Proportionen satter Elemente in klassischen Gruppen

von
David Dursthoff

Masterarbeit in Mathematik

vorgelegt der
Fakultät für Mathematik, Informatik und Naturwissenschaften
der Rheinisch-Westfälischen Technischen Hochschule Aachen

im September 2012

Gutachter

Prof. Dr. Gabriele Nebe
Prof. Dr. Alice Niemeyer

Erklärung

Hiermit versichere ich, diese Arbeit selbstständig verfasst zu haben. Außer den angegebenen Quellen und Hilfsmitteln habe ich keine weiteren verwendet.

Aachen, 19. September 2012 David Dursthoff

Zusammenfassung

Elemente der Generellen Linearen Gruppe über einem endlichen Körper, die keine Eigenwerte besitzen, kommen mit einer Proportion von circa e^{-1} vor. Bei hohem Grad ist die Abweichung fast ausschließlich von der Körperordnung abhängig.

Davon motiviert untersuchen wir Elemente, die keine invarianten Teilräume kleiner Dimension besitzen. Liegen alle Dimensionen über einer Schranke b, so sind Elemente mit dieser Eigenschaft etwa mit Wahrscheinlichkeit $e^{-1} \cdot e^{-1/2} \cdot .... \cdot e^{-1/b}$ zu finden. Wir geben für kleine Schranken und hohen Grad der Matrizen genauere Näherungen an.

Außerdem betrachten wir andere klassische Gruppen, namentlich die Symplektischen, Unitäten und Orthogonalen Gruppen, sowie den gesamten Matrixring und erhalten ähnliche Resultate für die Proportionen b-satter Matrizen in diesen Mengen.

Inhaltsverzeichnis

Kapitel 1

Einleitung

Endliche Gruppen können auf viele verschiedene Arten dargestellt werden, unter anderem als Permutationsgruppen, über Erzeuger und Relationen oder als Matrixgruppen. Die verschiedenen Möglichkeiten eignen sich verschieden gut in Computeralgebraprogrammen wie Magma[1], GAP[2] oder Maple[3]. So sind schon lange effektive Computeralgorithmen für Permutationsgruppen bekannt, solange die Anzahl der Punkte, auf denen die Permutationsgruppe operiert, nicht übermäßig groß ist. Matrixgruppen haben den Vorteil, dass der Grad, für den sie definiert sind, geringer ist und man außerdem weitere Strukturen wie den natürlichen Modul des Gruppenrings betrachten kann. Seit Anfang der 1990er Jahre wird intensiv nach guten Algorithmen zur Untersuchung von Matrixgruppen gesucht. [4]

Ein häufig auftretendes Problem ist das Suche und Finden von Elementen mit bestimmten Eigenschaften. Beispielsweise zur Berechnung der Komplexität des Algorithmus ist es daher hilfreich, die Proportion dieser Elemente zu kennen. Ein wichtiger Aspekt ist die Suche von invarianten Teilräumen oder die Suche nach Elementen einer Matrixgruppe, die keine nicht-trivialen invarianten Teilräume besitzen oder deren nicht-triviale Teilräume von hoher Dimension sind. Die Proportion der Matrizen mit letzterer Eigenschaft wollen wir ermitteln, in den Fällen einer klassischen algebraischen (Matrix-)Gruppe.

Wir betrachten klassische algebraische Gruppen über einem endlichen Körper K der Charakteristik q_0. Sei q eine Potenz von q_0.

In Abschnitt 2.1 konstruieren wir mehrere klassische algebraische Gruppen. Eine klassische algebraische Gruppe ist hier entweder die Generelle Lineare Gruppe, die Gruppe der Automorphismen eines Vektorraums ($GL(n,q)$), oder die Isometriegruppe eines geometrischen Raumes. Eine alternierende oder Hermitsche Bilinear- beziehungsweise Sesquilineraform bilden mit dem Vektorraum, auf dem sie definiert sind, einen Symplektischen beziehungsweise Unitären Raum. Die mit diesen Räumen als Invariantengruppe der Bilinear- beziehungsweise Sesquilinearformen definierten klassischen Gruppen sind die Symplekischen Gruppen ($Sp(2m,q)$) und die Unitären Gruppen ($U(n,q)$). Die Orthogonalen Gruppen ($O^\epsilon(2m,q)$ und $O(2m+1,q)$) werden als Invariantengruppen einer quadratischen Form definiert. Die quadratische Form bildet mit dem Vektorraum, auf dem sie definiert ist, einen orthogonalen Raum. Hierbei gibt $\epsilon \in \{+,-\}$ den Witt-Typ an.

$X(n,q)$ sei also eine klassische algebraische Gruppe, d.h.

$$X(n,q) \in \{GL(m,q), Sp(2m,q), U(m,q), O^\epsilon(2m,q), O(2m+1,q)\}.$$

[1] Computational Algebra Group, University of Sydney. Magma Computational Algebra System. (http://magma.maths.usyd.edu.au/magma/).

[2] The GAP Group. GAP - Groups, Algorithms, and Programming. (http://www.gap-system.org).

[3] Maplesoft. Maple.(http://www.maplesoft.com/products/maple/).

[4] Für weitere Informationen siehe man die Artikel von Eamonn O'Brien [9] und [10].

Der Körper, über dem die Gruppe definiert ist, sei mit K bezeichnet. K ist dann der endliche Körper $\mathbb{F}_q$ beziehungsweise $\mathbb{F}_{q^2}$ für die Unitären Gruppen $U(n,q) \leq GL(n,q^2)$. Weiterhin sei der natürliche Modul mit V bezeichnet und $n \in \mathbb{N}$ dessen Dimension, also n gleich m, $2m$ oder $2m+1$. In den beiden Fällen $X \in \{Sp, O^+\}$ ist m der Witt-Index. Der Witt-Index der Unitären Gruppe wird nicht beachtet und wir setzen $m := n$. Die Gruppe $O^-(2m,q)$ hat Witt-Index $m-1$. Weiterhin wollen wir den Matrixring $M(n,q) := \mathbb{F}_q^{n\times n}$ betrachten.[5]

Tabelle 1: Bezeichnungen

$X(n,q)$	$M(m,q)$	$GL(m,q)$	$Sp(2m,q)$	$U(n,q)$	$O^\epsilon(2m,q)$	$O(2m+1,q)$
K	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_{q^2}$	$\mathbb{F}_q$	$\mathbb{F}_q$
n	m	m	$2m$	m	$2m$	$2m+1$

Peter Neumann und Cheryl Praeger haben in [7] gezeigt, dass die Proportion der Matrizen ohne Eigenwerte in der Generellen Linearen Gruppe circa e^{-1} ist, beziehungsweise für steigenden Grad n dagegen konvergiert. Die Proportionen in den anderen klassischen Gruppen verhalten sich ähnlich. Die erste Spalte gibt die Struktur der behandelten Gruppe beziehungsweise des Rings an, die zweite den Grenzwert der Proportionen Eigenwert-freier Matrizen und die dritte eine Schranke der Konvergenzgeschwindigkeit (in n).

Tabelle 2: Proportionen Eigenwert-freier Elemente in klassischen Gruppen,[6] aus [7]

Gruppe	Limes der Proportionen	Konvergenzrate
$M(n,q)$	$e^{-1}(1-\frac{3}{2}q^{-1}+O(q^{-2}))$	$O(q^{-(n+1)(n+q)/(2(q-1))})$
$GL(n,q)$	$e^{-1}(1-\frac{1}{2}q^{-1}+O(q^{-2}))$	$O(q^{-(n+1)(n+q)/(2(q-1))})$
$Sp(2m,q)$, q ungerade	$e^{-1/2}(1-\frac{5}{4}q^{-1}+O(q^{-2}))$	$O(q^{-(m+1)^2/(q-1)})$
$Sp(2m,q)$, q gerade	$e^{-1/2}(1-\frac{3}{4}q^{-1}+O(q^{-2}))$	$O(q^{-(m+1)^2/(q-1)})$
$U(n,q)$	$e^{-3/2}(1+O(q^{-2}))$	$O(q^{-n(4n+q^2+3q+2)/(2(q^2+3q+2))})$
$O^\epsilon(2m,q)$, q ungerade	$\frac{1}{2}e^{-1/2}(1-\frac{5}{4}q^{-1}+O(q^{-2}))$	$O(q^{-m(m+(q-1)/2)/(q-1)})$
$O^\epsilon(2m,q)$, q gerade	$\frac{1}{2}e^{-1/2}(1-\frac{3}{4}q^{-1}+O(q^{-2}))$	$O(q^{-m(m+q/2)/(q-1)})$

In dieser Arbeit wollen wir diese Ergebnisse verallgemeinern. Das eigentliche Problem der Eigenwert-freien Matrizen lässt sich auf sogenannte Derangements zurückführen. Derangements sind die Neuordnung von n Zahlen, sodass keine an ihrem ursprünglichen Platz verbleibt. Also sind dies genau die Fixpunkt-freien Permutationen in der symmetrischen Gruppe auf n Punkten. Die Proportion der Derangements oder Fixpunkt-freien Permutationen in der symmetrischen Gruppe S_n ist

$$\sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx e^{-1}.$$

Für steigenden Grad n konvergiert die Reihe gegen e^{-1}, wobei die Konvergenz sehr schnell ist ($|\sum_{k=0}^{n} \frac{(-1)^k}{k!} - e^{-1}| < 1/(n+1)!$).[7]

Die Weylgruppe der Generellen Linearen Gruppe $GL(n,q)$ ist die Symmetrische Gruppe und die Eigenwerte eines Elementes werden durch den Anteil des Elementes in der Weylgruppe festgelegt. Es liegt also nahe, dass die Proportion der Eigenwert-freien Elemente der Proportion der Fixpunkt-freien Permutationen entspricht. Dies haben Peter Neumann und Cheryl Praeger in [7] bestätigt. Ähnliches gilt für andere klassische Gruppen.

[5] Für eine genauere Beschreibung der Begriffe Konstruktion der Gruppen verweisen wir auf Abschnitt 2.1.

[6] Die Orthogonalen Gruppen ungerader Dimension fehlen, eine Begründung liefert Bemerkung 1.3.

