

1. $$\forall a, b \in K \setminus \{0\}, n \in \mathbb{N} : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$$

2. $$\forall a \in K \setminus \{0\}, n \in \mathbb{N} : \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^n = \begin{pmatrix} a^n & na^{n-1} \\ 0 & a^n \end{pmatrix}$$

Beweis. Es ist jeweils Induktion nach $n \in \mathbb{N}$ durchzuführen. □

4.1.2 Bemerkung.

- Für Matrizen vom Typ 3a) gilt unter Beachtung des Lemmas 4.1.1 klarerweise:

$$\operatorname{ord}(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}) = \operatorname{ord}(a).$$

- Für Matrizen vom Typ 2) ergibt sich damit folgende Situation:

$$\operatorname{ord}(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}) = \min\{n \in \mathbb{N} \mid \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} = \min\{n \in \mathbb{N} \mid \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$$

$$= \operatorname{kgV}(\operatorname{ord}(a), \operatorname{ord}(b))$$

- Gemäß Lemma 4.1.1 ergibt sich für die Ordnung von Matrizen der Gestalt 3b):

$$\operatorname{ord}(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) = \min\{n \in \mathbb{N} \mid \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} = \min\{n \in \mathbb{N} \mid \begin{pmatrix} a^n & na^{n-1} \\ 0 & a^n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$$

$$= \operatorname{kgV}(\operatorname{ord}(a), p) = p \cdot \operatorname{ord}(a)$$

- Um die Ordnung von Matrizen des Typs 1, d.h. solchen Matrizen aus $GL(2, \mathbb{F}_q)$ angeben zu können, die ein irreduzibles charakteristisches Polynom aufweisen, sind einige algebraische Vorüberlegungen nötig.

4.1.3 Beobachtung.

Wir betrachten nun Matrizen vom Typ 1.
Sei also $\chi_A(x) = x^2 - bx - a \in K[x]$ das irreduzible charakteristische Polynom zur Matrix

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

Wir bestimmen zunächst den Zerfällungskörper des Polynoms $\chi_A(x)$.
Nach dem Verfahren von Kronecker erhalten wir:

$$K \subset L \cong K[x]/(x^2 - bx - a)$$

Sei $\alpha \in L \setminus \{0\}$ eine Nullstelle von $\chi_A(x)$. Dann gilt:

$$\alpha^2 - b\alpha - a = 0 \tag{9}$$
$$\Leftrightarrow \alpha^2 = b\alpha + a \tag{10}$$

Somit ergibt sich unter Verwendung von (10) und Beachtung des Frobenius-Homomorphismus:

$$\begin{aligned}
\chi_A(\alpha^q) &= (\alpha^q)^2 - b\alpha^q - a \\
&= (\alpha^2)^q - b\alpha^q - a \\
&= (b\alpha + a)^q - b\alpha^q - a \\
&= b^q\alpha^q + a^q - b\alpha^q - a \\
&= b\alpha + a - b\alpha - a \\
&= 0
\end{aligned}$$

Dann ist auch α^q Nullstelle von $\chi_A(x)$ und wir erhalten die Faktorisierung von χ_A durch:

$$\chi_A(x) = x^2 - bx - a = (x - \alpha)(x - \alpha^q) \quad \alpha \in L \setminus \{0\}$$

4.1.4 Algebraische Vorbereitungen.
Wir fassen im Nachfolgenden $L =< 1, \alpha >= \{x + \alpha y \mid x, y \in K\}$ insbesondere als $K-$ Vektorraum mit Basis $\{1, \alpha\}$ auf und bestimmen die Darstellungsmatrix der Multiplikation eines Elementes $\beta \in L$:

$$\begin{aligned}
\phi_\beta : L &\to L \\
z &\mapsto \beta \cdot z
\end{aligned}$$

Sei also $\beta = x + \alpha y$ fest gewählt. Dann gilt für die Basiselemente unter Verwendung von $\alpha^2 = b\alpha + a$:

$$\begin{aligned}
\phi_\beta(1 + 0\alpha) &= x + \alpha y \\
\phi_\beta(0 + 1\alpha) &= \alpha x + \alpha^2 y \\
&= \alpha x + (b\alpha + a)y \\
&= ay + \alpha(x + by)
\end{aligned}$$

Damit ergibt sich für die Darstellungsmatrix bzgl $\{1, \alpha\}$ offenbar:

$$M_\beta = \begin{pmatrix} x & ay \\ y & x + by \end{pmatrix}$$

Weiterhin stellen wir fest, dass die Abbildung

$$\begin{aligned}
\iota : \quad L &\hookrightarrow K^{2\times 2} \\
\beta &\mapsto M_\beta
\end{aligned}$$

eine nichttriviale Einbettung der Einheitengruppe L^* in die Menge der invertierbaren 2×2- Matrizen mit Einträgen aus K darstellt.
Für $\beta = \alpha \in L$ gilt:

$$\iota(\alpha) = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$$

Für $\beta = x,\ x \in K$ erhalten wir:

$$\iota(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

4.1.5 Bemerkung.
Mit der algebraischen Vorarbeit ergibt sich nun:

$$\mathrm{ord}_G(\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}) = \mathrm{ord}_G(\iota(\alpha)) = \mathrm{ord}_{L^*}(\alpha)$$

wegen der Invarianz der Ordnung unter injektiven Gruppenhomomorphismen.

4.2 Definition des Zykelzeigers

Wir lassen nun die Elemente von G auf X operieren und bestimmen für den jeweiligen Repräsentanten einer Konjugationsklasse die Zykelstruktur auf X. Hierzu ist die Entwicklung eines Begriffsapparates notwendig, mit welchem die Zerlegung der Menge X in Zykel unter Operation der Menge G in abstrakter Weise kodiert werden kann.
Bei der Notation orientiere ich mich im Nachfolgenden am Skript zur Vorlesung *Kombinatorik und Graphentheorie* von Prof. Dr. Ernst-Ulrich Gekeler aus dem WS 2011/2012.
4.2.1 Satz (Lemma von Burnside).
Die endliche Gruppe G operiere auf der endlichen Menge $\mathcal{X}$. Dann gilt:

$$|G \setminus \mathcal{X}| = \frac{1}{|G|} \sum_{g \in G} \phi_g$$

wobei ϕ_g die Anzahl der Fixpunkte von g bei Operation von G auf der Menge $\mathcal{X}$ bezeichnet. Insbesondere ist also der Mittelwert über die Fixpunktzahlen eine ganze Zahl.

Beweis. Es bezeichne $F := \{(g, x) \in G \times \mathcal{X} \mid g \cdot x = x\}$. Wir bestimmen nun die Kardinalität von F auf zwei verschiedene Weisen. Einerseits gilt:

$$|F| = \sum_{g \in G} \phi_g$$

Andererseits erhalten wir:

$$|F| = \sum_{x \in \mathcal{X}} |Stab_G(x)| = \sum_{x \in \mathcal{X}} \frac{|G|}{|Gx|} = |G| \sum_{x \in \mathcal{X}} \frac{1}{|Gx|} = |G| \sum_{G \setminus \mathcal{X}} 1 = |G||G \setminus \mathcal{X}|$$

Damit erhalten wir durch Gleichsetzen die Behauptung:

$$|G \setminus \mathcal{X}| = \frac{1}{|G|} \sum_{g \in G} \phi_g$$

□

(siehe auch [dB77], Seite 12, Satz 2.1 mit veränderter Notation).

4.2.2 Definition.
Die endliche Gruppe G operiere auf der endlichen Menge $\mathcal{X}$ mit $|\mathcal{X}| = n$. Unter Beachtung des schon in 3.2.6 definierten Zykeltyps betrachten wir die n verschiedenen Unbestimmten $X_1, ..., X_n$ und ordnen $g \in G$ das Monom $X_1^{c_1(g)} X_2^{c_2(g)} \cdots X_n^{c_n(g)}$ zu. Dann heißt der Ausdruck

$$Z_{G,\mathcal{X}}(X_1, ..., X_n) := \frac{1}{|G|} \sum_{g \in G} X_1^{c_1(g)} \cdots X_n^{c_n(g)}$$

der *Zykelzeiger* von G auf $\mathcal{X}$.

4.2.3 Beispiel.
Sei $G = S_3$ und $\mathcal{X} = \{1, 2, 3\}$. Dann operiert G auf $\mathcal{X}$ tautologisch vermöge:

$$\begin{aligned} G \times \mathcal{X} &\to \mathcal{X} \\ (\sigma, i) &\mapsto \sigma(i) \end{aligned}$$

Die Zykel auf $\mathcal{X}$ sind offenbar: $\{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (132)\}$. Damit ergibt sich:

$$Z_{G,\mathcal{X}}(X_1, X_2, X_3) = X_1^3 + 3X_1X_2 + 2X_3$$

4.2.4 Bemerkung.

- Ordnen wir X_i das Gewicht i zu, so ist $Z_{G,\mathcal{X}}$ ein isobares Polynom vom Gewicht n, d.h. es gilt: $\sum_{i=1}^{n} i c_i(g) = n$. Es seien $\mathcal{X}$ und $\mathcal{Y}$ Mengen mit $|\mathcal{X}| = n$ und $|\mathcal{Y}| = r$. Operiert G auf $\mathcal{X}$, so operiert G auch von links auf $\mathrm{Abb}(\mathcal{X}, \mathcal{Y}) := \mathcal{Y}^{\mathcal{X}}$ vermöge $(gf)(x) = f(g^{-1}x)$ für $f \in \mathcal{Y}^{\mathcal{X}}, x \in \mathcal{X}$ und $g \in G$.

- Man beachte, dass eine Operation der Gestalt

  $$\begin{aligned} G \times \mathcal{Y}^{\mathcal{X}} &\to \mathcal{Y}^{\mathcal{X}} \\ (g, f) &\mapsto f(g^{-1}x) \end{aligned}$$

  stets einer Abbildung von G in die Automorphismengruppe von $\mathcal{Y}^{\mathcal{X}}$ der folgenden Form entspricht:

  $$\begin{aligned} \epsilon : \quad G &\to \mathrm{Aut}(\mathcal{Y}^{\mathcal{X}}) \\ g &\mapsto \big(f \mapsto g \cdot f := x \mapsto f(g^{-1}x)\big) \end{aligned}$$

- Bei der Abbildung ϵ handelt es sich um einen Gruppenhomomorphismus. Dies erklärt die Verwendung von g^{-1} bei der induzierten Operation:

  $$\epsilon(gh)(f)(x) = gh \cdot f(x) = f((gh)^{-1}x) = f(h^{-1}g^{-1}x) = f(h^{-1}(g^{-1}x))$$

  Andererseits gilt aber auch:

  $$\epsilon(g) \circ \epsilon(h)(f)(x) = \epsilon(g)(h \cdot f)(x) = g \cdot h \cdot f(x) = h \cdot f(g^{-1}x) = f(h^{-1}g^{-1}x) = f(h^{-1}(g^{-1}x))$$

4.2.5 Satz.
Die Zahl der Bahnen von G auf $\mathcal{Y}^{\mathcal{X}}$ ist

$$|\mathcal{Y}^{\mathcal{X}} \setminus G| = Z_{G,\mathcal{X}}(r, ..., r) = \frac{1}{|G|} \sum_{g \in G} r^{c_1(g)+\cdots+c_n(g)}$$

Beweis. Nach dem Lemma von Burnside erhalten wir die Zahl der Bahnen auf $\mathcal{Y}^{\mathcal{X}}$ durch

$$\frac{1}{|G|} \sum_{g \in G} \phi_g$$

wobei $\phi_g = |\{$ Fixpunkte von g auf $\mathcal{Y}^{\mathcal{X}}\}|$. Für ein $g \in G$ gilt die folgende Kette von Äquivalenzen:
$f : \mathcal{X} \to \mathcal{Y}$ ist $g-$ invariant.
$\Leftrightarrow f$ ist konstant auf allen Zykeln von g.
$\Leftrightarrow f$ ist Funktion auf der Menge der Zykeln von g.
Hat g den Zykeltyp $(c_1, ..., c_n)$, so gibt es insgesamt genau $\sum_{i=1}^{n} c_i$ Zykel. Außerdem kann f genau r mögliche Werte auf einem Zykel annehmen. Damit gibt es also genau $r^{c_1+\cdots+c_n}$ solche $g-$ invariante Abbildungen $f \in \mathcal{Y}^{\mathcal{X}}$. □

([Eri96], Seite 121, Theorem 8.2)

4.3 Zykelstruktur bei Operation von G auf X

4.3.1 Zykelstruktur für Matrizen vom Typs 3.

- Leicht zu bestimmen ist die Zykelstruktur von Matrizen des Typs 3a).

$$(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, z) \mapsto \frac{az+0}{0z+a} = z \quad \forall z \in X$$

  Also erhalten wir die Zykelstruktur $\underbrace{1 + ... + 1}_{q+1}$ und demnach den Zykeltyp $(1, 1, ..., 1)$. Folglich erhalten wir mit $c_1(A) = q + 1$ und $c_i(A) = 0 \ \forall i > 1$ für Matrizen $A \in G$ der obigen Gestalt das entsprechende Monom im Zykelzeiger: X_1^{q+1}.

- Für die Matrizen vom Typ 3b) liegt die folgende Situation vor.

$$(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, \infty) \mapsto \frac{a}{0} = \infty$$

  Dies ergibt einen Zykel der Länge 1.
  Auf $\mathbb{F}_q \hookrightarrow \mathbb{P}^1(\mathbb{F}_q) \setminus \{\infty\}$ operiert $A = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ durch $z \mapsto \frac{ka+1}{a} = z + \frac{1}{a}$. Demnach ergibt sich: $(A^p, z) \mapsto z + \frac{p}{a} = z$. Daher zerfällt $\mathbb{F}_q$ unter der Gruppe $< A >$ in $\frac{q}{p}$ Zykel der Länge p. Wir erhalten also die nachfolgende Zykelstruktur:

$$1 + \underbrace{p + ... + p}_{\frac{q}{p}}$$

Also liegt gerade der Zykeltyp $(1, p, ..., p)$ vor, d.h. $c_1(A) = 1, c_p(A) = \frac{q}{p}, c_i(A) = 0 \ \forall i \neq 1, p.$

Das Monom im Zykelzeiger lautet: $X_1 X_p^{\frac{q}{p}}$.