[7] Zur besseren Übersicht geben wir die Beweise am Ende des Kapitels an. Siehe Satz 1.5 (i).

Eine Erweiterung ist nun die Betrachtung von Permutationen, die nicht nur keinen Fixpunkt besitzen, sondern sogar ihre Potenzen bis zu einer Schranke b Fixpunkt-frei sind. Bahnen ihres Erzeugnisses sollen, äquivalenterweise, eine Länge größer als b haben, wenn b eine gewählte Schranke ist. Für den Spezialfall $b = 1$ sind die gesuchten Permutationen genau die Derangements. Die Proportionen der Permutationen, deren Quadrate und sie selbst keine Fixpunkte besitzen, ist circa

$$e^{-1} \cdot e^{-1/2}.^{8}$$

Allgemein gibt Osias Gruder 1952 in [5] für alle Schranken $b \in \mathbb{N}$ folgenden Konvergenz an:

$$\frac{|\{\pi \in S_n \mid \pi,\ \pi^2,\ ...,\ \pi^b \text{ Fixpunkt-frei }\}|}{|S_n|} \longrightarrow e^{-\sum_{k=1}^{b} \frac{1}{k}},\ n \to \infty.^{9}$$

Als Übertragung auf Matrizen suchen wir die Proportion der Elemente einer Klassischen Gruppe, die keinen von Null verschiedenen invarianten Teilraum der Dimension b oder kleiner besitzt. Dies sind genau die Elemente, die keine Eigenwerte besitzen, wenn sie über den Körpererweiterungen von K, jeweils vom Grad 1 bis b, betrachtet werden. Die Vermutung ist, wenn wir einen Zusammenhang mit der Symmetrischen Gruppe zugrunde legen, dass die Proportion für die Generellen Linearen Gruppen circa

$$e^{-\sum_{k=1}^{b} \frac{1}{k}}$$

beträgt.

Wir führen den Begriff der satten Matrizen und, dem beschriebenen Zusammenhang folgend, der satten Permutationen ein.

Definition 1.1 *Sei $b \in \mathbb{N}$.*

- *Sei $g \in X(n,q)$. g heißt* b-satt*, falls für jeden g-invarianten Teilraum $W \neq 0$ von K^n gilt* $\dim W > b$.
- *Sei $\pi \in X(n,q)$ eine Permutation. π heißt* b-satt*, falls $\pi, \pi^2, ..., \pi^b$ Fixpunkt-frei sind.*

Unser Ziel ist, die Proportion der b-satten Matrizen in $X(n,q)$ abzuschätzen.

Definition 1.2 *Sei $n \in \mathbb{N}$.*

- *$S^b(X(n,q))$ bezeichne die Menge der $b-$satten Matrizen in $X(n,q)$.*
- *$v^b(X(n,q)) := \frac{|S^b(X(n,q))|}{|X(n,q)|}$ bezeichne die Proportion der b-satten Matrizen in $X(n,q)$.*

Wir setzen $v^b(X(0,q)) := 1$ für $X \in \{M, GL, Sp, U, O^+\}$ und $v^b(O^-(0,q)) := 0$ (es gibt keine Gruppe vom Typ $O^-(2m,q)$).
Wir schreiben auch $S_n^b := S^b(X(n,q))$ und $v_n^b := v^b(X(n,q))$, falls die Struktur von $X(n,q)$ klar festgelegt ist.

Wir werden die klassischen Gruppen einzeln betrachten.

Bemerkung 1.3 • *Für den Matrixring $M(n,q)$ können wir die Proportion der b-satten Elemente sofort aus der Proportion b-satter Elemente der $GL(n,q)$ berechnen. Denn jede*

[8] Siehe Satz 1.5 (ii).
[9] Siehe auch Satz 1.5 (iii).

Matrix, die nicht invertierbar ist, hat den Eigenwert 0 und ist damit nicht 1-satt und damit allgemein nicht b-satt für alle b. Es folgt

$$v^b(M(n,q)) = \frac{|GL(n,q)|}{|M(n,q)|} v^b(GL(n,q)) = \prod_{i=1}^{n}(1-q^{-i}) v^b(GL(n,q)).$$

Die Ergebnisse für den Matrixring sind, aufbauend auf den Resultaten für die Generellen Linearen Gruppen in Kapitel 4 und in Anhang B angegeben.

- *Die Orthogonalen Gruppen ungeraden Grades sind für uns von weniger großem Interesse, denn alle Elemente dieser Gruppen haben Eigenwerte und sind somit nicht b-satt für alle $b \in \mathbb{N}$. Einen Beweis werden wir in Satz 2.39 liefern. Wir wollen die Orthogonalen Gruppen ungeraden Grades nicht weiter betrachten.*

Für eine konkrete Dimension können wir die Proportionen b-satter Matrizen leider nicht berechnen oder eine gute Näherung angeben. Genauer diskutieren wir dies im Kapitel über Quokka-Mengen (siehe Kapitel 8, Seite 8.1).

Wir können allerdings Aussagen über das Konvergenzverhalten der Proportionen bei steigender Dimension treffen, wie sie Peter Neumann und Cheryl Praeger für Eigenwert-freie Matrizen - also 1-satte Matrizen - bereits berechnet haben. Wir übernehmen Neumanns und Praegers Vorgehen.

Definition 1.4 *Es soll der Grenzwert*

$$v^b(X,\infty,q) := \lim_{n\to\infty} v^b(X(n,q))$$

berechnet werden $\left(v^b_\infty := v^b(X,\infty,q) \text{ falls } X \text{ klar gewählt}\right)$*. Dafür ist die erzeugende Funktion der* v^b_n*, die* b-satte Potenzreihe*, hilfreich:*

$$V^b(z) := V^b(X,q;z) := \sum_{m=0}^{\infty} v^b(X(n,q)) z^m,$$

wobei n in Abhängigkeit von m wie in Tabelle 1 definiert ist (n gleich m oder 2m).

Als Ergebnis erhalten wir folgende Proportionen. Die erste Spalte gibt wieder die Struktur und die zweite den Grenzwert der Proportionen b-satter Elemente, $v^b(X,\infty,q)$, an.

Tabelle 3: Proportionen b-satter Elemente

Struktur	Limes der Proportionen: $v^b(X,\infty,q)$
$M(n,q)$	$e^{-\sum_{k=1}^{b} 1/k}(1+O(q^{-1}))$
$GL(n,q)$	$e^{-\sum_{k=1}^{b} 1/k}(1+O(q^{-1}))$
$Sp(2m,q)$, q gerade	$e^{-\frac{1}{2}(\sum_{k=1}^{b} 1/k)}(1-\frac{3}{4}q^{-1}+O(q^{-2}))$
$Sp(2m,q)$, q ungerade	$e^{-\frac{1}{2}(\sum_{k=1}^{b} 1/k)}(1-\frac{5}{4}q^{-1}+O(q^{-2}))$
$U(n,q)$	$e^{-\frac{3}{2}\left(\sum_{1\le k\le b,\ k\ ung.} 1/k\right)-\frac{1}{2}\left(\sum_{1\le k\le b,\ k\ ger.} 1/k\right)}(1+O(q^{-1}))$
$O^\epsilon(2m,q)$, q gerade	$\frac{1}{2}e^{-\frac{1}{2}(\sum_{k=1}^{b} 1/k)}(1-\frac{3}{4}q^{-1}+O(q^{-2}))$
$O^\epsilon(2m,q)$, q ungerade	$\frac{1}{2}e^{-\frac{1}{2}(\sum_{k=1}^{b} 1/k)}(1-\frac{5}{4}q^{-1}+O(q^{-2}))$

Die Fehlerterme in q lassen sich auch genauer berechnen. Im Falle der Generellen Linearen Gruppen und der Unipotenten Gruppen lässt sich erkennen, dass der Grad in q mit steigender Schranke b verschwindet. Im Anhang A beziehungsweise D sind entsprechende Werte für $b \in \{1, ..., 24\}$ angegeben. Bei den Symplektischen und Orthogonalen Gruppen sowie dem vollen Matrixring tritt dieses Verschwinden nicht auf, die angegeben Fehler sind für alle $b \geq 2$ durch einen nicht verschwindenden Term vom Grad q^{-1} gegeben. Die Werte der Symplektischen und Orthogonalen Gruppen sind bis auf einen Vorfaktor $\frac{1}{2}$ identisch. Entsprechende Werte sind in den Anhängen B (Matrixring) und C (Symplektische und Orthogonale Gruppen) aufgelistet.

Für die Generellen Linearen Gruppen sind einige Näherungen der Proportionen b-satter Elemente gegeben durch folgende Tabelle.

Tabelle 4: Proportionen b-satter Elemente in den Generellen Linearen Gruppen

b	Limes der Proportionen: $v^b(GL, \infty, q)$	
1	e^{-1}	$(1 - \frac{1}{2}q^{-1} + \frac{7}{24}q^{-2} - \frac{25}{48}q^{-3} + \frac{4583}{5760}q^{-4} - \frac{13907}{11520}q^{-5} + O(q^{-6}))$
2	$e^{-1-1/2}$	$(1 - \frac{7}{12}q^{-2} + \frac{1}{3}q^{-3} + \frac{77}{1440}q^{-4} - \frac{59}{180}q^{-5} + \frac{26371}{362880}q^{-6} + O(q^{-7})))$
3	$e^{-1-1/2-1/3}$	$(1 - \frac{1}{4}q^{-2} - \frac{1}{6}q^{-3} - \frac{41}{480}q^{-4} + \frac{49}{120}q^{-5} - \frac{17009}{40320}q^{-6} + O(q^{-7}))$
4	$e^{-1-...-1/4}$	$(1 - \frac{1}{6}q^{-3} - \frac{59}{120}q^{-4} + \frac{11}{30}q^{-5} - \frac{37}{504}q^{-6} + \frac{1133}{5040}q^{-7} + O(q^{-8}))$
5	$e^{-1-...-1/5}$	$(1 - \frac{1}{6}q^{-3} - \frac{7}{24}q^{-4} + \frac{1}{15}q^{-5} - \frac{37}{504}q^{-6} + \frac{193}{1008}q^{-7} + O(q^{-8}))$
6	$e^{-1-...-1/6}$	$(1 - \frac{1}{8}q^{-4} - \frac{1}{10}q^{-5} - \frac{85}{252}q^{-6} + \frac{1}{7}q^{-7} - \frac{97}{1920}q^{-8} + O(q^{-9}))$
7	$e^{-1-...1/7}$	$(1 - \frac{1}{8}q^{-4} - \frac{1}{10}q^{-5} - \frac{7}{36}q^{-6} - \frac{1}{14}q^{-7} - \frac{97}{1920}q^{-8} + O(q^{-9}))$
8	$e^{-1-...-1/8}$	$(1 - \frac{1}{10}q^{-5} - \frac{7}{36}q^{-6} - \frac{1}{14}q^{-7} - \frac{59}{240}q^{-8} + O(q^{-9}))$
9	$e^{-1-...-1/9}$	$(1 - \frac{1}{10}q^{-5} - \frac{1}{12}q^{-6} - \frac{1}{14}q^{-7} - \frac{59}{240}q^{-8} + O(q^{-9}))$
10	$e^{-1-...-1/10}$	$(1 - \frac{1}{12}q^{-6} - \frac{1}{14}q^{-7} - \frac{7}{48}q^{-8} + O(q^{-9}))$
11	$e^{-1-...-1/11}$	$(1 - \frac{1}{12}q^{-6} - \frac{1}{14}q^{-7} - \frac{7}{48}q^{-8} + O(q^{-9}))$
12	$e^{-1-...-1/12}$	$(1 - \frac{1}{14}q^{-7} - \frac{1}{16}q^{-8} + O(q^{-9}))$

Im Falle des Matrixring können wir genauere Näherungen angeben. Wie Neumann und Praeger bereits in [7] bewiesen haben, gilt für die Proportionen 1-satter Matrizen:

$$v^1(M, \infty, q) = e^{-1} \cdot \left(1 - \frac{3}{2}q^{-1} + O\left(q^{-2}\right)\right).$$

Für $b \geq 2$ zeigen wir in Satz 4.1 für die Proportionen b-satter Matrizen:

$$v^b(M, \infty, q) = e^{-\sum_{k=1}^{b} \frac{1}{k}} \cdot \left(1 - q^{-1} + O\left(q^{-2}\right)\right).$$

Mit Hilfe von Quokkamengen können wir eine obere Schranke für die Proportionen b-satter Elemente der Generellen Linearen Gruppen angeben. Im Abschnitt 8.2 und speziell in Satz 8.15 zeigen wir

$$v^b(GL, \infty, q) \leq e^{-\sum_{k=1}^{b} \frac{1}{k}}.$$

Eine gute untere Schranke zu finden ist schwieriger, in Satz 3.17 können wir folgende Abschätzung angeben:

$$v^b(GL, \infty, q) \geq e^{-\sum_{k=1}^{b} 1/k} \cdot (1 - \frac{1}{2}q^{-1} + O(q^{-2})).$$

Wie bereits erwähnt, ist ein Element der $GL(n, q)$ genau dann b-satt, wenn alle Eigenwerte, die es über dem algebraischen Abschluss hat, nicht in Erweiterungskörpern von $\mathbb{F}_q$ von kleinem

Grad vorkommen - genauer Grad kleiner gleich b. Diese Eigenwerte über dem algebraischen Abschluss nennen wir verallgemeinerte Eigenwerte oder einfach Eigenwerte. Wenn sie als Eigenwerte von b-satten Matrizen vorkommen können, nennen wir sie auch b-sättigend und sonst entsprechend nicht-b-sättigend.[10]

Die Eigenwertverteilungen der Elemente bildet eine Äquivalenzklasse von $GL(n, q)$. Zwei Matrizen sind genau dann äquivalent[11], wenn sie die selben Eigenwerte unter Beachtung der Vielfachheiten besitzen.

Uns interessieren eigentlich nur Matrizen, deren Eigenwerte alle b-sättigend sind. Unter diesen ist aber die Verteilung der Eigenwerte irrelevant. Wir führen dafür eine gröbere Äquivalenzrelation ein. Zwei Matrizen heißen b-äquivalent[12], falls sie die selben nicht-b-sättigenden Eigenwerte mit jeweils selber Dimension der Haupträume besitzen.

Wir können Kardinalitäten der $b-$Äquivalenzklassen als Produkt der Proportion b-satter Matrizen und der Proportion unipotenter Matrizen[13], jeweils von kleinerem Grad, schreiben. Dies erreichen wir durch eine Betrachtung von b-Haupträumen, die analog zur b-Äquivalenz definiert werden, und der Operation der $GL(n, q)$ auf der Menge der Zerlegungen von V in direkte Summen von b-Haupträumen.

Summieren wir über die b-Äquivalenzklassen auf, erhalten wir eine Summe der Proportionen. Eine Summe über die Grade (n von 0 bis unendlich) liefert ein Produkt von b-satter Potenzreihe und der erzeugenden Funktion der Proportionen unipotenter Matrizen. Diese Funktion lässt sich als Inverse der Euler'schen Funktion $G(x; z) := \prod_{i=1}^{\infty}(1 - x^{-i}z)$[14] schreiben, wobei x dann eine Potenz der Körperordnung q ist.

Die anderen klassischen Gruppen lassen sich auf gleiche Weise behandeln. Die Bestimmung der möglichen Verteilungen der Eigenwerte, vor allem der nicht-b-sättigenden, ist schwieriger und der wesentliche Unterschied zu den Generellen Linearen Gruppen.

Die mögliche Verteilung der nicht-b-satten Eigenwerte ist auch für die Generellen Linearen Gruppen der entscheidende Schritt, um die Proportionen für beliebige Schranken $b \in \mathbb{N}$ zu berechnen. Für $b = 1$ sind alle nicht-b-sättigenden Eigenwerte bereits Elemente des Grundkörpers $\mathbb{F}_q$. Alle Elemente von $\mathbb{F}_q^*$ können als Eigenwerte vorkommen und zu allen Kombinationen findet man Matrizen, die diese Eigenwerte besitzen. Alle Kombinationen müssen und können beachtet werden. Für $b = 2$ ist dies nicht mehr der Fall. Der Galois-Konjugierte eines Eigenwertes ist ebenfalls ein Eigenwert und beide kommen mit der selben Vielfachheit vor. Diese beiden Elemente von $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$ müssen also gemeinsam betrachtet werden. Für größere b gilt Entsprechendes.

Das zugrunde liegende Vorgehen der Betrachtung von b-Haupträumen und der Berechnung der Proportionen über die unipotenten Potenzreihen und die Euler'sche Funktion sind dem Artikel [7] von Peter Neumann und Cheryl Praeger entnommen. Die Klassifikation klassischer Gruppen beruht auf dem Buch [13] von Donald Taylor.

Danksagung

Zuallererst danke ich Alice Niemeyer für die Hilfe bei noch so komplizierten Ungleichungen und allgemein für die gute Betreuung – über 14 000 Kilometer hinweg! Für ihre Hilfsbereitschaft und Unterstützung möchte ich ebenso Gabriele Nebe und allen Kollegen am Lehrstuhl D für Mathematik meinen Dank aussprechen. Außerdem möchte ich meinen Eltern danken.

[10] Siehe Abschnitt 2.2.

[11] Bez.: $\sim_\chi$, "chi-Äquivalenz'", siehe Definition 2.34.

[12] Bez.: $\sim_b$, siehe Definition 2.38.

[13] Eine Matrix g heißt unipotent, falls $g - I$ nilpotent ist, also falls g nur den Eigenwert 1 hat, siehe Definition 2.45 und Abschnitt 2.3.1.

[14] Eine holomorphe Funktion für alle $z \in \mathbb{C}$ und alle $|x| > 1$, siehe Abschnitt 2.3.2.

Der folgende Satz gibt die Beweise an, die wir uns bis zum Schluss aufgehoben haben.

Satz 1.5 *(Proportionen von Derangements und b-satten Permutationen)*
Die Proportion b-satter Permutationen in der S_n sei mit p_n^b bezeichnet. Wir setzen $p^b(n) = 0$ falls $n \leq b$ und $p_n := p_n^1$ als die Proportion der Derangements.

(i) Die Proportion der Derangements ist

$$p_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

und die Folge $(p_n)_{n\in\mathbb{N}}$ konvergiert gegen e^{-1}. Genauer gilt

$$|p_n - e^{-1}| < \frac{1}{(n+1)!}.$$

(ii) Die Proportionen 2-satter Permutationen p_n^2 konvergieren für $n \to \infty$ gegen $e^{-1} \cdot e^{-1/2}$.

(iii) Die Proportionen b-satter Permutationen p_n^b konvergieren für n gegen unendlich gegen

$$e^{-\sum_{k=1}^{b} \frac{1}{k}}.$$

Beweis: Zu (i): Wir berechnen p_n über eine Siebformel:

$$p_n = \frac{1}{n!}(n! - \tbinom{n}{1}(n-1)! + \tbinom{n}{2}(n-2)! - ... \pm 1) = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Dies ist genau die Partialsumme der Potenzreihenentwicklung von e^{-1}.

Zu (ii): Die Proportion der Permutationen, die in Zykelzerlegung mindestens l 2-Zykel und k Fixpunkte besitzen, sei mit $a_{(k,l)}$ bezeichnet. Es ist

$$\begin{aligned} a_{(k,l)} &= \frac{1}{n!}\tbinom{n}{k}\tbinom{n-k}{2}\tbinom{n-k-2}{2}...\tbinom{n-k-2(l-1)}{2}\frac{(n-k-2l)!}{l!} \\ &= \frac{1}{k!}\frac{1}{l!}2^{-l}. \end{aligned}$$

Damit liefert eine Siebformel

$$p_n^2 = \sum_{0\leq k,l\leq n,\ k+2l\leq n} (-1)^{k+l} a_{(k,l)}.$$

Für $n \to \infty$ konvergiert die Proportion gegen

$$\left(\sum_{k=0}^{\infty} \frac{(-1)^k}{k!}\right) \cdot \left(\sum_{l=1}^{\infty} \frac{(-1)^l}{l!} 2^{-l}\right) = e^{-1} \cdot e^{-\frac{1}{2}}.$$

Zu (iii): Eine Möglichkeit ist es, wie in (i) und (ii) vorzugehen. Alternativ wollen wir ein Resultat von Osias Gruder nutzen, siehe [5] Abschnitt 1. Gruder gibt, auf unser Problem angewendet, eine Möglichkeit an, die erzeugende Funktion der Proportionen aller Permutationen, die in disjunkter Zykelzerlegung ausschließlich Zykel von Länge b oder kleiner besitzen auszudrücken. Genauer sei f_n die Proportion dieser Permutationen in der S_n. Dann gilt nach [5]

$$e^{h(z)} = \sum_{n=0}^{\infty} f_n z^n$$

mit $h(z) := z + \frac{z^2}{2} + ... + \frac{z^b}{b}$.