4.3.2 Zykelstruktur für Matrizen vom Typ 2.
Wir wollen nun die Zykelstruktur von Matrizen des Typs 2 bestimmen.

$$(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \infty) \mapsto \frac{a}{0} = \infty$$

$$(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, 0) \mapsto \frac{a0+0}{b0+0} = 0.$$

Damit sind die Elemente $0, \infty$ Fixpunkte unter der Operation von A und wir erhalten zwei Zykel der Länge 1.
Auf $\mathbb{F}_q^* = \mathbb{P}^1(\mathbb{F}_q) \setminus \{0, \infty\}$ operiert $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ durch $z \mapsto \frac{a}{b} z$, d.h. es gilt: $(A^m, z) \mapsto (\frac{a}{b})^m z = z$ mit $m = \text{ord}(\frac{a}{b})$. Daher zerfällt $\mathbb{F}_q^*$ unter der Gruppe $< A >$ in $\frac{q-1}{m}$ Zykel der Länge m. Also ergibt sich für die Zykelstruktur

$$1 + 1 + \underbrace{m + ... + m}_{\frac{q-1}{m}}$$

und der Zykeltyp lautet $(1, 1, m, ..., m)$, d.h. $c_1(A) = 2, c_m(A) = \frac{q-1}{m}, c_i(A) = 0 \ \forall i \neq 2, m.$
Das Monom im Zykelzeiger lautet: $X_1^2 X_m^{\frac{q-1}{m}}$.

4.3.3 Zykelstruktur für Matrizen vom Typ 1.
Nun wollen wir Matrizen vom Typ 1 betrachten. Wir nehmen also an, dass $A = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ mit irreduzbiblem charakterischem Polynom $\chi_A(x) = x^2 - bx - a \in K[x]$, über dem Zerfällungskörper L die Gestalt $\chi_A(x) = (x - \alpha)(x - \alpha^q)$ $\alpha \in L$ annimmt.
Wir wollen nun die Operation von A auf $\mathbb{P}^1(\mathbb{F}_q)$ geschickter mit den algebraischen Vorüberlegungen zur Ordnung beschreiben.
Identifikation $L^*/K^* = \mathbb{P}^1(K)$.

$$\begin{aligned} \rho: \quad L^*/K^* &\to \mathbb{P}^1(K) \\ \overline{(x + \alpha y)} &\mapsto [\begin{pmatrix} x \\ y \end{pmatrix}] \end{aligned}$$

Die Abbildung ρ ist eine wohldefinierte Bijektion.
a) Wohldefiniertheit
Seien $x + \alpha y, \ x' + \alpha y'$ zwei Elemente in der gleichen Äquivalenzklasse. Dann gilt: $\exists k \in K^*$ mit $x' = kx, \ y' = ky$. Also erhalten wir: $(x + \alpha y) \mapsto [\binom{x}{y}] = [\binom{kx}{ky}] = [\binom{x'}{y'}]$.
b) Bijektivität
Es gilt offenbar $|L^*/K^*| = \frac{q^2-1}{q-1} = q+1 = |\mathbb{P}^1(K)|$. Somit genügt es die Surjektivität zu zeigen. Trivialerweise ist aber $\forall (x, y) \neq (0, 0) \in K$ schon durch $\rho^{-1}([\binom{x}{y}]) = \overline{(x + \alpha y)}$ per definitionem ein Urbild gegeben.

Mit den obigen Identifikationen und Korrespondenzen entspricht also die Operation von $\iota(\alpha) = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ auf $\mathbb{P}^1(K)$ vermöge Möbiustransformation der Multiplikation mit der Klasse $\overline{\alpha} \in L^*/K^*$. $\overline{a}$ operiert fixpunktfrei auf $\mathbb{P}^1(K) = L^*/K^*$, d.h. es gilt für die Zykelstruktur:

$$\underbrace{d + ... + d}_{\frac{q+1}{d}}$$

Also erhalten wir den Zykeltyp $(d, ..., d)$ mit $c_d(A) = \frac{q+1}{d}, c_i(A)\ \forall i \neq d$.
Das Monom im Zykelzeiger lautet also: $X_d^{\frac{q+1}{d}}$.

4.3.4 Bemerkung.
Damit sind sämtliche Ordnungen von Matrizen und Monome des Zykelzeigers bestimmt, sodass wir folgende tabellarische Übersicht erhalten:

Typ	Repräsentant	Ordnung	Monom
1	$\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$	$\mathrm{ord}_L(\alpha)$	$X_d^{\frac{q+1}{d}}$ $d := \mathrm{ord}_{L^*/K^*}(\overline{\alpha})$
2	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\mathrm{ord}(\frac{a}{b}) := m$	$X_1^2 X_m^{\frac{q-1}{m}}$
3 a)	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\mathrm{ord}(a)$	X_1^{q+1}
3 b)	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$p \cdot \mathrm{ord}(a)$	$X_1 X_p^{\frac{q}{p}}$

5 Bestimmung des Zykelzeigers

Wir erinnern uns, dass in Abschnitt 4.2 der Zykelzeiger für die Operation einer Gruppe auf einer Menge definiert wurde. Im vorangegangenen Abschnitt haben wir dann schon die auftretenden Monome für die Operation von G auf X bestimmt. Das Ziel dieses Abschnittes ist es nun den Zykelzeiger für die Operation von G auf X zu bestimmen. Die Anzahl für das Auftreten von $m = \mathrm{ord}(\frac{a}{b})$ mit $a \neq b \in K^*$ und $d = \mathrm{ord}_{L^*/K^*}(\alpha)$ mit $\alpha \in L^*$ in der Summe über Elemente der Gruppe G bei der Bestimmung des Zykelzeigers, können wir mit Hilfe der eulerschen φ- Funktion angeben, da wir die Gesamtzahl an auftretenden Summanden kennen.
Wir setzen hierbei $\sum_{e|n, e>0} \varphi(e) = n$ als bekannt voraus voraus ([FS82], Seite 170, Bemerkung 4.3.6).

5.1 Dritter und vierter Term im Zykelzeiger

5.1.1 Lemma.
Zu jedem Teiler $m \geq 2$ von $q-1$ gibt es $\varphi(m)\frac{(q-1)q(q+1)}{2}$ Summanden mit dem Monom $X_1^2 X_m^{\frac{q-1}{m}}$.

Beweis. Zu jedem Teiler $m \mid (q-1)$ gibt es $\varphi(m)$ viele Elemente $c \in \mathbb{F}_q^*$ der Ordnung m. Daher gibt es gerade $(q-1)\varphi(m)$ viele Matrizen $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ mit $\frac{a}{b} =: c$, wobei $c \in \mathbb{F}_q^*$ ein Element der Ordnung m ist.

Da jede Konjugationklasse die Größe $q(q+1)$ hat, erhalten wir somit $q(q+1)(q-1)\varphi(m)$ Elemente von angegebenem Zykeltyp. Diese werden allerdings doppelt gezählt, da $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix}$. Daher erhalten wir genau $\varphi(m)\frac{(q-1)q(q+1)}{2}$ Elemente der gesuchten Form. □

5.1.2 Lemma.
Es gibt genau $\varphi(d)\frac{q-1}{2}$ Summanden mit dem Monom $X_d^{\frac{q+1}{d}}$.

Beweis. Es bezeichne $I := \{f(x) = x^2 - bx - a \mid f(x) \in \mathbb{F}_q[x] \text{ irreduzibel}\}$.
Wir betrachten die Abbildung

$$\begin{aligned} \nu: \quad L^* &\to \{y \in L^* \mid y^{q+1} = 1\} =: W \\ \alpha &\mapsto \alpha^{q-1} \end{aligned}$$

Die Abbildung ν ist surjektiv mit Kern K^*, also gilt nach dem Homomorphiesatz für Gruppen:
$L^*/K^* \cong W$. Die Klasse $\overline{\alpha}$ von α in L^*/K^* hat dieselbe Ordnung wie $\nu(\alpha)$ in W.
Für $\alpha \in L^*/K^*$ gilt offenbar: $\nu(\alpha^q) = \alpha^{q(q-1)} = \alpha^{q^2-q} = \alpha^{1-q} = \nu(\alpha)^{-1}$. Daher stimmen die Ordnungen $\nu(\alpha)$ und $\nu(\alpha^q)$ überein.
Sei $2 \leq d \mid (q+1)$. Es gibt $\varphi(d)$ viele $y \in W$ mit der Ordnung d, also $(q-1)\varphi(d)$ viele α, sodass $\nu(\alpha)$ die Ordnung d hat. Die Menge dieser α zerfällt in $\frac{q-1}{2}\varphi(d)$ viele Paare $\{\alpha, \alpha^q\}$. Diese Paare entsprechen durch $\{\alpha, \alpha^q\} \mapsto (x-\alpha)(x-\alpha^q)$ eineindeutig den Elementen von I. □

5.2 Gestalt des Zykelzeigers

Mit der in Abschnitt 2 vorgenommer Einteilung der Gruppe G in Konjugationsklassen und der in Abschnitt 4 bestimmten Kodierung der Operation von G auf X in Monomen des Zykelzeigers, haben wir nun mit Lemma 5.1.1 und 5.1.2 und unter Beachtung der Invarianz der Zykelstruktur unter Konjugation alle Informationen zusammengestellt, um den Zykelzeiger für die Operation von G auf X angeben zu können.

$$Z_{G,X}(X_1, ..., X_{q+1}) = \frac{1}{|G|} \sum_{g \in G} X_1^{c_1(g)} \cdots X_{q+1}^{c_{q+1}(g)}$$

$$\begin{aligned} &= \frac{1}{(q-1)q(q^2-1)}((q-1)X_1^{q+1} + (q-1)(q^2-1)X_1 X_p^{\frac{q}{p}} \\ &+ \frac{q(q^2-1)}{2} \underbrace{\sum_{m \geq 2, m \mid (q-1)}^{q-1} \varphi(m) X_1^2 X_m^{\frac{q-1}{m}}}_{q-2 \text{ Summanden}} \\ &+ \frac{q(q-1)^2}{2} \underbrace{\sum_{d \geq 2, d \mid (q+1)}^{q+1} \varphi(d) X_d^{\frac{q+1}{d}})}_{q \text{ Summanden}} \end{aligned}$$

5.2.1 Bemerkung.
Für die Operation der Gruppe $\overline{G}$ auf X erhalten wir den gleichen Zykelzeiger wie für die Operation

der Gruppe G. Die Berechnung des Zykelzeigers durch Operation der Gruppe G erspart uns jedoch die Einteilung der Gruppe $\overline{G}$ in Konjugationsklassen.

6 Anwendung des Satzes von Pólya

Da wir nun den Zykelzeiger für die Operation von $\overline{G}$ auf X ermittelt haben, wollen wir jetzt die Abzählprobleme aus Abschnitt 4 sowie Verallgemeinerungen hiervon mit Hilfe des Zykelzeigers in eleganter Weise lösen. Dabei wird sich der Zykelzeiger als mächtiges Werkzeug entpuppen, mit dessen Hilfe unter vergleichsweise geringem Rechenaufwand die Zahl an $l-$ Punktkonfigurationen in X modulo der Operation von $\overline{G}$ bestimmt werden kann.

6.1 Der Satz von Pólya

6.1.1 Satz (Pólya 1937).
Es seien $\mathcal{X}$ und $\mathcal{Y}$ endliche Mengen mit Kardinalitäten $|\mathcal{X}| = n$ und $|\mathcal{Y}| = r$, wobei $\mathcal{Y} = \{y_1, ..., y_r\}$ und es bezeichne $\mathcal{Y}^{\mathcal{X}} =: \mathcal{F}$. Weiterhin sei G eine endliche Gruppe. Für $\underline{a} = (a_1, ..., a_r) \in \mathbb{N}_0^r$ mit $w(\underline{a}) := \sum_{j=1}^{r} a_j = n$ sei

$$\mathcal{F}(\underline{a}) := \{f \in \mathcal{F} \mid |f^{-1}(y_j)| = a_j\}$$

Somit ist also $\mathcal{F} = \bigcup_{w(\underline{a})=n} \mathcal{F}(\underline{a})$. Ferner ist $\mathcal{F}(\underline{a})$ stabil unter der Operation der Gruppe G, d.h. $\mathcal{F}(\underline{a})$ ist disjunkte Vereinigung von Bahnen von G auf $\mathcal{F}$. Für jedes $y_j \in \mathcal{Y}$ sei Y_j eine Unbestimmte. Dann gilt:

$$Z_{G,\mathcal{X}}\left(\sum_{1\le j\le r} Y_j, \sum_{1\le j\le r} Y_j^2, ..., \sum_{1\le j\le r} Y_j^n\right) = \sum_{\underline{a}\in\mathbb{N}_0^r \; w(\underline{a})=n} |G \setminus \mathcal{F}(\underline{a})| Y_1^{a_1} Y_2^{a_2} \cdots Y_r^{a_r}$$

(siehe auch in der Originalarbeit von Pólya [Pó37], Seite 162, Hauptsatz).

Beweis. siehe [Eri96], Seite 125, Beweis zu Theorem 8.3. □

6.1.2 Bemerkung.
Gemäß dem Satz von Pólya erhalten wir mit X und der Gruppe $\overline{G}$ folgende Interpretation:

- $\mathcal{Y} = \{y_1, ..., y_r\}$ sei eine Menge von r Farben.
- $f \in \mathcal{Y}^X$ sei eine Färbung auf der Menge X mit r Farben.
- Die Operation von $\overline{G}$ auf $\mathcal{Y}^X$ entspricht einer Permutation der gefärbten Punkte.

6.1.3 Ausgangssituation.
Für die in dieser Arbeit vornehmlich betrachtete Problemstellung- die Bestimmung der Anzahl von $l-$ Punktkonfigurationen in X modulo der Operation von $\overline{G}$ (insbesondere für $l = 3, 4, 5$)- benötigen wir Zweifärbungen. Wir betrachten also die folgende Situation.

$$X = \{x_1, ..., x_{q+1}\} \qquad \mathcal{Y} = \{y_1, y_2\}$$

$$\mathcal{F} = \mathrm{Abb}(X, \mathcal{Y}) = \mathcal{Y}^X$$

$$\underline{a} = (a_1, a_2) \in \mathbb{N}_0^2$$

wobei für die Gewichtsfunktion w stets gilt:

$$w(\underline{a}) = \sum_{j=1}^{2} a_j = a_1 + a_2 = q + 1 = |X|$$

Wir stellen fest, dass es ohne die Operation der Gruppe $\overline{G}$ zu beachten gerade 2^{q+1} mögliche Zweifärbungen auf der Menge X gibt. Dies deckt sich mit der im Satz von Pólya gewählten Zerlegung der Färbungen.

$$|\mathcal{F}| = |\bigcup_{w(\underline{a})=q+1} \mathcal{F}(\underline{a})\ | = \sum_{\underline{a}\in\mathbb{N}_0^2\ w(\underline{a})=q+1} |\mathcal{F}(\underline{a})| = \sum_{k=0}^{q+1} \binom{q+1}{k} = 2^{q+1}$$

Man beachte hierbei, dass die obige Vereinigung disjunkt ist. Es gelten im Nachfolgenden die Bezeichnungen:

$$\mathcal{F}_l := \mathcal{F}(\underline{a}) \qquad (a_1, a_2) = (l, q + 1 - l)$$

Wir erhalten für festes $S = \{z_1, ..., z_k\} \subset X$ und $l \in \{1, ..., q + 1\}$:

$$\begin{aligned} \mathrm{Stab}_{\overline{G}}(\mathcal{F}_l) &= \{g \in \overline{G} \mid f(g^{-1}S) = f(S)\} \\ &= \{g \in \overline{G} \mid g^{-1}S = S\} \\ &= \{g \in \overline{G} \mid gS = S\} \\ &= \mathrm{Stab}_{\overline{G}}(S) \end{aligned}$$

Dies zeigt, dass die Bestimmung der l- Punktkonfigurationen $\mathcal{X}_l$ (wie für $l = 3, 4$ in Abschnitt 4 und 5 „von Hand“ geschehen) äquivalent ist zur Bestimmung von $\mathcal{F}_l$, d.h. der Zahl der Zweifärbungen auf l Punkten. Der für unsere Überlegungen interessante Spezialfall ist also gerade $r = 2$ mit $Y = \{y_1, y_2\}$, wobei etwa gelte: $y_1 \leftrightarrow$ grün und $y_2 \leftrightarrow$ rot.
Die Anzahl der Konfigurationen von l grün gefärbten Punkten modulo der Operation der Gruppe $\overline{G}$ ist also der Koeffizient von $Y_1^l Y_2^{q+1-l}$ im Zykelzeiger beim Einsetzen von: $X_i \leftarrow (\sum_{1\le j\le 2} Y_j^i)_{i=1,...,n}$

1. Monom X_1^{q+1}

$$(Y_1 + Y_2)^{q+1} = \sum_{k=0}^{q+1} \binom{q+1}{k} Y_1^k Y_2^{q+1-k}$$

$$\rightarrow \binom{q+1}{l} Y_1^l Y_2^{q+1-l}$$

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$

$$\begin{aligned}(Y_1+Y_2)(Y_1^p+Y_2^p)^{\frac{q}{p}} &= Y_1((Y_1^p+Y_2^p)^{\frac{q}{p}}) + Y_2((Y_1^p+Y_2^p)^{\frac{q}{p}}) \\ &= Y_1 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p)^{\frac{q}{p}-k} + Y_2 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p)^{\frac{q}{p}-k} \\ &= ... \\ &= \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk+1} Y_2^{q-kp} + \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} Y_2^{q+1-kp} \\ &\to (\binom{\frac{q}{p}}{\frac{l-1}{p}} + \binom{\frac{q}{p}}{\frac{l}{p}}) Y_1^l Y_2^{q+1-l}\end{aligned}$$

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$

$$\begin{aligned}(Y_1+Y_2)^2(Y_1^m+Y_2^m)^{\frac{q-1}{m}} &= (Y_1^2+2Y_1Y_2+Y_2^2)(Y_1^m+Y_2^m)^{\frac{q-1}{m}} \\ &= Y_1^2(Y_1^m+Y_2^m)^{\frac{q-1}{m}} + 2Y_1Y_2(Y_1^m+Y_2^m)^{\frac{q-1}{m}} + Y_2^2(Y_1^m+Y_2^m)^{\frac{q-1}{m}} \\ &= ... \\ &= \sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_1^{km+2} Y_2^{q-1-km} + \sum_{k=0}^{\frac{q-1}{m}} 2\binom{\frac{q-1}{m}}{k} Y_1^{km+1} Y_2^{q-km} + \\ &\quad \sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_1^{km} Y_2^{q+1-km} \\ &\to (\binom{\frac{q-1}{m}}{\frac{l-2}{m}} + 2\binom{\frac{q-1}{m}}{\frac{l-1}{m}} + \binom{\frac{q-1}{m}}{\frac{l}{m}}) Y_1^l Y_2^{q+1-l}\end{aligned}$$

4. Monome vom Typ $X_d^{\frac{q+1}{d}}$

$$\begin{aligned}(Y_1^d+Y_2^d)^{\frac{q+1}{d}} &= \sum_{k=0}^{\frac{q+1}{d}} \binom{\frac{q+1}{d}}{k} (Y_1^d)^k (Y_2^d)^{\frac{q+1}{d}-k} \\ &= \sum_{k=0}^{\frac{q+1}{d}} \binom{\frac{q+1}{d}}{k} Y_1^{dk} Y_2^{q+1-dk} \\ &\to \binom{\frac{q+1}{d}}{\frac{l}{d}} Y_1^l Y_2^{q+1-l}\end{aligned}$$

6.1.4 Lemma.
Eine detaillierte Auswertung der einzelnen Monome liefert für festes l stets: Der Beitrag im Zykelzeiger ergibt ein Polynom vom Grad $l-3$ in $\mathbb{Q}[q]$.
$|\{l\text{- Punktkonfigurationen in } X \text{ modulo } \overline{G}\}| = \frac{q^{l-3}}{l!} + \mathcal{O}(q^{l-4})$.

Beweis. Wir werten die einzelnen Monome aus und ordnen die Ergebnisse gemäß der polynomialen Ordnung von q.

1. Monom X_1^{q+1}

$$\binom{q+1}{l} = \frac{(q+1)q(q-1)\cdots(q+1-(l-1))}{l!} = \frac{q(q^2-1)(q-2)\cdots(q+2-l)}{l!}$$
$$\Rightarrow (q-1)q(q^2-1)\frac{(q-2)\cdots(q+2-l)}{l!} = |G| \underbrace{\frac{(q-2)\cdots(q+2-l)}{l!}}_{\in\mathbb{Q}[q] \text{ Grad } l-3}$$

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$
   a) $p \mid l-1$

$$\binom{\frac{q}{p}}{\frac{l-1}{p}} = \frac{\frac{q}{p}(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l-1}{p}+1)}{(\frac{l-1}{p})!}$$
$$\Rightarrow (q-1)(q^2-1)q\frac{1}{p}\frac{(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l-1}{p}+1)}{(\frac{l-1}{p})!} = |G| \underbrace{\frac{1}{p}\frac{(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l-1}{p}+1)}{(\frac{l-1}{p})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l-1}{p}-1}$$

   b) $p \mid l$

$$\binom{\frac{q}{p}}{\frac{l}{p}} = \frac{\frac{q}{p}(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l}{p}+1)}{(\frac{l}{p})!}$$
$$\Rightarrow (q-1)(q^2-1)q\frac{1}{p}\frac{(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l}{p}+1)}{(\frac{l}{p})!} = |G| \underbrace{\frac{1}{p}\frac{(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l}{p}+1)}{(\frac{l}{p})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l}{p}-1}$$

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$
   a) $(m \mid l-2) \wedge (m \mid q-1)$

$$\binom{\frac{q-1}{m}}{\frac{l-2}{m}} = \frac{\frac{q-1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-2}{m}+1)}{(\frac{l-2}{m})!}$$
$$\Rightarrow \frac{q(q^2-1)}{2}\varphi(m)q-1\frac{\frac{1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-2}{m}+1)}{(\frac{l-2}{m})!} = |G|\frac{\varphi(m)}{2m}\underbrace{\frac{(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-2}{m}+1)}{(\frac{l-2}{m})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l-2}{m}}$$

b) $(m \mid l-1) \wedge (m \mid q-1)$

$$2\binom{\frac{q-1}{m}}{\frac{l-1}{m}} = 2\frac{\frac{q-1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-1}{m}+1)}{(\frac{l-1}{m})!}$$

$$\Rightarrow \frac{q(q^2-1)}{2}2\varphi(m)q-1\frac{\frac{1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-1}{m}+1)}{(\frac{l-1}{m})!} = |G|\frac{\varphi(m)}{m}\underbrace{\frac{(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-1}{m}+1)}{(\frac{l-1}{m})!}}_{\in\mathbb{Q}[q]\text{ Grad }\frac{l-1}{m}}$$

c) $(m \mid l) \wedge (m \mid q-1)$

$$\binom{\frac{q-1}{m}}{\frac{l}{m}} = \frac{\frac{q-1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!}$$

$$\Rightarrow \frac{q(q^2-1)}{2}\varphi(m)q-1\frac{\frac{1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!} = |G|\frac{\varphi(m)}{2m}\underbrace{\frac{(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!}}_{\in\mathbb{Q}[q]\text{ Grad }\frac{l}{m}}$$

4. Monome vom Typ $X_d^{\frac{q+1}{d}}$
   $(d \mid l) \wedge (d \mid q+1)$

$$\binom{\frac{q+1}{d}}{\frac{l}{d}} = \frac{\frac{q+1}{d}(\frac{q+1}{d}-1)\cdots(\frac{q+1}{d}-\frac{l}{d}+1)}{(\frac{l}{d})!}$$

$$\Rightarrow \frac{q(q-1)^2}{2}\varphi(d)q+1\frac{\frac{1}{d}(\frac{q+1}{d}-1)\cdots(\frac{q+1}{d}-\frac{l}{d}+1)}{(\frac{l}{d})!} = |G|\frac{\varphi(d)}{2d}\underbrace{\frac{(\frac{q+1}{d}-1)\cdots(\frac{q+1}{d}-\frac{l}{d}+1)}{(\frac{l}{d})!}}_{\in\mathbb{Q}[q]\text{ Grad }\frac{l}{d}-1}$$

Nun stellen wir fest, dass das erste Polynom bei Auswertung der Monome vom Typ X_1^{q+1} bei Ausmultiplikation der einzelnen Faktoren gerade die gewünschte Form $\frac{q^{l-3}}{l!} + \mathcal{O}(q^{l-4})$ annimmt. Dieses Monom tritt, unabhängig von der speziellen Wahl von q und l, immer in genau dieser Gestalt auf. Die übrigen Monome ergeben Polynome in q, die stark abhängig von den Parametern q und l sind, allerdings stets einen Grad vom Wert kleiner gleich $l-4$ aufweisen. □

6.2 Auswertung des Zykelzeigers für drei Punkte

Wir bestimmen nun die gewünschten Koeffizienten im Zykelzeiger für drei Punkte und vergleichen diese mit dem schon aus dem Dreipunktesatz bekannten Ergebnis für die Anzahl der Bahnen. Für drei Punkte gesucht: Koeffizient von $Y_1^3 Y_2^{q-2}$.

1. Monom X_1^{q+1}

$$\to \binom{q+1}{3} Y_1^3 Y_2^{q-2}$$

   $\to$ Beitrag für alle $q \geq 2$.

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$.

$$\to (\binom{\frac{q}{p}}{\frac{2}{p}} + \binom{\frac{q}{p}}{\frac{3}{p}}) Y_1^3 Y_2^{q-2}$$

→ Beitrag für $p \in \{2, 3\}$.

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$

$$\to (\binom{\frac{q-1}{m}}{\frac{1}{m}} + 2\binom{\frac{q-1}{m}}{\frac{2}{m}} + \binom{\frac{q-1}{m}}{\frac{3}{m}}) Y_1^3 Y_2^{q-2}$$

$$\stackrel{m \geq 2}{\longrightarrow} (2\binom{\frac{q-1}{m}}{\frac{2}{m}} + \binom{\frac{q-1}{m}}{\frac{3}{m}}) Y_1^3 Y_2^{q-2}$$

→ Beitrag für $m \in \{2, 3\}$.

4. Monome vom Typ $X_d^{\frac{q+1}{d}}$

$$\to \binom{\frac{q+1}{d}}{\frac{3}{d}} Y_1^3 Y_2^{q-2}$$

→ Beitrag für $d = 3$.

Mit obigen Auswertungen an den einzelnen Monomen im Zykelzeiger bringen wir den Zykelzeiger auf eine für uns günstige Form, indem wir die Kardinalität der Gruppe G ausklammern.

1. Beitrag durch Auswerten des 1. Terms

   $\to \frac{(q-1)q(q^2-1)}{6} = |G|\frac{1}{6}$

2. Beitrag durch Auswerten des 2. Terms

   - $p = 2$
     $\to (q-1)(q^2-1)\binom{\frac{q}{2}}{1} = |G|\frac{1}{2}$

   - $p = 3$
     $\to (q-1)(q^2-1)\binom{\frac{q}{3}}{1} = |G|\frac{1}{3}$

3. Beitrag durch Auswerten des 3. Terms

   - $m = 2$
     $\to \frac{q(q^2-1)}{2}\varphi(2)2\binom{\frac{q-1}{2}}{1} = |G|\frac{1}{2}$

- $m = 3$
  $\rightarrow \frac{q(q^2-1)}{2}\varphi(3)\binom{\frac{q-1}{3}}{1} = |G|\frac{1}{3}$

4. Beitrag durch Auswerten des 4. Terms

   $\rightarrow \frac{q(q-1)^2}{2}\varphi(3)\binom{\frac{q+1}{3}}{1} = |G|\frac{1}{3}$

Nun müssen diejenigen q bestimmt werden, für welche die obigen Monome tatsächlich einen Beitrag im Zykelzeiger liefern. Hierzu ist eine Fallunterscheidung notwendig.

1. $p = 2 \quad q = 2^n$
   n gerade
   1. Term: $|G|\frac{1}{6}$
   2. Term: $|G|\frac{1}{2}$
   3. Term: $|G|\frac{1}{3}$ (Beitrag für $m = 3$)
   4. Term: Kein Beitrag!

   $$\rightarrow \quad \frac{1}{6} + \frac{1}{2} + \frac{1}{3} = 1$$

   n ungerade
   1. Term: $|G|\frac{1}{6}$
   2. Term: $|G|\frac{1}{2}$
   3. Term: Kein Beitrag!
   4. Term: $|G|\frac{1}{3}$

   $$\rightarrow \quad \frac{1}{6} + \frac{1}{2} + \frac{1}{3} = 1$$

2. $p = 3 \quad q = 3^n$
   1. Term: $|G|\frac{1}{6}$
   2. Term: $|G|\frac{1}{3}$
   3. Term: $|G|\frac{1}{2}$ (Beitrag für $m = 2$)
   4. Term: Kein Beitrag!

   $$\rightarrow \quad \frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1$$

3. $q \equiv 1 \mod 6$
   1. Term: $|G|\frac{1}{6}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{1}{2} + \frac{1}{3}) = |G|\frac{5}{6}$ (Beitrag für $m = 2, 3$)
   4. Term: Kein Beitrag!

   $$\rightarrow \quad \frac{1}{6} + \frac{5}{6} = 1$$

4. $q \equiv 5 \mod 6$
   1. Term: $|G|\frac{1}{6}$
   2. Term: Kein Beitrag!