Jedes Element der Symmetrischen Gruppe besteht aus Zykeln von Länge kleiner oder gleich b und aus längeren Zykeln. Damit gilt

$$1 = \sum_{l=0}^{n} f_l \cdot p_{n-l}^b.$$

Wir erhalten eine Gleichung für die erzeugenden Funktionen, indem wir beide Seiten mit z^n multiplizieren und über n summieren:

$$(1-z)^{-1} = \sum_{n=0}^{\infty} f_n z^n \cdot \sum_{n=0}^{\infty} p_n^b z^n.$$

Um den Grenzwert der p_n^b zu ermitteln, drücken wir die Inverse der erzeugenden Funktion hier f_n als Potenzreihe aus:

$$e^{-h(z)} = \sum_{n=0}^{\infty} f_n^- z^n$$

mit $f_n^- \in \mathbb{R}$. Damit gilt für die Potenzreihen

$$\sum_{n=0}^{\infty} p_n^b z^n = (1-z)^{-1} \sum_{n=0}^{\infty} f_n^- z^n = \sum_{n=0}^{\infty} \sum_{l=0}^{n} f_l^- z^n.$$

Wir erhalten mit einem Koeffizientenvergleich

$$p_n^b = \sum_{l=0}^{n} f_l^- \longrightarrow \sum_{l=0}^{\infty} f_l^-, \; n \to \infty,$$

der Grenzwert ist aber gerade $e^{-h(1)} = e^{-\sum_{k=1}^{b} 1/k}$.

□

Kapitel 2

Klassische Gruppen

In diesem Kapitel wollen wir Vorbereitungen für unsere Betrachtungen von klassischen Gruppen treffen. Wir definieren benötigte Begriffe und erwähnen einige hilfreiche Sätze.

Zunächst konstruieren wir die klassischen Gruppen, die wir in Tabelle 1 angegeben haben. Die Klassifikation klassischer Gruppen im folgenden Abschnitt beruht auf Donald Taylor [13].

2.1 Klassifikation

In diesem Abschnitt sei V ein endlichdimensionaler Vektorraum über einem endlichen Körper K. Die Dimension von V sei $n \in \mathbb{N}$. Wir betrachten Abbildungen des Vektorraums auf sich selbst, die die Vektorraum-Struktur erhalten.

Definition 2.1

- *Eine Abbildung $f : V \to V$ heißt* semilinear*, falls ein Körperautomorphismus $\sigma \in Aut(K)$ existiert, sodass $f(av + w) = \sigma(a)f(v) + f(w)$ für alle $a \in K$, $v, w \in V$ gilt. f heißt dann auch σ-*linear*.*
- $\Gamma L(V) := \{f : V \to V \mid f \text{ semilinear } \}$ *ist die* semilineare Gruppe*.*
- *Die* Generelle Lineare Gruppe $GL(V) := \{f \in \Gamma L \mid f \ 1-linear \ \}$ *ist ein Normalteiler von ΓL.*
- *Die* Spezielle Lineare Gruppe $SL(V)$ *ist die Kommutatorgruppe von $GL(V)$ und der Kern der Determinantenabbildung* $\det : GL(V) \to K^*$*.*
- *V ist isomorph zu K^n. Indem wir eine Basis von V fixieren, können wir ein $g \in \Gamma L(V)$ als $(n \times n)-$*Abbildungsmatrix *über K auffassen und damit ist $\Gamma L(V) \cong \Gamma L(K^n)$. Für $K = \mathbb{F}_q$ setzen wir*

$$\Gamma L(n, q) := \Gamma L(n, K) := \Gamma L(K^n), \ GL(n, q) := GL(n, K) := GL(K^n), ...$$

- *Wir betrachten auch den* Matrixring $M(V) := End_K(V)$*, $M(n, q) := K^{n\times n}$.*

Bekanntermaßen ist $GL(V)$ die Einheitengruppe von $M(V)$, worauf wir in späteren Kapiteln zurückkommen wollen.

Wir wollen im weiteren $V = K^n$ und damit $GL(V) = GL(n, q)$ annehmen.

Bemerkung 2.2 *$GL(n, q)$ operiert regulär auf den (geordneten) Basen von V. Deren Anzahl ist dann die Ordnung der $GL(n, q)$:*

$$|GL(n, q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1).$$

Zusätzlich gibt es im wesentlichen drei weitere Klassen von klassischen Gruppen, die Symplektischen, die Unitären und die Orthogonalen Gruppen. Diese wollen wir jetzt über ihre Sesquilinearformen (siehe nächste Definition) und Quadratische Formen (siehe Definition 2.6) konstruieren.

Definition 2.3

- *Der* Dualraum *von V ist der Vektorraum der Linearformen von V, d.h.*

$$V^* := \{\varphi : V \to K | \varphi \text{ linear}\}.$$

- *Eine Abbildung $\beta : V \times V \to K$ ist eine Sesquilinearform, falls ein Körperautomorphimus $\sigma \in Aut(K)$ existiert, sodass für alle $u, v, w \in V$ und $a \in K$ gilt:*

$$\beta(au + w, v) = a\beta(u, v) + \beta(w, v)$$

und

$$\beta(u, av + w) = \sigma(a)\beta(u, v) + \beta(u, w).$$

*β heißt dann auch $\sigma-$*sesquilinear*.*

- *Eine Sesquilinearform β heißt* nicht-ausgeartet*, falls $\beta(v, u) = 0$ für alle $u \in V$ impliziert, dass $v = 0$ gilt.*

- *Eine Sesquilinearform β heißt* relexiv*, falls $\beta(v, u) = 0$ äquivalent zu $\beta(u, v) = 0$ ist.*

- *Ein Vektorpaar $(u, v) \in V^2$ heißt* orthogonal*, falls $\beta(u, v) = 0$.*

- *Für einen Untervektorraum $W \leq V$ definieren wir das* orthogonale Komplement

$$W^\perp := \{u \in V \mid \beta(u, v) = 0 \ \forall \ v \in W\}.$$

Ist $\sigma = 1 = id_k$, so sind die $\sigma-$Sesquilinearformen gerade Bilinearformen.

Wir können die Orthogonalitätsrelation auf den Paaren von Vektoren definieren. Dann ist β genau dann reflexiv, wenn die Relation symmetrisch ist. Dies ist, falls β nicht-ausgeartetet ist, äquivalent dazu, dass $(W^\perp)^\perp = W$ für alle $W \leq V$ gilt.

Satz 2.4 *(Birkhoff, von Neumann) V sei ein endlich-dimensinaler $K-$Vektorraum der Dimension $n \geq 3$. β sei eine reflexive, nicht-ausgeartete σ-Sesquilinearform, $\sigma \in Aut(K)$.*

Dann gilt einer von drei Fällen:

(i) (Alternierend) $\sigma = 1$ und $\beta(v, v) = 0$ für alle $v \in V$.

(ii) (Symmetrisch) $\sigma = 1$ und $\beta(u, v) = \beta(v, u)$ für alle $u, v \in V$.

(iii) (Hermitsch) $\sigma^2 = 1$ und $\beta(u, v) = \sigma(\beta(v, u))$ für alle $u, v \in V$.

Beweis: Siehe [13], Theorem 7.1 (S. 53).

Definition 2.5 *Ist β eine* alternierende Bilinearform *oder* Hermitsche Sesquilinearform *(d.h. β ist vom Typ (i) bzw. (ii)), so heißt (V, β)* Symplektischer *bzw.* Unitärer Raum*.*

Ist eine Bilinearform β symetrisch, so werden wir den zugehörige Raum als Orthogonalen Raum bezeichnen. Allerdings ist eine Definition dieses Raumes über β für Körper der Charakteristik 2, d.h. Primkörper $\mathbb{F}_{q_0} = \mathbb{F}_2$, ungünstig für die Betrachtung der Orthogonalen Gruppen. Wir definieren Orthogonale Räume über quadratische Formen.

Definition 2.6
- *Eine Abbildung $Q : V \to K$ heißt* quadratische Form*, falls $Q(av) = a^2Q(v)$ für alle $v \in V, a \in K$ gilt und*

$$\beta : V \times V \to K, (u, v) \mapsto Q(u + v) - Q(u) - Q(v)$$

  eine Bilinearform ist. β heißt Polarform *zu Q.*

- *Eine Quadratische Form Q heißt* nicht-ausgeartet*, falls für $u \in V$ mit $Q(u) = 0$ und $\beta(u, v) = 0$ für alle $v \in V$ bereits $u = 0$ folgt.*

- *(V, Q) heißt* Orthogonaler Raum*.*

Ist die Charakteristik von K ungerade, so ist die Polarform β eine symmetrische Bilinearform und Q ist durch β festgelegt. Die orthogonalen Räume über Körpern ungerader Charakteristik sind somit wie die symplektischen über eine Bilinearform definiert.

Ist die Charakteristik aber 2, so ist β alternierend. Q ist aus β im Allgemeinen nicht rekonstruierbar. Die orthogonalen Gruppen über Körpern gerader Charakteristik müssen also (zunächst) gesondert betrachtet werden.

Wir wollen Untergruppen der Generellen Linearen Gruppe klassifizieren, deren Elemente mit einer Sesquilinearform verträglich sind. Diese, Isometrien genannt, werden dann die gesuchten Gruppen bilden.