3. Term: $|G|\frac{1}{2}$ (Beitrag für $m = 2$)
4. Term: $|G|\frac{1}{3}$

$$\rightarrow \quad \frac{1}{6} + \frac{1}{2} + \frac{1}{3} = 1$$

6.2.1 Fazit.
Für Dreipunktkonfigurationen liefert der Dreipunktesatz unmittelbar das Ergebnis. Eine Auswertung des Zykelzeigers ist also für drei Punkte noch deutlich aufwendiger. Wir erhalten aber, wie nach dem Dreipunktesatz zu erwarten war:

$$\left\{ Z_{G,X} \left(\sum_{1 \leq j \leq 2} Y_j, \sum_{1 \leq j \leq 2} Y_j^2, ..., \sum_{1 \leq 2 \leq r} Y_j^{q+1} \right) \right\}_{Y_1^3 Y_2^{q-2}} = 1$$

6.3 Auswertung des Zykelzeigers für vier Punkte

Wir wollen nun den Zykelzeiger für vier Punkte auswerten und unser Ergebnis wiederum mit dem bereits „von Hand“ ermittelten Wert für die Zahl an Vierpunktkonfigurationen abgleichen. Für vier Punkte gesucht: Koeffizient von $Y_1^4 Y_2^{q-3}$.

1. Monom X_1^{q+1}

$$\rightarrow \binom{q+1}{4} Y_1^4 Y_2^{q-3}$$

→ Beitrag für alle $q \geq 3$.

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$

$$\rightarrow (\binom{\frac{q}{p}}{\frac{3}{p}} + \binom{\frac{q}{p}}{\frac{4}{p}}) Y_1^4 Y_2^{q-3}$$

→ Beitrag für $p \in \{2, 3\}$.

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$

$$\rightarrow (\binom{\frac{q-1}{m}}{\frac{2}{m}} + 2\binom{\frac{q-1}{m}}{\frac{3}{m}} + \binom{\frac{q-1}{m}}{\frac{4}{m}}) Y_1^4 Y_2^{q-3}$$

⇒ Beitrag für $m \in \{2, 3, 4\}$.

4. Monome vom Typ $X_d^{\frac{q+1}{d}}$

$$\rightarrow \binom{\frac{q+1}{d}}{\frac{4}{d}} Y_1^4 Y_2^{q-3}$$

→ Beitrag für $d \in \{2, 4\}$.

Mit obigen Auswertungen an den einzelnen Monomen im Zykelzeiger bringen wir den Zykelzeiger auf eine für uns günstige Form, indem wir die Kardinalität der Gruppe G ausklammern.

1. Beitrag durch Auswerten des 1. Terms
   $\to (q-1)q(q^2-1)\frac{q-2}{24} = |G|\frac{q-2}{24}$

2. Beitrag durch Auswerten des 2. Terms

   - $p = 2$
     $\to (q-1)(q^2-1)\binom{\frac{q}{2}}{2} = (q-1)(q^2-1)\frac{q(q-2)}{8} = |G|\frac{q-2}{8}$

   - $p = 3$
     $\to (q-1)(q^2-1)\binom{\frac{q}{3}}{1} = |G|\frac{1}{3}$

3. Beitrag durch Auswerten des 3. Terms

   - $m = 2$
     $\to \frac{q(q^2-1)}{2}\varphi(2)(\binom{\frac{q-1}{2}}{1} + \binom{\frac{q-1}{2}}{2}) = \frac{q(q^2-1)}{2}\binom{\frac{q+1}{2}}{2} = \frac{q(q^2-1)}{2}\frac{(q+1)(q-1)}{8} = |G|\frac{q+1}{16}$
   - $m = 3$
     $\to \frac{q(q^2-1)}{2}\varphi(3)2\binom{\frac{q-1}{3}}{1} = |G|\frac{2}{3}$
   - $m = 4$
     $\to \frac{q(q^2-1)}{2}\varphi(4)\binom{\frac{q-1}{4}}{1} = |G|\frac{1}{4}$

4. Beitrag durch Auswerten des 4. Terms

   - $d = 2$
     $\to \frac{q(q-1)^2}{2}\varphi(2)\binom{\frac{q+1}{2}}{2} = \frac{q(q-1)^2}{2}\frac{(q-1)(q+1)}{8} = |G|\frac{q-1}{16}$
   - $d = 4$
     $\to \frac{q(q-1)^2}{2}\varphi(4)\binom{\frac{q+1}{4}}{1} = |G|\frac{1}{4}$

Da beim dritten Monom im Zykelzeiger Kongruenzen modulo $2, 3, 4$ zu untersuchen sind, müssen wir insgesamt Kongruenzen modulo $\mathrm{kgV}(2,3,4) = 12$ betrachten. Hier bei ist es notwendig Charakteristik $2, 3$ gesondert zu behandeln.

1. $p = 2 \quad q = 2^n$
   n gerade
   1. Term: $|G|\frac{q-2}{24}$
   2. Term: $|G|\frac{q-2}{8}$
   3. Term: $|G|\frac{2}{3}$ (Beitrag für $m = 3$)
   4. Term: Kein Beitrag!

   $$\to \quad \frac{q+2}{6}$$

n ungerade
1. Term: $|G|\frac{q-2}{24}$
2. Term: $|G|\frac{q-2}{8}$
3. Term: Kein Beitrag!
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{q-2}{6}$$

2. $p = 3 \quad q = 3^n$
n gerade
1. Term: $|G|\frac{q-2}{24}$
2. Term: $|G|\frac{1}{3}$
3. Term: $|G|(\frac{q+1}{16} + \frac{1}{4})$ (Beitrag für $m = 2, 4$)
4. Term: $|G|\frac{q-1}{16}$ (Beitrag für $d = 2$)

$$\rightarrow \quad \frac{q+3}{6}$$

n ungerade
1. Term: $|G|\frac{q-2}{24}$
2. Term: $|G|\frac{1}{3}$
3. Term: $|G|\frac{q+1}{16}$ (Beitrag für $m = 2$)
4. Term: $|G|(\frac{q-1}{16} + \frac{1}{4})$ (Beitrag für $d = 2, 4$)

$$\rightarrow \quad \frac{q+3}{6}$$

3. $q \equiv 1 \mod 12$
1. Term: $|G|\frac{q-2}{24}$
2. Term: Kein Beitrag!
3. Term: $|G|(\frac{q+1}{16} + \frac{2}{3} + \frac{1}{4})$ (Beitrag für $m = 2, 3, 4$)
4. Term: $|G|\frac{q-1}{16}$ (Beitrag für $d = 2$)

$$\rightarrow \quad \frac{q+5}{6}$$

4. $q \equiv 5 \mod 12$
1. Term: $|G|\frac{q-2}{24}$
2. Term: Kein Beitrag!
3. Term: $|G|(\frac{q+1}{16} + \frac{1}{4})$ (Beitrag für $m = 2, 4$)
4. Term: $|G|\frac{q-1}{16}$ (Beitrag für $d = 2$)

$$\rightarrow \quad \frac{q+1}{6}$$

5. $q \equiv 7 \mod 12$
1. Term: $|G|\frac{q-2}{24}$
2. Term: Kein Beitrag!

3. Term: $|G|(\frac{q+1}{16} + \frac{2}{3})$ (Beitrag für $m = 2, 3$)
4. Term: $|G|(\frac{q-1}{16} + \frac{1}{4})$ (Beitrag für $d = 2, 4$)

$$\rightarrow \quad \frac{q+5}{6}$$

6. $q \equiv 11 \mod 12$
   1. Term: $|G|\frac{q-2}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q+1}{16})$ (Beitrag für $m = 2$)
   4. Term: $|G|(\frac{q-1}{16} + \frac{1}{4})$ (Beitrag für $d = 2, 4$)

$$\rightarrow \quad \frac{q+1}{6}$$

6.3.1 Zusammenfassung.
Wir können die Kongruenzen modulo 12 zusammenfassen zu Kongruenzen modulo 6 und erhalten somit gerade eine Bestätigung unserer Überlegungen aus Abschnitt 3, indem wir die Gesamtzahl der Bahnen in eine Summe mit den bekannten Ausnahmebahnen zerlegen.

Fall	Parameter q, p	Zahl an Vierpunktkonfigurationen
1	$q = 2^n,\ n = 2k,\ 2 \leq k \in \mathbb{N}$	$\frac{q+3}{6} = \frac{q-3}{6} + 1$
2	$q = 2^n,\ n = 2k-1,\ 2 \leq k \in \mathbb{N}$	$\frac{q-2}{6}$
3	$q = 3^n,\ 2 \leq n \in \mathbb{N}$	$\frac{q+3}{6} = \frac{q-3}{6} + 1$
4	$q \equiv 1 \mod 12$ $q \equiv 7 \mod 12$	$\frac{q+5}{6} = \frac{q-7}{6} + 1 + 1$
5	$q \equiv 5 \mod 12$ $q \equiv 11 \mod 12$	$\frac{q+1}{6} = \frac{q-5}{6} + 1$

6.4 Auswertung des Zykelzeigers für fünf Punkte

Um die Zahl an Fünfpunktkonfigurationen in X modulo der Operation von $\overline{G}$ durch direktes Ausrechnen der Bahnen zu bestimmen, muss man zunächst eine geeignete projektive Invariante definieren. Wir wollen im Nachfolgenden die Zahl der Fünfpunktkonfigurationen unter Verwendung des Zykelzeigers bestimmen. Für fünf Punkte gesucht: Koeffizient von $Y_1^5 Y_2^{q-4}$.

1. Monom X_1^{q+1}

$$\to \binom{q+1}{5} Y_1^5 Y_2^{q-4}$$

   $\to$ Beitrag $\forall q \geq 4$.

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$

$$\to (\binom{\frac{q}{p}}{\frac{4}{p}} + \binom{\frac{q}{p}}{\frac{5}{p}}) Y_1^4 Y_2^{q-3}$$

   $\to$ Beitrag für $p \in \{2, 5\}$.

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$

$$\to (\binom{\frac{q-1}{m}}{\frac{3}{m}} + 2\binom{\frac{q-1}{m}}{\frac{4}{m}} + \binom{\frac{q-1}{m}}{\frac{5}{m}}) Y_1^5 Y_2^{q-4}$$

   $\to$ Beitrag für $m \in \{2, 3, 4, 5\}$.

4. Monome vom Typ $X_d^{\frac{q+1}{d}}$

$$\to \binom{\frac{q+1}{d}}{\frac{5}{d}} Y_1^5 Y_2^{q-4}$$

   $\to$ Beitrag für $d = 5$.

Mit obigen Auswertungen an den einzelnen Monomen im Zykelzeiger fassen wir wiederum geschickt zusammen.

1. Beitrag durch Auswerten des 1. Terms
   $\to (q-1)q(q^2-1)\frac{(q-2)(q-3)}{120} = |G|\frac{(q-2)(q-3)}{120}$

2. Beitrag durch Auswerten des 2. Terms

   - $p = 2$
     $\to (q-1)(q^2-1)\binom{\frac{q}{2}}{2} = (q-1)(q^2-1)\frac{q(q-2)}{8} = |G|\frac{q-2}{8}$

   - $p = 5$
     $\to (q-1)(q^2-1)\binom{\frac{q}{5}}{1} = (q-1)(q^2-1)\frac{q}{5} = |G|\frac{1}{5}$

3. Beitrag durch Auswerten des 3. Terms
   - $m = 2$
     $\to \frac{q(q^2-1)}{2}\varphi(2)2\binom{\frac{q-1}{2}}{2} = q(q^2-1)\frac{(q-1)(q-3)}{8} = |G|\frac{q-3}{8}$
   - $m = 3$
     $\to \frac{q(q^2-1)}{2}\varphi(3)\binom{\frac{q-1}{3}}{1} = q(q^2-1)\frac{q-1}{3} = |G|\frac{1}{3}$
   - $m = 4$
     $\to \frac{q(q^2-1)}{2}\varphi(4)2\binom{\frac{q-1}{4}}{1} = q(q^2-1)2\frac{q-1}{2} = |G|\frac{1}{2}$
   - $m = 5$
     $\to \frac{q(q^2-1)}{2}\varphi(5)\binom{\frac{q-1}{5}}{1} = q(q^2-1)2\frac{q-1}{5} = |G|\frac{2}{5}$
4. Beitrag durch Auswerten des 4. Terms
   $\to \frac{q(q-1)^2}{2}\varphi(5)\binom{\frac{q+1}{5}}{1} = q(q-1)^2 2\frac{q+1}{5} = |G|\frac{2}{5}$

Nun müssen wir noch die jeweiligen Werte von q bestimmen, für welche die obigen Monome einen Beitrag liefern. Hierzu ist wieder eine umfassende Fallunterscheidung notwendig. Da beim dritten Monom im Zykelzeiger Kongruenzen modulo $3, 4, 5$ zu untersuchen sind, müssen wir insgesamt Kongruenzen modulo $\mathrm{kgV}(3, 4, 5) = 60$ betrachten. Hier bei ist es notwendig Charakteristik $2, 5$ gesondert zu behandeln. Außerdem empfiehlt es sich, den Fall $p = 3$ ebenfalls getrennt zu untersuchen, um sich die Untersuchung einer Vielzahl von Kongruenzen modulo 60 zu ersparen. Behandeln wir also Körper mit Charakteristik $2, 3, 5$ gesondert, so müssen nur noch Kongruenzen von Primzahlen modulo 60 betrachtet werden.