Definition 2.7 *Seien β_1, β_2 reflexive σ_1- bzw. σ_2-Sesquilinearformen auf $K-$Vektoräumen V_1 bzw. V_2. Eine $\sigma-$lineare Abbildung $g : V_1 \to V_2$ heißt* Isometrie*, falls $\sigma_2\sigma = \sigma\sigma_1$ und*

$$\beta_2(g(u), g(v)) = \sigma(\beta_1(u, v))$$

für alle $u, v \in V_1$ gilt.

Ist g linear, also $\sigma = 1$, so heißt g lineare Isometrie*.*

Bemerkung 2.8 *Ist β eine Sesquilinearform auf V, so ist*

$$\{g \in GL(V) |\ g \text{ ist lineare Isometrie bezüglich } (V, \beta)\}$$

$$= \{g \in GL(V) |\ \beta(g(u), g(v)) = \beta(u, v)\ \forall\ u, v \in V\}$$

eine Gruppe, die Invariantengruppe von β. Dies werden für die entsprechenden Typen von Sesquilinearformen die Symplektischen, Unitären und, für ungerade Charakteristik, die Orthogonalen Gruppen sein. Dies sind die weiteren klassischen Gruppen, die wir betrachten wollen.

Bevor wir die Gruppen einzeln betrachten, wollen wir noch einige Begriffe einführen und den bekannten Satz von Witt erwähnen.

Definition 2.9 *Sein V ein K-Vektorraum, β eine Sesquilinearform und Q eine quadratische Form auf V*

- *Das* Radikal *von β ist der Untervektorraum $\text{rad } V := V^\perp = \{v \in V |\ \beta(v, u)\ \forall\ u \in V\}$.*

- *Ein Vektor $v \in V$, $v \neq 0$, heißt* isotrop*, falls $\beta(v, v) = 0$.*

- *Ein Untervektorraum $W \leq V$ heißt* total isotrop*, falls $W^\perp \subseteq W$.*

- *Eine Vektor $v \in V$, $v \neq 0$, heißt* singulär*, falls $Q(v) = 0$.*

- *Ein Untervektorraum $W \leq V$ heißt* total singulär*, falls alle $v \in W$ singulär sind.*

- *Ein Untervektorraum $W \leq V$ heißt* degeneriert*, falls $W \cap W^\perp \neq \emptyset$.*

- *Falls* $V = U \oplus W$ *und* $U \subseteq W^{\perp}$, *so schreiben wir* $V = U \perp W$ *und bezeichnen dies als* orthogonale direkte Summe.
- *Eine* (orthogonale) Zerlegung *von* V *ist eine orthogonale direkte Summe von Untervektorräumen* $U_1, ..., U_s$ *mit*
$$V = U_1 \perp U_2 \perp ... \perp U_s$$
($\perp$ *ist assoziativ).*
- *Ein Paar* $(u, v) \in V^2$ *heißt* hyperbolisches Paar, *falls* u *und* v *isotrope Vektoren sind und* $\beta(u, v) = 1$ *gilt. Im Falle eines Orthogonalen Raumes* (V, Q) *seien* u *und* v *außerdem singuläre Vektoren. Das Erzeugnis* $\langle u, v\rangle \leq V$ *heißt* hyperbolische Gerade *(als Element des Projektiven Raums aufgefasst).*

Satz 2.10 *(Witt) Sei* V *ein* K*-Vektorraum und* β *eine nicht-ausgeartete Sesquilinearform auf* V. *Sein* $W \leq V$ *und* $f : W \to V$ *eine lineare Isomentrie bzgl.* β.

Dann existiert eine lineare Isometrie $g : V \to V$ *mit* $g_{|W} = f$ *genau dann, wenn* $f(rad\ V \cap W) = rad\ V \cap f(W)$ *gilt.*

Beweis: Siehe [13], Theorem 7.4 (S.57).

Folgerung 2.11 *Alle maximalen, total isotropen Untervektorräume haben die gleiche Dimension.*

Bekanntermaßen gilt für Untervektorräume W die Dimensionsformel

$$\dim W + \dim W^{\perp} = \dim V = n.$$

Somit haben isotrope Untervektorräume höchstens Dimension $\frac{n}{2}$.

Definition 2.12 *Sei* $W \leq V$ *ein maximaler, total isotroper Untervektorraum von* V *bzgl.* β. *Dann heißt* $m := \dim W \leq \frac{n}{2}$ *der Witt-Index von* (V, β).

Ist Q *eine quadratische Form, so bezeichnet der Witt-Index von* (V, Q) *die Dimension des (eindeutigen) maximalen, total singulären Untervektorraums.*

2.1.1 Symplektische Gruppen

Betrachten wir zunächst den ersten Fall in Birkhoffs und von Neumanns Satz (s. 2.4). Also seien im Folgenden V ein $\mathbb{F}_q-$Vektorraum der Dimension $n \geq 2$ und β eine nicht-ausgeartete alternierende Bilinearform auf V.

Definition 2.13
- (V, β) *heißt* Symplektischer Raum.
- *Wir definieren* $f : V \to V^*,\ v \mapsto \beta(-, v)$ *und damit die* Symplektische Gruppe *als*
$$Sp(V) := \{g \in GL(V) |\ gf = fg\}.$$

Wir fassen einige hilfreiche Eigenschaften zusammen.

Bemerkung 2.14 *(i)* $\beta(u, v) = -\beta(v, u)\ \forall\ u, v \in V$.

(ii) Für $g \in GL(V)$ *gilt:*
$$g \in Sp(V) \Leftrightarrow \beta(g(u), g(v)) = \beta(u, v)\ \forall\ u, v \in V.$$

(iii) *Sei $B = (b_1, ..., b_n)$ eine Basis von V und Φ die zugehörige Gram-Matrix, d.h. $\Phi := (\beta(b_i, b_j))_{i,j=1,...,n}$. Ein Element $g \in GL(n, q)$ sei als Abbildungsmatrix bezüglich der Basis B aufgefasst. Dann liegt g genau dann in $Sp(V)$, wenn*

$$g^{tr}\Phi g \;=\; \Phi$$

gilt.

(iv) *Die letzte Eigenschaft liefert eine Isomorphie von $Sp(V)$ und $Sp(K^n) \leq GL(n, q)$.*

Im Folgenden sei V mit K^n identifiziert.

Definition 2.15 *$Sp(n, q) := Sp(n, K) := Sp(K^n)$ (wie in Definition 2.1).*

Wir wollen die Ordnungen der Symplektischen Gruppen bestimmen. Dazu wollen wir wieder Basen zählen, wie wir bereits zur Bestimmung der Ordnung der $GL(n, q)$ vorgegangen sind. Wir schränkten uns auf gewisse Basen ein.

Sei $(u, v) \in V^2$ ein hyperbolisches Paar, d.h es gelte $\beta(u, v) = 1$. Da β alternierende Bilinearform ist, gilt damit $\beta(u, u) = \beta(v, v) = 0$ und $\beta(v, u) = -1$. So ein Paar existiert immer, da β nicht-ausgeartet ist. Haben wir so ein Paar gefunden, können wir eine Basis konstruieren, die das Paar enthält und ansonsten nur orthogonale Vektoren zu u und v. Dieses Vorgehen kann fortgesetzt werden.

Lemma 2.16 *Sei $(u, v) \in V^2$ ein hyperbolisches Paar. Dann gilt*

$$V = \langle u, v\rangle \perp \langle u, v\rangle^{\perp}.$$

Setzen wir dieses Vorgehen fort und suchen ein hyperbolisches Paar in $\langle u, v\rangle^{\perp}$ usw., so können wir eine Basis konstruieren.

Insgesamt existiert eine Basis $(e_1, f_1, ..., e_m, f_m)$ mit $(e_1, f_1), ..., (e_m, f_m)$ hyperbolischen Paaren. $m = \frac{n}{2}$ ist der Witt-Index von (V, β) und insbesondere ist n gerade. Weiterhin stehen die Paare orthogonal zueinander, d.h. die Gram-Matrix ist

$$\Phi = Diag\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \dots\ , \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right).$$

Beweis: Wegen $\beta(u, v) \neq 0 \neq \beta(v, u)$ gilt $\langle u, v\rangle \cap \langle u, v\rangle^{\perp} = \emptyset$. Aus Dimensionsgründen folgt eine orthogonale Summe

$$V = \langle u, v\rangle \perp \langle u, v\rangle^{\perp}.$$

β ist nicht-ausgeartet und somit ist insbesondere $\dim\langle u, v\rangle^{\perp} \geq 2$ (oder $\dim V = 2$ und wir sind fertig). Ein hyperbolisches Paar in $\langle u, v\rangle^{\perp}$ existiert damit und wir können unser Vorgehen fortsetzen. Wir erhalten eine Basis aus hyperbolischen Paaren. Die Paare sind paarweise orthogonal zueinander. Insbesondere ist $\dim V = n$ gerade.

Sei nun $(e_1, f_1, ..., e_m, f_m)$ so eine Basis von hyperbolischen Paaren. Die Grammatrix hat dann die angegebene Form und $\langle e_1, e_2, ..., e_m\rangle$ ist ein total isotroper Teilraum. Dieser ist offensischtlich maximal, also ist m der Witt-Index von (V, β). □

Die Basen mit dieser Eigenschaft heißen auch symplektische Basen. Die Symplektische Gruppe operiert regulär auf den geordneten symplektischen Basen. Die Ordnung der Gruppe ist also gleich der Anzahl der symplektischen Basen.

Satz 2.17 *Es gilt*

$$|Sp(2m, q)| = q^{m^2} \prod_{i=1}^{m} (q^{2i-1} - 1).$$

Beweis: Seien (u, v) und (u, v') hyperbolische Paare. Mit dem letzten Lemma gilt $\beta(u, v') = \beta(u, v) = 1$. Alle $v + w \in V$ mit $w \in \langle v \rangle^{\perp}$ bilden mit u andererseits symplektische Paare. Eine Normierung liefert die Anzahl der symplektischen Paare:

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

Die Anzahl der symplektischen Basen und damit die Ordnung der Symplektischen Gruppe ist dann wegen der orthogonalen direkten Summe im letzten Lemma gleich

$$\prod_{i=1}^{m}(q^{2i} - 1)q^{2i-1} \;=\; q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1).$$

□

2.1.2 Unitäre Gruppen

Als nächstes betrachten wir den Fall, dass V ein $\mathbb{F}_{q^2}-$Vektorraum der Dimension $n \geq 1$ und β eine nicht-ausgeartete $\sigma-$Sesquilinearform auf V ist mit $\sigma^2 = id$. Für $u, v \in V$ gilt außerdem $\beta(u, v) = \sigma(\beta(v, u))$.

Definition 2.18

- (V, β) *heißt* Unitärer Raum.
- *Wir definieren die* Unitäre Gruppe *als*

$$U(V) := \{g \in GL(V) |\ \beta(g(u), g(v)) = \beta(u, v)\ \forall\ u, v \in V\}.$$

Bemerkung 2.19 *Einige hilfreichen Eigenschaften sind*

(i) $\det(g)\sigma(\det(g)) = 1$ *für alle* $g \in U(V)$,

(ii) $\det(U(V)) = \{\lambda \in \mathbb{F}_{q^2} \mid \lambda\sigma(\lambda) = 1\}$.

(iii) Sei $B = (b_1, ..., b_n)$ *eine Basis von* V *und* Φ *die zugehörige Gram-Matrix, d.h.* $\Phi := (\beta(b_i, b_j))_{i,j=1,...,n}$. *Ein Element* $g \in GL(n, q)$ *sei als Matrix bezüglich der Basis* B *aufgefasst. Dann liegt* g *genau dann in* $U(V)$, *wenn*

$$g^{tr}\Phi(\sigma g) \;=\; \Phi$$

gilt.

Das Bild der Determinantenabbildung ist genau der maximale Teilkörper $\mathbb{F}_q$ von $\mathbb{F}_{q^2}$. Der Körperautomorphismus σ ist der Frobeniusautomorphismus:

$$(\bar{}) := \sigma :\ \mathbb{F}_{q^2} \to \mathbb{F}_{q^2},\ \lambda \mapsto\ \overline{\lambda} := \sigma(\lambda) = \lambda^q.$$

Damit ist die Unitäre Gruppe $U(V)$ auch eindeutig, unabhängig von σ, gegeben. Wir können uns auf die Betrachtung von $V = K^n$ beschränken.

Definition 2.20 $U(n, q) := U(n, K) := U(K^n)$.

Das nächste Lemma zeigt, dass wir wieder Basen aus paarweise orthogonalen hyperbolischen Paaren finden werden (wenn die Dimension gerade ist). Bezeichnen wir Basen mit dieser Eigenschaft als unitäre Basen, so operiert $U(V)$ auf diesen Basen regulär. Wir werden die Ordnung der Unitären Gruppe bestimmen, indem wir die unitären Basen zählen.

Lemma 2.21 *(i) Ist $n = dimV \geq 2$, so enthält V ein hyperbolisches Paar.*

(ii) Sei $(u, v) \in V^2$ so ein Paar. Dann gilt

$$V = \langle u, v\rangle \perp \langle u, v\rangle^{\perp}.$$

(iii) Ist n gerade, so existiert eine Basis $(e_1, f_1, ..., e_l, f_l)$ von V mit $(e_1, f_1), ..., (e_l, f_l)$ hyperbolischen Paare, die paarweise orthogonal zueinander sind. $l = \frac{n}{2}$ ist der Witt-Index von (V, β).

(iv) Ist n ungerade, so existiert eine Basis $(e_1, f_1, ..., e_l, f_l, w)$ von V mit $(e_1, f_1), ..., (e_l, f_l)$ hyperbolischen Paare, die paarweise orthogonal zueinander sind. w ist orthogonal zu allen Paaren und kann so gewählt werden, dass $\beta(w, w) = 1$ gilt. Der Witt-Index von (V, β) ist dann $l = \frac{n-1}{2}$.

Beweis: β ist nicht alternierend, also existiert ein $\tilde{v} \in V$ mit $\lambda := \beta(\tilde{v}, \tilde{v}) \neq 0$. Dann gilt $\overline{\lambda} = \lambda$. Sei $\tilde{u} \in V$ orthogonal zu $\tilde{v}$ und $a \in \mathbb{F}_{q^2}$ so gewählt, dass $a\overline{a} = \frac{-\beta(\tilde{u},\tilde{u})}{\lambda}$ gilt (dies geht immer, da $\frac{-\beta(\tilde{u},\tilde{u})}{\lambda} \in \mathbb{F}_q$ und $x \mapsto x\overline{x}$ gerade die Normabbildung der Körpererweiterung $\mathbb{F}_{q^2}/\mathbb{F}_q$ ist). Damit gilt

$$\beta(a\tilde{v} + \tilde{u}, a\tilde{v} + \tilde{u}) = \beta(a\tilde{v}, a\tilde{v}) + \beta(\tilde{u}, \tilde{u}) = a\overline{a}\lambda + \beta(\tilde{u}, \tilde{u}) = 0$$

und somit ist $v := a\tilde{v} + \tilde{u}$ ein isotroper Vektor. Da β nicht-ausgeartet ist, finden wir einen Vektor u, für den $\beta(v, u) = 1$ gilt. Ohne Einschränkung ist u isotrop (sonst verfahre man wie oben). (u, v) ist somit ein hyperbolisches Paar. Damit haben wir (i) gezeigt. (ii) folgt sofort aus Dimensionsgründen.

Setzen wir das Vorgehen fort, so erhalten wir maximal $2l$ linear unabhängige Vektoren, bestehend aus l hyperbolischen Paaren, die alle paarweise orthogonal zueinander sind. Mit (i) ist $l = \frac{n}{2}$, falls n gerade ist, und $l = \frac{n-1}{2}$, falls n ungerade ist. Seien $(e_1, f_1), ..., (e_l, f_l)$ diese Paare. Ist n gerade, so bilden $e_1, f_1, ..., e_l, f_l$ eine Basis und (iii) ist offensichtlich. Ist n ungerade, so ist $\langle e_1, f_1, ..., e_l, f_l\rangle^{\perp}$ ein eindimensionaler Teilraum. Sei $w \neq 0$ ein Element dieses Raums. Dann ist $(e_1, f_1, ..., e_l, f_l, w)$ eine Basis von v. Wir müssen noch zeigen, dass w nicht isotrop ist. Dies ist aber sofort ersichtlich, denn β ist nicht-ausgeartet und w ist orthogonal zu allen anderen Basiselementen.

□

Eine Basis der Form $(e_1, f_1, ..., e_l, f_l)$ wie in (iii) im letzten Lemma oder $(e_1, f_1, ..., e_l, f_l, w)$ wie in (iv) bezeichnen wir als unitäre Basis. Auf den unitären Basen operiert die Unitäre Gruppe regulär und wir haben somit einen Ansatz, um die Ordnung der Gruppe zu bestimmen.

Satz 2.22 *Es gilt*

$$|U(n, q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{m} (q^i - (-1)^i).$$

Beweis: Wir wollen die Anzahl der unitären Basen bestimmen. Dafür gehen wir in mehreren Schritten vor.

1. Schritt: Sei (u, v) ein hyperbolisches Paar. Dann enthält $\langle u, v\rangle$ genau $(q^2-1)(q+1)$ isotrope Vektoren.
Denn die Vektoren $a \cdot u$ für $a \in \mathbb{F}_{q^2}^*$ sind sicher isotrop. Ein Element $u + bv$ ist genau dann isotrop, wenn gilt $\beta(u + bv, u + bv) = 0$. Mit

$$\beta(u + bv, u + bv) = \overline{b}\beta(v, u) + b\beta(u, v) = \overline{b} + b$$

gilt dies genau dann, wenn b im Kern der Spurabbildung

$$Spur : \mathbb{F}_{q^2} \to \mathbb{F}_q,\ \lambda \mapsto \lambda + \overline{\lambda}$$

ist. Die Spur ist surjektiv, also gibt es $\frac{q^2}{q} = q$ mögliche b. Somit sind $(q^2-1)+(q^2-1)q = (q^2-1)(q+1)$ isotrope Vektoren in $\langle u, v\rangle$ enthalten.

2. Schritt: V enthält $(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)$ isotrope Vektoren.
Denn sei ι_n die Anzahl der isotropen Vektoren in $V = K^n$. Es ist $\iota_1 = 0$, denn β ist nichtausgeartet und $\iota_2 = (q^2-1)(q+1)$ nach Schritt 1.

Sei nun $n > 2$ und (u, v) ein hyperbolisches Paar. Wir zählen zunächst die isotropen Vektoren in $\langle u\rangle^\perp$. Sei $w \in V$ orthogonal zu u. Dann ist $w = au + w'$ mit $a \in \mathbb{F}_{q^2}$ und $w' \in \langle u, v\rangle^\perp$ eindeutig schreibbar. w ist genau dann isotrop, wenn w' isotrop und a beliebig oder $w' = 0$ und $a \neq 0$ sind. Es gibt also $(q^2-1)+q^2\iota_{n-2}$ isotrope Vektoren in $\langle u\rangle^\perp$. Sei nun $w \in V\backslash\langle u\rangle^\perp$. Dann ist w eindeutig schreibbar als $w = au + bv + w'$ mit $a, b \in \mathbb{F}_{q^2}$ und $w' \in \langle u, v\rangle^\perp$. Es muss $b \neq 0$ gelten. Es gibt q^{2n-4} hyperbolische Geraden $\langle u, w\rangle$, die insbesondere nicht entartet sind ($a = 0$ und w' frei wählbar). Damit gibt es also $(q^2-1)q^{2n-3}$ weitere isotrope Vektoren.

Wir erhalten für $n > 2$ die Rekursionsgleichung

$$\iota_n = q^2\iota_{n-2} + (q^2-1)q^{2n-3} + (q^2-1).$$

Aus dieser Gleichung erhalten wir leicht die angegebene Anzahl.