1. $p = 2 \quad q = 2^n$
   n gerade
   a) $n \equiv 0 \mod 4$.
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: $|G|\frac{q-2}{8}$
   3. Term: $|G|(\frac{1}{3} + \frac{2}{5}) = |G|\frac{11}{15}$ (Beitrag für $m = 3, 5$)
   4. Term: Kein Beitrag!

$$\to \quad \frac{(q-2)(q+12)+88}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{64}{120}$$

   b) $n \equiv 2 \mod 4$.
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: $|G|\frac{q-2}{8}$
   3. Term: $|G|\frac{1}{3}$ (Beitrag für $m = 3$)
   4. Term: $|G|\frac{2}{5}$

$$\to \quad \frac{(q-2)(q+12)+88}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{64}{120}$$

   n ungerade
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: $|G|\frac{q-2}{8}$

3. Term: Kein Beitrag!
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-2)(q+12)}{120} = \frac{q^2}{120} + \frac{10}{120}q - \frac{24}{120}$$

2. $p = 3 \quad q = 3^n$

n gerade

a) $n \equiv 0 \mod 4$

1. Term: $|G|\frac{(q-2)(q-3)}{120}$
2. Term: Kein Beitrag!
3. Term: $|G|(\frac{q-3}{8} + \frac{1}{2} + \frac{2}{5})$ (Beitrag für $m = 2, 4, 5$)
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+108}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{69}{120}$$

b) $n \equiv 2 \mod 4$

1. Term: $|G|\frac{(q-2)(q-3)}{120}$
2. Term: Kein Beitrag!
3. Term: $|G|(\frac{q-3}{8} + \frac{1}{2})$ (Beitrag für $m = 2, 4$)
4. Term: $|G|\frac{2}{5}$

$$\rightarrow \quad \frac{(q-3)(q+13)+108}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{69}{120}$$

n ungerade

1. Term: $|G|\frac{(q-2)(q-3)}{120}$
2. Term: Kein Beitrag!
3. Term: $|G|\frac{q-3}{8}$ (Beitrag für $m = 2$)
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)}{120} = \frac{q^2}{120} + \frac{10}{120}q - \frac{39}{120}$$

3. $p = 5, q = 5^n$

n gerade

1. Term: $|G|\frac{(q-2)(q-3)}{120}$
2. Term: $|G|\frac{1}{5}$
3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3} + \frac{1}{2}) = |G|(\frac{q-3}{8} + \frac{5}{6})$ (Beitrag für $m = 2, 3, 4$)
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+124}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{85}{120}$$

n ungerade

1. Term: $|G|\frac{(q-2)(q-3)}{120}$
2. Term: $|G|\frac{1}{5}$
3. Term: $|G|(\frac{q-3}{8} + \frac{1}{2}) =$ (Beitrag für $m = 2, 4$)
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+84}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{45}{120}$$

4. $q \equiv 1 \mod 60$
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3} + \frac{1}{2} + \frac{2}{5}) = |G|(\frac{q-3}{8} + \frac{37}{30})$ (Beitrag für $m = 2, 3, 4, 5$)
   4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+184}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{145}{120}$$

5. $q \equiv 7 \mod 60$
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3})$ (Beitrag für $m = 2, 3$)
   4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+40}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{1}{120}$$

6. $q \equiv 11 \mod 60$
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{2}{5})$ (Beitrag für $m = 2, 5$)
   4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+48}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{9}{120}$$

7. $q \equiv 13 \mod 60$
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3} + \frac{1}{2}) = |G|(\frac{q-3}{8} + \frac{5}{6})$ (Beitrag für $m = 2, 3, 4$)
   4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+100}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{61}{120}$$

8. $q \equiv 17 \mod 60$
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{1}{2})$ (Beitrag für $m = 2, 4$)
   4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+60}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{21}{120}$$

9. $q \equiv 19 \mod 60$
   1. Term: $|G|\frac{(q-2)(q-3)}{120}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3})$ (Beitrag für $m = 2, 3$)
   4. Term: $|G|\frac{2}{5}$

$$\rightarrow \quad \frac{(q-3)(q+13)+88}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{49}{120}$$

10. $q \equiv 23 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|\frac{q-3}{8}$ (Beitrag für $m = 2$)
    4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)}{120} = \frac{q^2}{120} + \frac{10}{120}q - \frac{39}{120}$$

11. $q \equiv 29 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|(\frac{q-3}{8} + \frac{1}{2})$ (Beitrag für $m = 2, 4$)
    4. Term: $|G|\frac{2}{5}$

$$\rightarrow \quad \frac{(q-3)(q+13)+108}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{69}{120}$$

12. $q \equiv 31 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3} + \frac{2}{5}) = |G|(\frac{q-3}{8} + \frac{11}{15})$ (Beitrag für $m = 2, 3, 5$)
    4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+88}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{49}{120}$$

13. $q \equiv 37 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|(\frac{q-3}{8} + \frac{1}{3} + \frac{1}{2}) = |G|(\frac{q-3}{8} + \frac{5}{6})$ (Beitrag für $m = 2, 3, 4$)
    4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+100}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{61}{120}$$

14. $q \equiv 41 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!

3. Term: $|G|(\frac{q-3}{8}+\frac{1}{2}+\frac{2}{5}) = |G|\frac{9}{10}$ (Beitrag für $m = 2, 4, 5$)
4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+108}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{69}{120}$$

15. $q \equiv 43 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|(\frac{q-3}{8}+\frac{1}{3})$ (Beitrag für $m = 2, 3$)
    4. Monom: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+40}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{1}{120}$$

16. $q \equiv 47 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|\frac{q-3}{8}$ (Beitrag für $m = 2$)
    4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)}{120} = \frac{q^2}{120} + \frac{10}{120}q - \frac{39}{120}$$

17. $q \equiv 53 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|(\frac{q-3}{8}+\frac{1}{2})$ (Beitrag für $m = 2, 4$)
    4. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-3)(q+13)+60}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{21}{120}$$

18. $q \equiv 59 \mod 60$
    1. Term: $|G|\frac{(q-2)(q-3)}{120}$
    2. Term: Kein Beitrag!
    3. Term: $|G|\frac{q-3}{8}$ (Beitrag für $m = 2$)
    4. Term: $|G|\frac{2}{5}$

$$\rightarrow \quad \frac{(q-3)(q+13)+48}{120} = \frac{q^2}{120} + \frac{10}{120}q + \frac{9}{120}$$

6.4.1 Zusammenfassung.

Fassen wir also Kongruenzen zusammen, so ergeben sich letztlich 12 verschiedene Werte für Fünfpunktkonfigurationen in Abhängigkeit von q. Wir erhalten außerdem eine Bestätigung von Lemma 6.1.4 mit dem führenden Term $\frac{q^2}{120} + \frac{1}{12}q$. Die Zahl der Fünfpunktkonfigurationen unterscheidet sich also nur bezüglich des absoluten Term $a \in \mathbb{Q}$ in einem quadratischen Polynom in q, ist also stets von der Form $\frac{q^2}{120} + \frac{1}{12}q + a$ Dies können wir übersichtlich in einer Tabelle zusammenstellen.

Fall	Parameter q, p	a
1	$q = 2^n,\ n = 2k,\ 4 \leq k \in \mathbb{N}$	$\frac{8}{15}$
2	$q = 2^n,\ n = 2k-1,\ 2 \leq k \in \mathbb{N}$	$-\frac{1}{5}$
3	$q = 3^n,\ n = 2k,\ 2 \leq k \in \mathbb{N}$ $q \equiv 29 \mod 60$ $q \equiv 41 \mod 60$	$\frac{23}{40}$
4	$q = 3^n,\ n = 2k-1,\ k \in \mathbb{N}$ $q \equiv 23 \mod 60$ $q \equiv 47 \mod 60$	$-\frac{13}{40}$
5	$q = 5^n,\ n = 2k,\ k \in \mathbb{N}$	$\frac{17}{24}$
6	$q = 5^n,\ n = 2k-1,\ k \in \mathbb{N}$	$\frac{3}{8}$
7	$q \equiv 1 \mod 60$	$\frac{29}{24}$
8	$q \equiv 7 \mod 60$ $q \equiv 43 \mod 60$	$\frac{1}{120}$
9	$q \equiv 11 \mod 60$ $q \equiv 59 \mod 60$	$\frac{3}{40}$
10	$q \equiv 13 \mod 60$ $q \equiv 37 \mod 60$	$\frac{61}{120}$
11	$q \equiv 17 \mod 60$ $q \equiv 53 \mod 60$	$\frac{7}{40}$
12	$q \equiv 19 \mod 60$ $q \equiv 31 \mod 60$	$\frac{49}{120}$

Eine direkte Rekonstruktion der Ausnahmekonfigurationen für fünf Punkte ist zwar erstrebenswert, erscheint aber mit dieser Vorgehensweise nicht möglich. Eine Berechnung der Zahl an 5- Punktkonfigurationen auf X modulo der Operation von $\overline{G}$ ohne Verwendung des Satzes von Pólya ist jedoch relativ kompliziert. Bei einer weiter wachsenden Zahl von Punkten wird die Berechnung „von Hand“ umständlich bis unmöglich, allerdings mit der Auswertung des Zykelzeigers vergleichsweise elegant realisiert.

7 Spezielle Dreifärbungen auf X

Wir betrachten nun auch Punktkonfigurationen unter Dreifärbungen auf der Menge X. Hierbei wollen wir uns lediglich speziellen Dreifärbungen auf X zuwenden, welche eine Auswertung des Zykelzeigers ohne größeren Rechenaufwand zulassen.

7.1 Situation.

Zeichnet man in einer $l-$ Punktkonfiguration einen Punkt zusätzlich aus, so entspricht dies gerade einer speziellen Dreifärbung.

$$X = \{x_1, ..., x_{q+1}\} \qquad \mathcal{Y} = \{y_1, y_2, y_3\}$$

$$F = Abb(X, \mathcal{Y}) = \mathcal{Y}^X$$

$$\underline{a} = (1, a_2, a_3) \in \{1\} \times \mathbb{N}_0^2$$

wobei für die Gewichtsfunktion w stets gilt:

$$w(\underline{a}) = 1 + a_2 + a_3 = q + 1 = |X|$$

Wir beschränken uns also auf den Spezialfall von einem ausgezeichneten Punkt. Wir werten den Zykelzeiger aus für Färbungen der Gestalt $(1, l, q + 1 - (l + 1)) = (1, l, q - l)$.
Gesucht ist also der Koeffizient von $Y_1^1 Y_2^l Y_3^{q-l}$.

1. Term: X_1^{q+1}

$$(Y_1 + Y_2 + Y_3)^{q+1} = (Y_1 + (Y_2 + Y_3))^{q+1} = \sum_{k=0}^{q+1} \binom{q+1}{k} Y_1^k (Y_2 + Y_3)^{q+1-k}$$

$$\overset{k=0}{\to} \binom{q+1}{1}\binom{q}{l} Y_1^1 Y_2^l Y_3^{q-l}$$

2. Term: $X_1 X_p^{\frac{q}{p}}$

$$\begin{aligned}(Y_1 + Y_2 + Y_3)(Y_1^p + Y_2^p + Y_3^p)^{\frac{q}{p}} &= Y_1(Y_1^p + Y_2^p + Y_3^p)^{\frac{q}{p}} + Y_2(Y_1^p + Y_2^p + Y_3^p)^{\frac{q}{p}} + Y_3(Y_1^p + Y_2^p + Y_3^p)^{\frac{q}{p}} \\ &= Y_1 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p + Y_3^p)^{\frac{q}{p}-k} + Y_2 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p + Y_3^p)^{\frac{q}{p}-k} + \\ &\quad Y_3 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p + Y_3^p)^{\frac{q}{p}-k} \\ &= ...\end{aligned}$$

Der erste Summand liefert nur für $k = 0$ einen Beitrag. Der zweite und dritte Summand würden lediglich für $k = \frac{1}{p}$ einen Beitrag liefern, was wegen $p > 1$ jedoch nicht möglich ist. Damit ergibt

also die Auswertung des ersten Summanden für $k = 0$ gerade Folgendes:

$$Y_1^1(Y_2^p + Y_3^p)^{\frac{q}{p}} = Y_1 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_2^{pk}(Y_3^p)^{\frac{q}{p}-k}$$

$$\rightarrow \binom{\frac{q}{p}}{\frac{l}{p}} Y_1^1 Y_2^l Y_3^{q-l}$$

3. Term $X_1^2 X_m^{\frac{q-1}{m}}$

$$\begin{aligned}(Y_1 + Y_2 + Y_3)^2(Y_1^m + Y_2^m + Y_3^m)^{\frac{q-1}{m}} &= (Y_1 + (Y_2 + Y_3))^2(Y_1^m + Y_2^m + Y_3^m)^{\frac{q-1}{m}} \\ &= (Y_1^2 + 2Y_1(Y_2 + Y_3) + (Y_2 + Y_3)^2)(Y_1^m + Y_2^m + Y_3^m)^{\frac{q-1}{m}} \\ &= Y_1^2(Y_1^m + Y_2^m + Y_3^m)^{\frac{q-1}{m}} + 2Y_1(Y_2 + Y_3)(Y_1^m + Y_2^m + Y_3^m)^{\frac{q-1}{m}} + \\ &\quad (Y_2 + Y_3)^2(Y_1^m + Y_2^m + Y_3^m)^{\frac{q-1}{m}} \\ &= ...\end{aligned}$$

Der erste Summand liefert keinen Beitrag. Der dritte Summand kann bei näherer Betrachtung auch keinen Beitrag liefern, denn werten wir diesen Summanden aus so ergibt sich Folgendes:

$$(Y_2 + Y_3)^2(Y_1^m + (Y_2^m + Y_3^m))^{\frac{q-1}{m}} = (Y_2 + Y_3)^2 \sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_1^{km}(Y_2^m + Y_3^m)^{\frac{q-1}{m}-k}$$

Es müsste $k = \frac{1}{m}$ gelten, was jedoch wegen $m \geq 2$ nicht sein kann. Also muss lediglich der zweite Summand ausgewertet werden.

$$2Y_1Y_2 \sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_2^{km} Y_3^{q-1-km} + 2Y_1Y_3 \sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_2^{km} Y_3^{q-1-km}$$

$$\rightarrow 2(\binom{\frac{q-1}{m}}{\frac{l-1}{m}} + \binom{\frac{q-1}{m}}{\frac{l}{m}}) Y_1^1 Y_2^l Y_3^{q-l}$$

4. Term $X_d^{\frac{q+1}{d}}$

$$\begin{aligned}(Y_1^d + Y_2^d + Y_3^d)^{\frac{q+1}{d}} &= (Y_1^d + (Y_2^d + Y_3^d))^{\frac{q+1}{d}} \\ &= \sum_{k=0}^{\frac{q+1}{d}} \binom{\frac{q+1}{d}}{k} Y_1^{kd}(Y_2^d + Y_3^d)^{\frac{q+1}{d}-k}\end{aligned}$$

Es müsste $k = \frac{1}{d}$ gelten, was jedoch wegen $d \geq 2$ wiederum nicht sein kann. Daher liefern Ausdrücke der obigen Form keinen Beitrag zum gesuchten Koeffizienten im Zykelzeiger.

7.1.1 Lemma.
Eine detaillierte Auswertung der einzelnen Monome liefert für festes l stets: Der Beitrag im Zyklenzeiger ergibt ein Polynom vom Grad $l-2$ in $\mathbb{Q}[q]$.
$|\{l$- Punktkonfigurationen in X modulo $\overline{G}$ mit zusätzlich markiertem Punkt $\}| = \frac{q^{l-2}}{l!} + \mathcal{O}(q^{l-3})$.

Beweis. 1. Term

$$\binom{q+1}{1}\binom{q}{l} = \frac{(q+1)q(q-1)\cdots(q+1-l)}{l!} = \frac{q(q^2-1)(q-2)\cdots(q+1-l)}{l!}$$
$$\to (q-1)q(q^2-1)\frac{(q-2)\cdots(q+1-l)}{l!} = |G| \underbrace{\frac{(q-2)\cdots(q+1-l)}{l!}}_{\in\mathbb{Q}[q] \text{ Grad } l-2}$$

2. Term

$$\binom{\frac{q}{p}}{\frac{l}{p}} = \frac{\frac{q}{p}(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l}{p}+1)}{(\frac{l}{p})!}$$
$$\to (q-1)(q^2-1)q\frac{1}{p}\frac{(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l}{p}+1)}{(\frac{l}{p})!} = |G| \underbrace{\frac{1}{p}\frac{(\frac{q}{p}-1)\cdots(\frac{q}{p}-\frac{l}{p}+1)}{(\frac{l}{p})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l}{p}-1}$$

3. Term
   a) $(m \mid l-1) \wedge (m \mid q-1)$

$$2\binom{\frac{q-1}{m}}{\frac{l-1}{m}} = 2\frac{\frac{q-1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-1}{m}+1)}{(\frac{l-1}{m})!}$$
$$\to \frac{q(q^2-1)}{2}2\varphi(m)q-1\frac{\frac{1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-1}{m}+1)}{(\frac{l-1}{m})!} = |G|\frac{\varphi(m)}{m}\underbrace{\frac{(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l-1}{m}+1)}{(\frac{l-1}{m})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l-1}{m}}$$

   b) $(m \mid l) \wedge (m \mid q-1)$

$$2\binom{\frac{q-1}{m}}{\frac{l}{m}} = \frac{\frac{q-1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!}$$
$$\to \frac{q(q^2-1)}{2}2\varphi(m)q-1\frac{\frac{1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!} = |G|\frac{\varphi(m)}{m}\underbrace{\frac{(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l}{m}}$$

Wir stellen wir fest, dass das erste Polynom bei Auswertung der Monome vom Typ X_1^{q+1} bei Ausmultiplikation der einzelnen Faktoren gerade die gewünschte Form $\frac{q^{l-2}}{l!} + \mathcal{O}(q^{l-3})$ annimmt. Analog zu Lemma 6.1.4 liefern die übrigen Ausdrücke in Abhängigkeit von q und l stets Polynome in q vom Grad kleiner gleich $l-3$. □

7.2 Auswertung für vier Punkte

Wir bestimmen nun die gewünschten Koeffizienten im Zykelzeiger für vier Punkte, d.h. $l = 3$. Ein spezieller Punkt in einer Vierpunktkonfiguration ist also zusätzlich markiert. Für $l = 3$ gesucht: Koeffizient von $Y_1^1 Y_2^3 Y_3^{q-3}$.

1. Monom: X_1^{q+1}

   $$\to \binom{q+1}{1}\binom{q}{3} Y_1^1 Y_2^3 Y_3^{q-3}$$

   $\to$ Beitrag für alle $q \geq 4$.

2. Monom: $X_1 X_p^{\frac{q}{p}}$.

   $$\to \binom{\frac{q}{p}}{\frac{3}{p}} Y_1^1 Y_2^3 Y_3^{q-3}$$

   $\to$ Beitrag für $p = 3$.

3. Monom $X_1^2 X_m^{\frac{q-1}{m}}$

   $$\to 2(\binom{\frac{q-1}{m}}{\frac{2}{m}} + \binom{\frac{q-1}{m}}{\frac{3}{m}}) Y_1^1 Y_2^3 Y_2^{q-3}$$

   $\to$ Beitrag für $m \in \{2, 3\}$.

Mit den Beiträgen der einzelnen Monome im Zykelzeiger werten wir den Zykelzeiger insgesamt aus.

1. Beitrag durch Auswerten des 1. Terms

   $\to \frac{(q-1)q(q^2-1)(q-2)}{6} = |G|\frac{q-2}{6}$

2. Beitrag durch Auswerten des 2. Terms
   $\to (q-1)(q^2-1)\binom{\frac{q}{3}}{1} = |G|\frac{1}{3}$

3. Beitrag durch Auswerten des 3. Terms

   - $m = 2$
     $\to q(q^2-1)\varphi(2)\binom{\frac{q-1}{2}}{1} = |G|\frac{1}{2}$

   - $m = 3$
     $\to q(q^2-1)\varphi(3)\binom{\frac{q-1}{3}}{1} = |G|\frac{2}{3}$

Nun müssen diejenigen q bestimmt werden, für welche obigen Monome tatsächlich einen Beitrag im Zykelzeiger liefern. Hierzu ist eine Fallunterscheidung notwendig. Wir behandeln Körper mit Charakteristik $p = 2, 3$ gesondert.

1. $p = 2 \quad q = 2^n$
   n gerade
   1. Term: $|G|\frac{q-2}{6}$
   2. Term: Kein Beitrag!
   3. Term: $|G|\frac{2}{3}$ (Beitrag für $m = 3$)

   $$\rightarrow \quad \frac{q+2}{6}$$

   n ungerade
   1. Term: $|G|\frac{q-2}{6}$
   2. Term: Kein Beitrag!
   3. Term: Kein Beitrag!

   $$\rightarrow \quad \frac{q-2}{6}$$

2. $p = 3 \quad q = 3^n$
   1. Term: $|G|\frac{q-2}{6}$
   2. Term: $|G|\frac{1}{3}$
   3. Term: $|G|\frac{1}{2}$ (Beitrag für $m = 2$)

   $$\rightarrow \quad \frac{q+3}{6}$$

3. $q \equiv 1 \mod 6$
   1. Term: $|G|\frac{q-2}{6}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{1}{2} + \frac{2}{3}) = |G|\frac{5}{6}$ (Beitrag für $m = 2, 3$)

   $$\rightarrow \quad \frac{q+5}{6}$$

4. $q \equiv 5 \mod 6$
   1. Term: $|G|\frac{q-2}{6}$
   2. Term: Kein Beitrag!
   3. Term: $|G|\frac{1}{2}$ (Beitrag für $m = 2$)

   $$\rightarrow \quad \frac{q+1}{6}$$

Dieses Ergebnis deckt sich verblüffenderweise gerade mit der in 6.3 ermittelten Zahl an Vierpunktkonfigurationen ohne zusätzlich markierten Punkt.

7.3 Auswertung für fünf Punkte

Ein spezieller Punkt in einer Fünfpunktkonfiguration ist nun zusätzlich ausgezeichnet. Für $l = 4$ gesucht: Koeffizient von $Y_1^1 Y_2^4 Y_3^{q-4}$.

1. Monom X_1^{q+1}
$$\to \binom{q+1}{1}\binom{q}{4} Y_1^1 Y_2^4 Y_3^{q-4}$$
$\to$ Beitrag für alle $q \geq 5$.

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$.
$$\to \binom{\frac{q}{p}}{\frac{4}{p}} Y_1^1 Y_2^4 Y_3^{q-4}$$
$\to$ Beitrag für $p = 2$.

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$
$$\to 2(\binom{\frac{q-1}{m}}{\frac{3}{m}} + \binom{\frac{q-1}{m}}{\frac{4}{m}}) Y_1^1 Y_2^3 Y_2^{q-3}$$
$\to$ Beitrag für $m \in \{2, 3\}$.

Durch geschicktes Zusammenfassen und Ausklammern der Kardinalität von G erhalten wir wiederum die Gesamtauswertung des Zykelzeigers.

1. Beitrag durch Auswerten des 1. Terms
$\to \frac{(q-1)q(q^2-1)(q-2)(q-3)}{24} = |G|\frac{(q-2)(q-3)}{24}$

2. Beitrag durch Auswerten des 2. Terms
$\to (q-1)(q^2-1)\binom{\frac{q}{2}}{2} = |G|\frac{q-2}{8}$

3. Beitrag durch Auswerten des 3. Terms

   - $m = 2$
   $\to q(q^2-1)\varphi(2)\binom{\frac{q-1}{2}}{2} = |G|\frac{q-3}{8}$

   - $m = 3$
   $\to q(q^2-1)\varphi(3)\binom{\frac{q-1}{3}}{1} = |G|\frac{2}{3}$

   - $m = 4$
   $\to q(q^2-1)\varphi(4)\binom{\frac{q-1}{4}}{1} = |G|\frac{1}{2}$

Nun müssen diejenigen q bestimmt werden, für welche obigen Monome tatsächlich einen Beitrag im Zykelzeiger liefern. Hierzu ist eine Fallunterscheidung notwendig. Wir behandeln Körper mit Charakteristik $p = 2, 3$ gesondert.

1. $p = 2 \quad q = 2^n$
   n gerade
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: $|G|\frac{q-2}{8}$
   3. Term: $|G|\frac{2}{3}$ (Beitrag für $m = 3$)

$$\rightarrow \quad \frac{q(q-2)+16}{24} = \frac{q^2}{24} - \frac{2}{24}q + \frac{16}{24}$$

   n ungerade
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: $|G|\frac{q-2}{8}$
   3. Term: Kein Beitrag!

$$\rightarrow \quad \frac{q(q-2)}{24} = \frac{q^2}{24} - \frac{2}{24}q$$

2. $p = 3 \quad q = 3^n$
   n gerade
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{1}{2})$ (Beitrag für $m = 2, 4$)

$$\rightarrow \quad \frac{(q-3)(q+1)+12}{24} = \frac{q^2}{24} - \frac{2}{24}q + \frac{9}{24}$$

   n ungerade
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|\frac{q-3}{8}$ (Beitrag für $m = 2, 4$)

$$\rightarrow \quad \frac{(q-3)(q+1)}{24} = \frac{q^2}{24} - \frac{2}{24}q - \frac{3}{24}$$

3. $q \equiv 1 \mod 12$
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8} + \frac{2}{3} + \frac{1}{2})$ (Beitrag für $m = 2, 3, 4$)

$$\rightarrow \quad \frac{(q-3)(q+1)+28}{24} = \frac{q^2}{24} - \frac{2}{24}q + \frac{25}{24}$$

4. $q \equiv 5 \mod 12$
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8}\frac{1}{2})$ (Beitrag für $m = 2, 4$)

$$\rightarrow \quad \frac{(q-3)(q+1)+12}{24} = \frac{q^2}{24} - \frac{2}{24}q + \frac{9}{24}$$

5. $q \equiv 7 \mod 12$
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8}\frac{2}{3})$ (Beitrag für $m = 2, 3$)

$$\rightarrow \quad \frac{(q-3)(q+1)+16}{24} = \frac{q^2}{24} - \frac{2}{24}q + \frac{13}{24}$$

6. $q \equiv 11 \mod 12$
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   2. Term: Kein Beitrag!
   3. Term: $|G|(\frac{q-3}{8})$ (Beitrag für $m = 2$)

$$\rightarrow \quad \frac{(q-3)(q+1)}{24} = \frac{q^2}{24} - \frac{2}{24}q - \frac{3}{24}$$

Fassen wir wiederum Kongruenzen zusammen, so ergeben sich letztlich 6 verschiedene Werte für Fünfpunktkonfigurationen mit einem zusätzlich markierten Punkt in Abhängigkeit von q. Wie bei Fünfpunktkonfigurationen ohne zusätzlich markierten Punkt, unterscheidet sich das Polynom nur bezüglich des absoluten Term $a \in \mathbb{Q}$ in einem quadratischen Polynom in q, ist also stets von der Form

$$\frac{q^2}{120} + \frac{1}{12}q + a$$

Dies können wir wiederum übersichtlich in einer Tabelle zusammenstellen.

Fall	Parameter q, p	a
1	$q = 2^n,\ n = 2k,\ 2 \leq k \in \mathbb{N}$	$\frac{2}{3}$
2	$q = 2^n,\ n = 2k-1,\ 2 \leq k \in \mathbb{N}$	0
3	$q = 3^n,\ n = 2k,\ k \in \mathbb{N}$ $q \equiv 5 \mod 12$	$\frac{3}{8}$
4	$q = 3^n,\ n = 2k-1,\ 2 \leq k \in \mathbb{N}$ $q \equiv 11 \mod 12$	$-\frac{1}{8}$
5	$q \equiv 1 \mod 12$	$\frac{25}{24}$
6	$q \equiv 7 \mod 12$	$\frac{13}{24}$

8 Spezielle Vierfärbungen auf fünf Punkten

8.1 Situation

Abschließend wollen wir auch spezielle Vierfärbungen auf fünf Punkten in X betrachten. Dabei betrachten wir nun den Spezialfall von zwei ausgezeichneten Punkten. Also wir werten den Zykelzeiger aus für Färbungen der Gestalt
$(1,1,l,q+1-(l+1+1)) = (1,1,l,q-1-l)$. Gesucht ist also der Koeffizient von $Y_1^1 Y_2^1 Y_3^l Y_4^{q-1-l}$.

1. Monom X_1^{q+1}

$$(Y_1+Y_2+Y_3+Y_4)^{q+1} = (Y_1+(Y_2+Y_3+Y_4))^{q+1} = \sum_{k=0}^{q+1} \binom{q+1}{k} Y_1^k (Y_2+Y_3+Y_4)^{q+1-k}$$

$$\overset{k=0}{\to} \binom{q+1}{1}\binom{q}{1}\binom{q-1}{l} Y_1^1 Y_2^1 Y_3^l Y_4^{q-l-1}$$

2. Monome vom Typ $X_1 X_p^{\frac{q}{p}}$.

$$\begin{aligned}(Y_1+Y_2+Y_3+Y_4)(Y_1^p+Y_2^p+Y_3^p+Y_4^p)^{\frac{q}{p}} &= Y_1(\sum_{i=1}^4 Y_i^p)^{\frac{q}{p}} + Y_2(\sum_{i=1}^4 Y_i^p)^{\frac{q}{p}} + Y_3(\sum_{i=1}^4 Y_i^p)^{\frac{q}{p}} + Y_4(\sum_{i=1}^4 Y_i^p)^{\frac{q}{p}} \\ &= Y_1 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p+Y_3^p+Y_4^p)^{\frac{q}{p}-k} + \\ &\quad Y_2 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p+Y_3^p+Y_4^p)^{\frac{q}{p}-k} + \\ &\quad Y_3 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p+Y_3^p+Y_4^p)^{\frac{q}{p}-k} + \\ &\quad Y_4 \sum_{k=0}^{\frac{q}{p}} \binom{\frac{q}{p}}{k} Y_1^{pk} (Y_2^p+Y_3^p+Y_4^p)^{\frac{q}{p}-k} \\ &= \ldots\end{aligned}$$

Der erste Summand kann nur für $k=0$ einen Beitrag liefern, was im nächsten Schritt aber zum Wert $k=\frac{1}{p}$ im Binomialkoeffizienten vor Y_2 führen muss. Dies ist jedoch wegen $p>1$ nicht möglich. Analog zeigt man, dass der zweite, dritte und vierte Summand lediglich für $k=\frac{1}{p}$ einen Beitrag liefern können, was nicht möglich ist. Damit ergibt also die Auswertung des zweiten Summanden keinen Beitrag.