3. Schritt: Die Anzahl an hyperbolischen Paaren in V ist $q^{2n-3}(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)$. Denn sei (u, v) ein hyperbolisches Paar. Dann liegt v nicht in $\langle u\rangle^\perp$ und in $\langle v\rangle$ gibt es keine weiteren Vektoren, die mit u ein hyperbolisches Paar bilden (hyperbolische Paare sind normiert). Nach unseren Überlegungen im 2. Schritt gibt es damit q^{2n-3} isotrope Vektoren, die mit u (in der 1. Komponente) ein hyperbolisches Paar bilden.

4. Schritt: Nun können wir die Anzahl der unitären Basen bestimmen. Sei zunächst n gerade. Dann ist die Anzahl der unitären Basen, unter Verwendung von (iii) des letzten Lemmas, gleich

$$q^{2n-3}(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)q^{2n-5}(q^{n-3}-(-1)^{n-3})(q^{n-2}-(-1)^{n-2})\cdot ...$$

$$= q^{\frac{n(n-1)}{2}}\prod_{i=1}^{m}(q^i-(-1)^i).$$

Sei nun n ungerade. Eine unitäre Basis hat nach (iv) im letzten Lemma die Form

$$(e_1, f_1, ..., e_l, f_l, w)$$

mit hyperbolische Paaren (e_i, f_i) und $\beta(w, w) = 1$. Es gibt $q+1$ Möglichkeiten, w zu wählen. Damit ist auch jetzt die Anzahl der unitären Basen gleich

$$q^{2n-3}(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)q^{2n-5}(q^{n-3}-(-1)^{n-3})(q^{n-2}-(-1)^{n-2})\cdot ...\cdot (q+1)$$

$$= q^{\frac{n(n-1)}{2}}\prod_{i=1}^{m}(q^i-(-1)^i)).$$

□

2.1.3 Orthogonale Gruppen

Die 3. Möglichkeit im Satz von Birkhoff und von Neumann ist, dass $\beta : V \times V \to \mathbb{F}_q$ eine symmetrische Bilinearform ist. Wie wir bereits erwähnt haben, ist es nicht ausreichend, die Invariantengruppe der Bilinearform zu betrachten. Wir betrachten die Invariantengruppe einer quadratischen Form. Sei also im Folgenden $Q : V \to \mathbb{F}_q$ eine quadratische Form, das heißt für $a \in \mathbb{F}_q$ und $v \in V$ gilt $Q(av) = a^2Q(v)$ und die Polarform $\beta : V \times V \to \mathbb{F}_q$ ist eine Bilinearform, wobei β definiert ist als

$$\beta(u, v) := Q(u+v) - Q(u) - Q(v) \text{ mit } u, v \in V.$$

Es sei außerdem vorrausgesetzt, dass Q nicht-ausgeartet ist, also dass 0 der einzige singuläre Vektor (bzgl. Q) im Radikal von β ist. (Äquivalenterweise ist die Einschränkung von Q auf dem Radikal injektiv, denn Q ist auf *rad* V additiv).

Definition 2.23
- (V, Q) *heißt* Orthogonaler Raum.
- *Wir definieren die* Orthogonale Gruppe *als Invariantengruppe von* Q*:*

$$Q(V) := \{g \in GL(V) \mid Q(g(v)) = Q(v)\ \forall v \in V\}.$$

Wir fassen einige hilfreiche Eigenschaften zusammen.

Bemerkung 2.24 *(i) Ist die Körpercharakteristik q_0 ungerade, so ist die Polarform β symmetrisch und nicht-ausgeartet und $O(V)$ ist die Invariantengruppe von β. Ist eine symmetrische Bilinearform β' gegeben, so können wir eine Quadratische Form über*

$$Q' := V \to \mathbb{F}_q,\ v \mapsto \frac{1}{2}\beta(v, v)$$

definieren, deren Polarform gerade wieder β' ist. Quadratische und Polarform legen sich also gegenseitig eindeutig fest.

(ii) Ist die Charakteristik wiederum 2, so gilt für $v \in V$

$$\beta(v, v) = Q(v + v) - Q(v) - Q(v) = 0.$$

Damit ist β alternierend und, da die Charakteristik 2 ist, damit auch symmetrisch. Offensichtlich können mehrere quadratische Formen die gleiche Polarform haben.

(iii) Sei $B = (b_1, ..., b_n)$ eine Basis von V und Φ die zugehörige Gram-Matrix von β, d.h. $\Phi := (\beta(b_i, b_j))_{i,j=1,...,n}$. Ein Element $g \in GL(n, q)$ sei bezüglich der Basis B aufgefasst. Wegen den beiden oberen Punkten folgt aus $g \in O(V)$, dass gilt

$$g^{tr}\Phi g \ = \ \Phi.$$

Ist die Charakteristik ungerade, so gilt auch umgekehrte Implikation.

(iv) Aus dem letzten Punkt folgt insbesondere, falls die Polarform β nicht-ausgeartet ist, dass Elemente der Orthogonalen Gruppe die Determinante 1 oder -1 haben. Dies gilt bei ungerader Charakteristik immer.

(v) Ist die Charakteristik gerade, so ist die Determinante immer 1 (die Elemente der Orthogonalen Gruppe lassen eine symplektische Form invariant und liegen somit in der Speziellen Linearen Gruppe, siehe auch [13] S. 137).

(vi) Sind $u, v \in V$ mit $\beta(u, v) = 0$, so erhalten wir durch Auswerten von $\beta(u, v)$ die nützliche Eigenschaft

$$Q(u + v) = Q(u) + Q(v).$$

Wir sollten noch erwähnen, dass die Struktur der Orthogonalen Gruppe $O(V)$ stark von den Eigenschaften der quadratischen Form Q abhängt. Häufig schreibt man deswegen auch $O(V, Q)$ statt $O(V)$. Das nächste Lemma wird uns aber liefern, dass es für ungerade Dimension nur einen Isomorphietyp der Orthogonalen Gruppen und für gerade Dimension genau zwei Isomorphietypen gibt. Wir werden unsere Notationen der Orthogonalen Gruppen danach entsprechend anpassen.

Lemma 2.25 *(i) Ist $n = \dim V \geq 3$, so enthält V ein hyperbolisches Paar aus zwei singulären Vektoren.*

(ii) Sei $(u, v) \in V^2$ so ein Paar. Dann gilt

$$V = \langle u, v\rangle \perp \langle u, v\rangle^{\perp}.$$

(iii) Es existieren hyperbolische Paare $(e_1, f_1), ..., (e_l, f_l)$ in V, jeweils aus singulären Vektoren, mit einer orthogonalen Zerlegung

$$V = \langle e_1, f_1\rangle \perp ... \perp \langle e_l, f_l\rangle \perp W,$$

wobei W keine singulären Vektoren enthält und $\dim W \in \{0, 1, 2\}$. Der Witt-Index von (V, Q) ist l.

Beweis: Zu (i): Zunächst zeigen wir, dass V einen singulären Vektor enthält. Sei zunächst q gerade. Dann existieren $v \in V\backslash\{0\}$ und $u \in \langle v\rangle^{\perp}\backslash\langle v\rangle$. Bemerkung 2.24 (vi) liefert

$$Q(au + by) = a^2Q(u) + b^2Q(v).$$

Alle Körperelemente von $\mathbb{F}_q$ sind Quadrate, also existieren $a, b \in \mathbb{F}_q$ mit $ab \neq 0$ und $a^2Q(u) + b^2Q(v) = 0$. Damit ist $au + by \neq 0$ ein singulärer Vektor. Sei nun q ungerade. Dann existieren linear unabhängige $u, v, w \in V$ mit $\beta(u, v) = 0$ und $\beta(u, w) = \beta(v, w) = 0$. Außerdem seien u, v und w nicht singulär (sonst sind wir fertig). Die Mengen $\{a^2Q(u)|a \in \mathbb{F}_q\}$ und $\{-(b^2Q(v) + Q(w))|b \in \mathbb{F}_q\}$ haben jeweils $\frac{q+1}{2}$ Elemente und damit ein gemeinsames. Es existieren also $a, b \in \mathbb{F}_q$ mit

$$Q(au + bv + w) = a^2Q(u) + b^2Q(v) + Q(w) = 0.$$

Wegen $Q(w) \neq 0$ ist $au + bv + w \neq 0$ ein singulärer Vektor.

Insgesamt gibt es also einen singulären Vektor $u \neq 0$. Sei $w \in V$ mit $\beta(u, w) \neq 0$ (Q ist nicht-ausgeartet und somit ist 0 der einzige nicht singuläre Vektor im Radikal von β). Wir setzen $v := -Q(w)\beta(u, w)^{-2}u + \beta(u, w)^{-1}w$. Es gilt

$$\beta(u, v) = -Q(w)\beta(u, w)^{-2}\beta(u, u) + \beta(u, w)^{-1}\beta(u, w) = 0 + 1 = 1$$

und

$$Q(v) = \beta(u, w)^{-2}Q(\frac{-Q(w)}{\beta(u, w)}u + w) = \beta(u, w)^{-2}(\beta(\frac{-Q(w)}{\beta(u, w)}u, w) + Q(\frac{-Q(w)}{\beta(u, w)}u) + Q(w) = 0.$$

Somit ist (u, v) ein hyperbolisches Paar aus singulären Vektoren.

(ii) und (iii) folgen jetzt sofort.

□

Verschiedene Orthogonale Räume können sich also bis auf Isometrie nur durch die Dimension des Teilraums W aus dem letzten Lemma und das Abbildungsverhalten auf dem Teilraum unterscheiden. Es gibt also insbesondere nur endlich viele Isomorphietypen von Orthogonalen Gruppen.

Folgerung 2.26 *(i) Ist $\dim W = 0$, so gilt für einen beliebigen Vektor $\sum_{i=1}^{l} a_ie_i + b_if_i \in V$ mit $a_i, b_i \in \mathbb{F}_q$:*

$$Q(\sum_{i=1}^{l} a_ie_i + b_if_i) = \sum_{i=1}^{l} a_ib_i.$$

Insbesondere sind alle Orthogonalen Räume, deren Witt-Index die Hälfte der Dimension ist, isometrisch. Die Polarformen sind immer nicht-ausgeartet. Alle Orthogonalen Gruppen dieser Räume sind isomorph.