3. Monome vom Typ $X_1^2 X_m^{\frac{q-1}{m}}$

$$(Y_1+Y_2+Y_3+Y_4)^2(\sum_{i=1}^{4} Y_i^m)^{\frac{q-1}{m}} = ((Y_1+Y_2)+(Y_3+Y_4))^2(Y_1^m+Y_2^m+Y_3^m)^{\frac{q-1}{m}}$$

$$= ((Y_1+Y_2)^2+2(Y_1+Y_2)(Y_3+Y_4)+(Y_3+Y_4)^2)(\sum_{i=1}^{4} Y_i^m)^{\frac{q-1}{m}}$$

Man sieht sofort, dass der dritte Summand in der Klammer $((Y_3+Y_4)^2\sum_{i=1}^4 Y_i^m)$ keinen Beitrag liefern kann, da stets $\frac{1}{m}$ im Binomialkoeffizienten bei der weiteren Auswertung vorkommt. Ebenso eliminiert man bei genauerem Hinsehen den Term $2(Y_1+Y_2)(Y_3+Y_4)\sum_{i=1}^4 Y_i^m$. Vom ersten Summanden in der Klammer bleibt nur noch $2Y_1Y_2\sum_{i=1}^4 Y_i^m$ übrig (da ansonsten Exponenten $2>1$ bei Y_1 bzw. Y_2 vorkommen).

$$2Y_1Y_2\sum_{i=1}^{4} Y_i^m = 2Y_1Y_2\sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_1^{km}(Y_2^m+Y_3^m+Y_4^m)^{\frac{q-1}{m}-k} \overset{k=0}{\to} 2Y_1Y_2(Y_2^m+Y_3^m+Y_4^m)^{\frac{q-1}{m}-k}$$

$$= 2Y_1Y_2\sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_2^{km}(Y_3^m+Y_4^m)^{\frac{q-1}{m}-k} \overset{k=0}{\longrightarrow} 2Y_1Y_2(Y_3^m+Y_4^m)^{\frac{q-1}{m}-k}$$

$$= 2Y_1Y_2\sum_{k=0}^{\frac{q-1}{m}} \binom{\frac{q-1}{m}}{k} Y_3^{km}Y_4^{q-1-km} \overset{k=\frac{l}{m}}{\longrightarrow} 2\binom{\frac{q-1}{m}}{\frac{l}{m}} Y_1^1Y_2^1Y_3^lY_4^{q-1-l}$$

4. Monom $X_d^{\frac{q+1}{d}}$

$$(Y_1^d+Y_2^d+Y_3^d+Y_4^d)^{\frac{q+1}{d}} = (Y_1^d+(Y_2^d+Y_3^d+Y_4^d))^{\frac{q+1}{d}}$$

$$= \sum_{k=0}^{\frac{q+1}{d}} \binom{\frac{q+1}{d}}{k} Y_1^{kd}(Y_2^d+Y_3^d+Y_4^d)^{\frac{q+1}{d}-k}$$

Es müsste $k=\frac{1}{d}$ gelten, was jedoch wegen $d\geq 2$ wiederum nicht sein kann. Daher liefern Ausdrücke der obigen Form keinen Beitrag zum gesuchten Koeffizienten im Zykelzeiger.

8.1.1 Lemma.
Eine detaillierte Auswertung der einzelnen Monome liefert für festes l stets: Der Beitrag im Zyklenzeiger ergibt ein Polynom vom Grad $l-1$ in $\mathbb{Q}[q]$.
$|\{l$- Punktkonfigurationen in X modulo $\overline{G}$ mit zwei zusätzlich markierten Punkten $\}|$
$= \frac{q^{l-1}}{l!} + \mathcal{O}(q^{l-2})$.

Beweis. 1. Monom

$$\binom{q+1}{1}\binom{q}{1}\binom{q-1}{l} = \frac{(q+1)q(q-1)\cdots(q-l)}{l!} = \frac{q(q^2-1)(q-2)\cdots(q-l)}{l!}$$

$$\to (q-1)q(q^2-1)\frac{(q-2)\cdots(q-l)}{l!} = |G| \underbrace{\frac{(q-2)\cdots(q-l)}{l!}}_{\in\mathbb{Q}[q] \text{ Grad } l-1}$$

2. Monom
$(m \mid l) \wedge (m \mid q-1)$

$$2\binom{\frac{q-1}{m}}{\frac{l}{m}} = \frac{\frac{q-1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!}$$

$$\to \frac{q(q^2-1)}{2}2\varphi(m)q-1\frac{\frac{1}{m}(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!} = |G|\frac{\varphi(m)}{m}\underbrace{\frac{(\frac{q-1}{m}-1)\cdots(\frac{q-1}{m}-\frac{l}{m}+1)}{(\frac{l}{m})!}}_{\in\mathbb{Q}[q] \text{ Grad } \frac{l}{m}}$$

Analog zur Vorgehensweise bei der asymptotischen Betrachtung von l- Punktkonfigurationen (mit einem zusätzlich markierten Punkt) genügt es den ersten Term im Zykelzeiger, der für alle q stets den gleichen Beitrag liefert auszumultiplizieren. □

8.2 Auswertung für fünf Punkte

Zwei Punkte in einer Fünfpunktkonfiguration sind nun zusätzlich ausgezeichnet. Für $l = 3$ gesucht: Koeffizient von $Y_1^1Y_2^1Y_3^3Y_4^{q-4}$.

1. Monom X_1^{q+1}

$$\to \binom{q+1}{1}\binom{q}{1}\binom{q-1}{3}Y_1^1Y_2^1Y_3^3Y_4^{q-4}$$

→ Beitrag für alle $q \geq 5$.

2. Monome vom Typ $X_1^2X_m^{\frac{q-1}{m}}$

$$\to 2\binom{\frac{q-1}{m}}{\frac{3}{m}}Y_1^1Y_2^1Y_3^3Y_4^{q-4}$$

→ Beitrag für $m = 3$.

Mit obigen Auswertungen an den einzelnen Monomen im Zykelzeiger werten wir zunächst den Zykelzeiger insgesamt aus:

1. Beitrag durch Auswerten des 1. Monoms
→ $\frac{(q-1)q(q^2-1)(q-2)(q-3)}{24} = |G|\frac{(q-2)(q-3)}{6}$

2. Beitrag durch Auswerten des 3. Monoms
   $m = 3$
   $\rightarrow q(q^2-1)\varphi(3)\binom{\frac{q-1}{3}}{1} = |G|\frac{2}{3}$

Nun müssen diejenigen q bestimmt werden, für welche obigen Monome tatsächlich einen Beitrag im Zykelzeiger liefern. Hierzu ist eine Fallunterscheidung notwendig. Wir unterscheiden anhand von Kongruenzen modulo 3.

1. $q \equiv 0 \mod 3,\ p = 3 \quad q = 3^n$
   1. Term: $|G|\frac{(q-2)(q-3)}{6}$
   3. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-2)(q-3)}{6} = q^2 + \frac{5}{6}q + 1$$

2. $q \equiv 1 \mod 3$
   1. Term: $|G|\frac{(q-2)(q-3)}{6}$
   3. Term: $|G|\frac{2}{3}$

$$\rightarrow \quad \frac{(q-2)(q-3)+4}{6} = q^2 + \frac{5}{6}q + \frac{5}{3}$$

3. $q \equiv 2 \mod 3$
   1. Term: $|G|\frac{(q-2)(q-3)}{24}$
   3. Term: Kein Beitrag!

$$\rightarrow \quad \frac{(q-2)(q-3)}{6} = q^2 + \frac{5}{6}q + 1$$

Bemerkenswerterweise wird die Auswertung des Zykelzeigers für diese speziellen Vierfärbungen sogar leichter als die Auswertung für Zwei- und Dreifärbungen. Die meisten Monome liefern keine Beiträge und wir müssen nur anhand von Kongruenzen modulo 3 unterscheiden. Es ergibt sich wiederum ein quadratisches Polynom, welches die Gestalt $\frac{q^2}{6} + \frac{5}{6}q + a$ mit $a \in \{1, \frac{5}{3}\}$ hat.

Fall	Parameter q, p	a
1	$q \equiv 0 \mod 3$	1
2	$q \equiv 1 \mod 3$	$\frac{5}{3}$
3	$q \equiv 2 \mod 3$	1

9 Zusammenfassung und Ausblick

Abschließend sollen noch einmal die Ergebnisse dieser Arbeit in kompakter Weise zusammengefasst, und ein Ausblick auf etwaige weiterführende Forschungsmöglichkeiten gegeben werden.
In *Abschnitt 1* wurden die meisten der für diese Arbeit benötigten Grundbegriffe motiviert und eingeführt. Die Strategie zur Charakterisierung der Operation von $GL(2, \mathbb{F}_q)$ auf $\mathbb{P}^1(\mathbb{F}_q)$ bestand dabei in folgenden Schritten:

1. Bestimmung von Anzahl und Größe der Konjugationsklassen von $GL(2, \mathbb{F}_q)$

2. Bestimmung des Zykeltyps eines Repräsentanten jeder Konjugationsklasse (dabei macht man sich zunutze, dass konjugierte Elemente vom gleichen Zykeltyp sind)

Daher wurde in *Abschnitt 2* die Gruppe $GL(2, \mathbb{F}_q)$ in Konjugationsklassen eingeteilt. Mit Sicherheit hätte ich mir die ausführliche Begründung dieser Klassifikation durch Angabe einer geeigneten Referenz sparen können. Allerdings hat somit auch der im Mathematikstudium noch nicht soweit fortgeschrittene Leser die Gelegenheit diese Klassifikation Schritt für Schritt nachzuvollziehen, zumal ich auch keine geeignete Literatur gefunden habe, wo die Einteilung der Gruppe $GL(2, \mathbb{F}_q)$ in detaillierter Weise zu finden ist.
In *Abschnitt 3* haben wir die Zahl an 3- bzw. 4- Punktkonfigurationen durch direktes Ausrechnen der Bahnen mit Hilfe von Invarianten aus der projektiven Geometrie angegeben.
Außerdem wurde die jeweilige Stabilisatorgruppe von vier Punkten in Abhängigkeit von q ausgerechnet. Beide Vorgehensweise führen auf das gleiche Ergebnis.
In *Abschnitt 4* wurde die Zykelstruktur der Operation eines Repräsentanten jeder Konjugationsklasses auf $\mathbb{P}^1(\mathbb{F}_q)$ bestimmt und in Monomen des Zykelzeigers zusammengefasst.
Bei drei Punkten lieferte uns ein Satz aus der projektiven Geometrie unmittelbar das Ergebnis, dass es nur eine solche Konfiguration von Punkten gibt. Für vier Punkte erhielten wir mit dieser Vorgehensweise eine, respektive der Kardinalität des Stabilisators gewichtete, Formel für die gesuchte Zahl der Konfigurationen. Hierbei konnten wir explizit die Ausnahmebahnen, d.h. die ausgezeichneten Punktkonfigurationen in $\mathbb{P}^1(\mathbb{F}_q)$, bestimmen.
In *Abschnitt 5* haben wir dann die noch fehlenden Vorbereitungen abgeschlossen, um schließlich den Zykelzeiger für die Operation von $GL(2, \mathbb{F}_q)$ auf $\mathbb{P}^1(\mathbb{F}_q)$ angeben zu können. Dabei konnten wir auf die Einteilung von $PGL(2, \mathbb{F}_q)$ in Konjugationsklassen verzichten, da wir offensichtlich für beide Gruppen den gleichen Zykelzeiger erhalten.
Abschnitt 6 diente einerseits dazu den für den weiteren Verlauf der Arbeit benötigten Satz von Polya anzugeben und andererseits diesen Satz auf l-Punktkonfigurationen (mit $l \in \{3, 4, 5\}$) anzuwenden, d.h. den jeweils gesuchten Koeffizienten im Zykelzeiger zu bestimmen. Dabei kamen wir für $l = 3, 4$ zum gleichen, wie schon „von Hand“, d.h. ohne die Abzähltheorie von Pólya, ermittelten Ergebnis. Für Fünfpunktkonfigurationen erhielten wir ein, jeweils von der Kardinalität des Körpers $\mathbb{F}_q$ abhängiges, quadratisches Polynom in q. Dieses Ergebnis wirft insbesondere folgende Fragen auf:

- Gibt es eine Möglichkeit die Zahl der, gemäß Stabilisatorgruppe gewichteten, Fünfpunktkonfigurationen aus dem, mit Hilfe des Zykelzeigers ermittelten, Ergebnis zu rekonstruieren?

- Kann man eine allgemeine projektive Invariante von l Punkten angeben, mit deren Hilfe die Berechnung der Ausnahmekonfigurationen von l Punkten in $\mathbb{P}^1(\mathbb{F}_q)$ relativ leicht möglich ist?

In *Abschnitt 7* und *Abschnitt 8* haben wir auch die Zahl von speziellen Drei- und Vierfärbungen auf vier bzw. fünf Punkten mit Hilfe des Zykelzeigers ausgewertet. Hierbei konnten wir feststellen, dass sich die Zahl der Vierpunktkonfigurationen bei zusätzlicher Markierung eines Punktes nicht verändert.
Bei fünf Punkten ergab sich, wie für Zweifärbungen, ein quadratisches Polynom in q, wobei die Komplexität der Auswertung des Zykelzeigers für diese speziellen Färbungen sogar abgenommen hat.
Wenden wir uns dem allgemeinen Fall von k- Färbungen zu, so ist klar, dass das erste Monom im Zykelzeiger, unabhängig von q, stets den gleichen Beitrag liefert. Anhand dieser Daten lassen sich einige, durch heuristische Überlegungen gesicherte, Vermutungen aufstellen, deren Beweis den Rahmen der Arbeit sprengen würde:

- Für k- Färbungen der Form $(a_1, a_2, ..., a_{k-1}, q+1-(a_1+...+a_{k-1})$ wobei $1 \leq a_1, ..., a_k < q+1$ mit $a_1 + ... + a_k = q+1$ ergibt das erste Monom im Zykelzeiger stets den Wert

$$\frac{1}{q(q-1)(q^2-1)}(q-1)\prod_{i=1}^{k-1}\binom{q+1-\sum_{j=1}^{k-1}a_j}{a_i}$$

- Für $a_1 = a_2 = a_3 = 1$ minimal, taucht spätestens im dritten Faktor das Produkt $(q+1)q(q-1)$ auf, sodass sich durch Herausziehen aus dem Produkt die Gruppenordnung wegkürzt und ein Polynom in q vom Grad $a_1 + ... + a_{k-1} - 3$ als allgemeiner Beitrag des ersten Monoms übrig bleibt.

- Das erste Monom dominiert bei der Auswertung des Zykelzeigers für k- Färbungen der obigen Gestalt über alle anderen Monome, sodass wir stets einen Wert:

$$\frac{q^{a_1+...+a_{k-1}-3}}{\prod_{j=1}^{k-1}a_j!} + \mathcal{O}(q^{a_1+...+a_{k-1}-4})$$

  für die Zahl der $\sum_{i=1}^{k-1} a_i =: l$-Punktkonfigurationen in $\mathbb{P}^1(\mathbb{F}_q)$ bzgl. k-Färbungen erhalten.

Neben der Verallgemeinerung bezüglich der Zahl der Färbungen, kann man das Problem natürlich auch auf höherdimensionale projektive Räume übertragen. Beispielsweise kann man die Frage nach der Zahl der l- Punktkonfigurationen im projektiven Raum $\mathbb{P}^2(\mathbb{F}_q)$ mit $|\mathbb{P}^2(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^3\setminus\{0\}|}{|\mathbb{F}_q\setminus\{0\}|} = \frac{q^3-1}{q-1} = q^2+q+1$ stellen, wobei wir hier fordern müssen, dass die „Punkte“ (also gerade die Ursprungsgeraden in $\mathbb{F}_q^3$) in allgemeiner Lage sind. Die Beantwortung einer solchen Fragestellung erfordert aber etwa die Einteilung der Gruppe $GL(3, \mathbb{F}_q)$ in Konjugationsklassen, was schon deutlich anspruchsvoller ist und den Umfang dieser Arbeit übersteigen würde.
Dieses Gebiet bietet also noch viele weitere interessante Forschungsmöglichkeiten.

10 Anhang

Anhang A: Historische Anmerkungen zur Originalarbeit von G. Pólya

Gegeben sind 6 Kugeln von drei verschiedenen Farben, 3 rote, 2 blaue, 1 gelbe; Kugeln gleicher Farbe sind als ununterscheidbar anzusehen. Auf wie viele Arten kann man diese 6 Kugeln auf die 6 Ecken eines frei im Raume beweglichen Oktaeders verteilen?
...Der springende Punkt der Aufgabe ist aber der, dass die Ecken weder individualisiert, noch vollständig ununterscheidbar sind, sondern dass solche und nur solche Positionen unter den erwähnten 60($\frac{6!}{3!2!1!} = 60$) *als nicht verschieden gelten, welche durch Drehungen des Oktaeders ineinander überführbar sind.*
([Pó37], Seite 146)
Durch solche und ähnliche Fragestellungen motiviert, veröffentlichte der ungarische Mathematiker George Pólya (1887-1985) im Jahr 1937 die Abhandlung „Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen“, was die Grundlage für das in dieser Arbeit angewandte Abzählverfahren bildet. Auf Pólya zurückzuführen ist die Idee, die Operation einer endlichen Gruppe auf einer endlichen Menge abstrakt in einem Polynom zu kodieren. *Wir zerlegen diese Permuation in Zyklen und wir ordnen jedem Zyklus von gegebener Ordnung eine Unbestimmte zu...*
Zu Beginn der Arbeit, in der sich Pólya zunächst mit der speziellen Problematik bezüglich obigen Oktaeders beschäftigt, führte er den Begriff des Zykelzeigers ein
...Man nehme das arithmetische Mittel der 24 Produkte, die den 24 Drehungen zugeordnet sind; das entstehende Polynom der Unbestimmten f_1, f_2, f_3, f_4,

$$\frac{f_1^6 + 6f_1^2f_4 + 3f_1^2f_2^2 + 6f_2^2 + 8f_3^2}{24}$$

nenn ich den Zykelzeiger der Permutationsgruppe, welche die Oktaedergruppe zwischen den 6 Oktaederecken veranlasst. ([Pó37], Seite 147)
Die Vorgehensweise von G. Pólya ist sehr anwendungsorientiert und stark durch das Abzählproblem aller stereoisomeren Alkane der Form C_nH_{2n+2} und der Frage nach der Anzahl von Isomerieklassen ähnlicher Kohlenwasserstoffverbindungen geprägt.
Im Verlaufe der Ausarbeitung nimmt Polya aber auch die notwendige abstrakte Formulierung und Begriffsfassung vor.
Einerseits müssen die „farbigen Kugeln“ von denen in Nr. 2 die Rede war, durch allgemeinere komplizierte Gebilde ersetzt werden, welche im Folgenden „Figuren“ heissen sollen; andererseits muss die in Nr. 2 betrachtete, durch die Oktaederdrehungen veranlasste spezielle Permutationsgruppe durch eine allgemeine Permutationsgruppe ersetzt werden.
([Pó37], Seite 147)
Der, dieser Bachelorarbeit zugrunde liegende, Hauptsatz ist aber aufgrund der veralteten Sprechweise (etwa „Figurenvorrat“ für die Zahl an Abbildungen $\mathcal{Y}^{\mathcal{X}}$) und ähnlicher nicht mehr gebräuchlicher Bezeichnungen, sowie der ausführlich begründeten Technik bei der Formulierung und Beweisführung nicht wörtlich übernommen, sondern stattdessen in moderner Neuformulierung in die Arbeit eingebunden. Für diejenigen Leser, die aber einen Eindruck von der Anwendung der Abzähltheorie Pólyas in der organischen Chemie haben wollen, ist die Lektüre der Originalarbeit sehr zu empfehlen.

Anhang B: Tabellen

Der Zyklenzeiger wurde für die Werte von q zwischen 2 und 25 mit Hilfe des Computeralgebrasystems *GAP* bestimmt. Hier eine Übersicht:

- $q = 2$

$$Z_{G,X} = \frac{1}{6}(X_1^3 + 3X_1X_2 + 2X_3)$$

- $q = 3$

$$Z_{G,X} = \frac{1}{48}(2X_1^4 + 12X_1^2X_2 + 16X_1X_3 + 6X_2^2 + 12X_4)$$

- $q = 4 = 2^2$

$$Z_{G,X} = \frac{1}{180}(3X_1^5 + 45X_1X_2^2 + 60X_1^2X_3 + 72X_5)$$

- $q = 5$

$$Z_{G,X} = \frac{1}{480}(4X_1^6 + 96X_1X_5 + 60X_1^2X_2^2 + 120X_1^2X_4 + 40X_2^3 + 80X_3^2 + 80X_6)$$

- $q = 7$

$$Z_{G,X} = \frac{1}{2016}(6X_1^8 + 288X_1X_7 + 168X_1^2X_2^3 + 336X_1^2X_3^2 + 336X_1^2X_6 + 126X_2^4 + 252X_4^2 + 504X_8)$$

- $q = 8 = 2^3$

$$Z_{G,X} = \frac{1}{3528}(7X_1^9 + 441X_1X_2^4 + 1512X_1^2X_7 + 392X_3^3 + 1176X_9)$$

- $q = 9 = 3^2$

$$Z_{G,X} = \frac{1}{5760}(8X_1^{10} + 640X_1X_3^3 + 360X_1^2X_2^4 + 720X_1^2X_4^2 + 1440X_1^2X_8 + 288X_2^5 + 1152X_5^2 + 1152X_{10})$$

- $q = 11$

$$Z_{G,X} = \frac{1}{13200}(10X_1^{12} + 1200X_1X_{11} + 660X_1^2X_2^5 + 2640X_1^2X_5^2 + 2640X_1^2X_{10} + 550X_2^6 + 1100X_3^4 + 1100X_4^3 + 1100X_6^2 + 2200X_{12})$$

- $q = 13$

$$Z_{G,X} = \frac{1}{26208}(12X_1^{14} + 2016X_1X_{13} + 1092X_1^2X_2^6 + 2184X_1^2X_3^4 + 2184X_1^2X_4^3 + 2184X_1^2X_6^2 + 4368X_1^2X_{12} + 936X_2^7 + 5616X_7^2 + 5616X_{14})$$

- $q = 16 = 2^4$

$$Z_{G,X} = \frac{1}{61200}(15X_1^{17} + 3825X_1X_4^4 + 4080X_1^2X_3^5 + 8160X_1^2X_5^3 + 16320X_1^2X_{15} + 28800X_{17})$$

- $q = 17$

$$Z_{G,X} = \frac{1}{78336}(16X_1^{18} + 4608X_1X_{17} + 2448X_1^2X_2^8 + 4896X_1^2X_4^4 + 9792X_1^2X_8^2 + 19584X_1^2X_{16} + 2176X_2^9 + 4352X_3^6 + 4352X_6^3 + 13056X_9^2 + 13056X_{18})$$

- $q = 19$

$$Z_{G,X} = \frac{1}{123120}(18X_1^{20} + 6480X_1X_{19} + 3420X_1^2X_2^9 + 6840X_1^2X_3^6 + 6840X_1^2X_6^3 + 20520X_1^2X_9^2 + 20520X_1^2X_{18} + 12312X_5^4 + 12312X_{10}^2 + 3078X_2^{10} + 6156X_4^5 + 24624X_{20})$$

Tabelle 1.
Gemäß Satz 4.2.5 erhalten wir die Gesamtzahl an k- Färbungen auf X durch Einsetzen von k in den Zykelzeiger für alle Monome $X_1, ..., X_{q+1}$. Dies ist im Nachfolgenden für die oben angegebenen Zykelzeiger mit $k \in \{2, 3, 4\}$ tabellarisch zusammengestellt.

$q\backslash k$	2	3	4
2	4	10	20
3	5	15	35
4	6	21	56
5	7	29	94
7	10	66	355
8	10	85	684
9	14	162	1844
11	20	575	13794
13	35	2637	126690
16	50	31854	4212064
17	113	81629	14076430
19	260	516579	160893868

Tabelle 2.
Mit *GAP* wurde eine Programm geschrieben, welches die Zahl der l- Punktkonfigurationen in $\mathbb{F}_q$ angibt. Hier ist eine tabellarische Übersicht in Körpern kleiner Charakteristik mit kleinen Werten von l angegeben. Für größere Werte von q und l werden die entsprechenden Zahlwerte zu groß und die Tabelle unübersichtlich.

	$n\backslash l$	3	4	5	6	7
$p=2, q=2^n$	2	1	1			
	3	1	1	1	1	1
	4	1	3	4	8	10
	5	1	5	11	53	148
	6	1	11	40	396	2741
	7	1	21	147	3045	47988
	8	1	43	568	23840	807850
	9	1	85	2227	188581	13271065
	10	1	171	8824	1500012	215211024
$p=3, q=3^n$	2	1	2	2	2	1
	3	1	5	8	34	73
	4	1	14	62	796	7283
	5	1	41	512	20428	653992
	6	1	122	4490	542534	54979894
	7	1	365	40040	14568190	4510156300
	8	1	1094	359270	392622160	4510156300
	9	1	3281	3230144	10594336696	29759512917493
$p=5, q=5^n$	1	1	1	1		
	2	1	5	8	28	54
	3	1	21	141	2847	43537
	4	1	105	3308	342358	29610794
	5	1	521	81641	42466997	18837678808
	6	1	2605	2035808	5300225608	11815730550723
	7	1	13021	50869141	662324695747	7390124670346308
	8	1	65105	1271598308	82785500431858	4619490064923691794
$p=7, q=7^n$	1	1	2	1	1	1
	2	1	25	185	849	54
	3	1	58	1009	57037	2638273
	4	1	401	48241	19272121	6555588515
	5	1	2802	2355361	6596189881	15818621060481
$p=11, q=11^n$	1	1	2	2	4	2
	2	1	21	133	2587	38112
	3	1	222	14874	3289730	616215791
	4	1	2441	1787545	4360715053	9108299521252
$p=13, q=13^n$	1	1	3	3	5	5
	2	1	29	253	6947	149427
	3	1	367	40407	14768759	4593347361
	4	1	4761	6800137	32365250149	131962416576921
$p=17, q=17^n$	1	1	3	4	10	10
	2	1	49	721	34229	1319922
	3	1	819	201556	164906674	115271081407
$p=19, q=19^n$	1	1	4	5	13	18
	2	1	61	1117	66439	3243592
	3	1	1144	392621	448569607	438255073095
$p=23, q=23^n$	1	1	4	6	22	36
	2	1	89	2377	207953	15136410
	3	1	2028	1234646	2502834906	4343141733529

Programmcode.

1.Hilfsfunktion
```
berechnep:= function(q)
local p;
for p in Primes do
if q mod p = 0 then
return p;
fi;
end;
```

2. Hilfsfunktion
```
summe:= function(q, l)
local sum;
sum:=0;
if (q+1) mod 2 = 0 and (l-2) mod 2 = 0 then
sum:= Binomial((q+1)/2, l/2)/(2*(q-1));
fi;
return sum;
end;
```

3. Hauptfunktion
```
zykel:= function(q, l)
local m1, m2, m3, m4, p, m, sum2, sum1, sum0, l2, l1, l0, d, sumd, ld, bin;
bin:= summe(q, l);
m1:=0;
m2:=0;
p:= berechnep(q);
if (l-1) mod p = 0 then
m2:= Binomial (q/p, l/p)/q;
fi;
l2:=[   ];
l1:=[   ];
l0:=[   ];
sum2:=0;
sum1:=0;
sum0:=0;
m3:=0;
for m in [3..(l-2)] do
if (q-1) mod m = 0 and (l-2) mod m = 0 then
Add(l2, m);
fi;
od;
for m in [3..(l-1)] do
```

```
if (q-1) mod m = 0 and (l-1) mod m = 0 then
Add(l1, m);
fi;
od;
for m in [3..l] do
if (q-1) mod m = 0 and l mod m = 0 then
Add(l0, m);
fi;
od;
for m in l2 do
sum2:= sum2 + (Phi(m)*Binomial((q-1)/m, (l-2)/m))/(2*(q-1));
od;
for m in l1 do
sum1:= sum1 + (Phi(m)*Binomial((q-1)/m, (l-1)/m))/(q-1);
od;
for m in l0 do
sum0:= sum0 + (Phi(m)*Binomial((q-1)/m, l/m))/(2*(q-1));
od;
m3:= sum2 + sum1 + sum0;
ld:=[   ];
sumd:= 0;
m4:= 0;
for d in [2..(q+1)] do
if (q+1) mod d = 0 and l mod d = 0 then
Add(ld, d);
fi;
od;
for d in ld do
sumd:= sumd + (Phi(d)*Binomial((q+1)/d, l/d))/(2*(q+1));
od;
m4:= sumd;
return m1 + m2 + m3 + m4 + bin;
end;

zykel(q, l);
```

Dies liefert nun den gewünschten Wert für die Zahl der l- Punktkonfigurationen über dem Körper $\mathbb{F}_q$.

Literatur

[BE08] Busam, Rolf und Thomas Epp: *Prüfungstrainer Lineare Algebra.* Spektrum, Berlin und Heidelberg, 2008.

[Bos01] Bosch, Siegfried: *Algebra.* Springer, Münster, 2001.

[dB77] Brujin, N.G. de: *Pólyas Abzähltheorie: Muster für Graphen und chemische Verbindungen.* Springer, Berlin und Heidelberg, 1977.

[Eri96] Erickson, Martin J.: *Introduction to Combinatorics.* Wiley-Interscience, New York, 1996.

[Fis01] Fischer, Gerd: *Analytische Geometrie.* vieweg, Düsseldorf, 2001.

[FS82] Fischer, Gerd und Reinhard Sacher: *Einführung in die Algebra.* Teubner, Regensburg, 1982.

[Lan79] Lang, Serge: *Algebraische Strukturen.* Vandenhocek Ruprecht, Göttingen, 1979.

[Pó37] Pólya, Georg: *Kombinatorische Anzahlbestimmung für Gruppen, Graphen und chemische Verbindungen.* Acta mathematica, Zürich, 1937.