(ii) Ist $\dim W = 1$, *d.h* $W = \langle w \rangle$ *mit* $Q(w) \neq 0$, *so gilt für einen beliebigen Vektor* $\sum_{i=1}^{l}(a_i e_i + b_i f_i) + cw \in V$ *mit* $a_i, b_i, c \in \mathbb{F}_q$*:*

$$Q(\sum_{i=1}^{l}(a_i e_i + b_i f_i) + cw) = \sum_{i=1}^{l} a_i b_i + c^2 Q(w).$$

Ist q gerade, so gibt es nur einen Isometrietyp dieser Orthogonalen Räume. Die zugehörige Polarform ist ausgeartet mit Radikal W*. Ist q ungerade, so gibt es zwei Isometrietypen, die Räume, bei denen* $Q(w)$ *ein Quadrat ist, und die Räume, bei denen das nicht gilt.*

(iii) Ist $\dim W = 2$, *d.h* $W = \langle e, f \rangle$ *mit* $Q(e) = 1$ *und* $\beta(e, f) = 1$, *so gilt für einen beliebigen Vektor* $\sum_{i=1}^{l}(a_i e_i + b_i f_i) + ae + bf \in V$ *mit* $a_i, b_i, a, b \in \mathbb{F}_q$*:*

$$Q(\sum_{i=1}^{l}(a_i e_i + b_i f_i) + ae + bf) = \sum_{i=1}^{l} a_i b_i + a^2 + ab + b^2 Q(f).$$

Die Polarform ist nicht-ausgeartet und alle Orthogonalen Räume dieser Form sind isometrisch.

Vertreter der Isomorphietypen aus (i) bis (iii) definieren wir entsprechend.

Definition 2.27 *(i) Ist* $(\mathbb{F}_q^n, Q)$ *ein Orthogonaler Raum mit gerader Dimension,* $\dim V = n = 2m$*, und Witt-Index m, so nennen wir sie auch vom Witt-Typ +. Die Orthogonale Gruppe bezeichnen wir mit*

$$O^+(2m, q) := O(V).$$

(ii) Ist $(\mathbb{F}_q^n, Q)$ *ein Orthogonaler Raum mit ungerader Dimension,* $\dim V = n = 2m + 1$*, (Witt-Typ 0) so bezeichen wir die Orthogonale Gruppe, unabhängig vom Isomorphietyp, mit*

$$O(2m + 1, q) := O(V).$$

(iii) Ist $(\mathbb{F}_q^n, Q)$ *ein Orthogonaler Raum mit gerader Dimension,* $\dim V = n = 2m$*, und Witt-Index* $m - 1$*, so hat sie Witt-Typ −. Wir bezeichen die Orthogonale Gruppe mit*

$$O^-(2m, q) := O(V).$$

(iv) Setzen wir $\epsilon := 2m - n + 1$*, so ist* ϵ *gleich* $1, 0$ *oder* -1*, je nachdem, ob wir die Fälle (i), (ii) oder (iii) betrachten. Wir schreiben* $O^\epsilon(2m, q)$ *für die Gruppen* $O^+(2m, q)$ *beziehungsweise* $O^-(2m, q)$*.*

Wir wollen jetzt die Ordnungen der Orthogonalen Gruppen bestimmen.

Satz 2.28 *Es gelten*

(i)

$$|O^+(2m, q)| = 2q^{m(m-1)}(q^m - 1) \prod_{i=1}^{m-1}(q^{2i} - 1),$$

(ii)

$$|O^+(2m + 1, q)| = \begin{cases} q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1) & \text{falls } q \text{ gerade,} \\ 2q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1) & \text{falls } q \text{ ungerade,} \end{cases}$$

(iii)

$$|O^-(2m,q)| = 2q^{m(m-1)}(q^m+1)\prod_{i=1}^{m-1}(q^{2i}-1).$$

Beweis: Sei $\epsilon = 2m-n+1$. Wir gehen in mehreren Schritten vor.

1. Schritt: Die Anzahl der singulären Vektoren in V ist $(q^{l-\epsilon}+1)(q^l-1)$, wobei l den Witt-Index bezeichnet.
Denn sei σ_l^ϵ die Anzahl der singulären Vektoren. Für $l=0$ gibt es keine singulären Vektoren, d.h. $\sigma_0^\epsilon = 0$. Ansonsten seien $(u,v) \in V^2$ ein hyperbolisches Paar aus singulären Vektoren und $w \in V$ ein singulärer Vektor. Dieser ist eindeutig schreibbar als $w = au + bv + w'$ mit $a,b \in \mathbb{F}_q$ und $w' \in \langle u,v\rangle^\perp$. Ist $b=0$ so ist w genau dann singulär, wenn $w'=0$ und $a \neq 0$ oder wenn $w' \neq 0$ singulär und $a \in \mathbb{F}_q$ beliebig sind. Es gibt damit $q-1+q\sigma_{l-1}^\epsilon$ singuläre Vektoren in $\langle u\rangle^\perp$. Angenommen $w \notin \langle u\rangle^\perp$, d.h. $b \neq 0$, dann gilt $Q(w) = ab + Q(w') = 0$ genau dann, wenn $a = \frac{-Q(w')}{b}$. Es gibt also weitere $q^{n-2}(q-1)$ singuläre Vektoren. Insgesamt gilt

$$\sigma_l^\epsilon = q\sigma_{l-1}^\epsilon + q^{n-2}(q-1) + q - 1.$$

Wie erwähnt ist $\sigma_0^\epsilon = 0$ und damit

$$\sigma_l^\epsilon = (q^{l-\epsilon}+1)(q^l-1).$$

2. Schritt: Die Anzahl der hyperbolischen Paare in V ist $q^{n-2}\sigma_l^\epsilon$.
Denn ist u ein singulärer Vektor und $v \in V$ so, dass (u,v) ein hyperbolisches Paar ist. Ein anderer Vektor v' bildet mit u genau dann ein weiteres hyperbolisches Paar, wenn v' die Form $v' = -Q(w') + v + w'$ mit $w' \in \langle u,v\rangle^\perp$ (beliebig) hat. w' ist also frei wählbar und wegen $\dim\langle u,v\rangle^\perp = n-2$ gibt es genau $q^{n-2}\sigma_l^\epsilon$ hyperbolische Paare.

3. Schritt: Verwenden wir die Zerlegungen in Lemma 2.25 (iii) und zählen die Möglichkeiten, sukzessiv geordnete hyperbolische Paare zu wählen, so erhalten wir für die Ordnung der Orthogonalen Gruppen

$$|O(V)| = q^{2l-1-\epsilon}\sigma_l^\epsilon q^{2l-3-\epsilon}\sigma_{l-1}^\epsilon \cdots q^{1-\epsilon}\sigma_1^\epsilon |O(W)|,$$

wobei W ein Untervektorraum wie in Lemma 2.25(iii) sei.

4. Schritt: Es bleibt die Ordnung von $O(W)$ für einen Vektorraum W der Dimension $0,1$ oder 2, der keine singulären Vektoren einer quadratischen Form Q enthält, zu bestimmen. Es ist

$$|O(W)| = \begin{cases} 1 & \text{falls } \dim W = 0, \\ 2 & \text{falls } \dim W = 1, \\ 2(q+1) & \text{falls } \dim W = 2. \end{cases}$$

Denn für $\dim W = 0$ ist $O(W) = O(0,q) = \{1\}$ und für $\dim W = 1$ ist $O(W) = \{\pm 1\}$. Sei nun $\dim W = 2$, wollen wir die Ordnung der Gruppe $O^-(2,q)$ bestimmen. Es ist $W = \langle e,f\rangle$ mit $e,f \in V$ wie im Lemma, das heißt $Q(e) = \beta(e,f) = 1$ und $Q(f) \neq 0$. Die Quadratische Fom ist gegeben durch

$$Q(ae+bf) = a^2 + ab + b^2Q(f) \text{ mit } a,b \in \mathbb{F}_q.$$

Das Polynom $x^2 + x + Q(f) \in \mathbb{F}_q[x]$ ist irreduzibel (sonst gäbe es einen singulären Vektor). Sei ω eine Nullstelle. Wir identifizieren $\mathbb{F}_{q^2} = \mathbb{F}_q[\omega]$ und erhalten den Isomorphismus

$$\varphi : W \to \mathbb{F}_{q^2},\ ae+bf \mapsto a - b\omega.$$

Sei $\tau : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ der nichttriviale Galoisautomorphismus. τ bildet ω auf $-\omega - 1$ ab. Die Norm N der Körpererweiterung ist somit gegeben durch $N = Q \circ \varphi^{-1}$. Wir wollen

$$O^-(2m,q) = \{\varphi^{-1}b\tau^i\varphi \mid b \in \mathbb{F}_{q^2},\ N(b) = 1,\ i = 0,1\}$$

zeigen. Sei also $g \in O^-(2m,q)$. Wir setzen $b := \varphi g(e) = \varphi g \varphi^{-1}(1)$. b hat Norm 1, denn $N(b) = Q(g(e)) = Q(e) = 1$. Sei nun $b = 1$ angenommen. Wir setzten $c := \varphi g(-f) = \varphi g \varphi^{-1}(\omega)$ und sehen $N(c) = Q(f) = N(\omega)$. $1 + c$ hat ebenso Norm $Q(f)$, denn

$$N(1+c) = Q\left(g(\varphi(1+\omega))\right) = Q\left(\varphi(1+\omega)\right) = N(1+\omega) = (1+\omega)(-\omega)N(\omega).$$

Damit ist c eine Nullstelle von $x^2 + x + Q(f)$ und somit $c = \omega$ oder $c = \tau(\omega) = -1 - \omega$. Damit gilt $\varphi g \varphi^{-1} \in \langle \tau \rangle$. Als Ordnung ergibt sich somit $|O^-(2m,q)| = 2(q+1)$.

Die angegebenen Ordnungen können jetzt leicht berechnet werden. □

2.2 Eigenwerte

Wir wollen noch Eigenschaften von einzelnen Matrizen betrachten. Bekanntermaßen ist $\lambda \in K$ ein Eigenwert zu $g \in X(n,q)$, wenn ein Vektor $v \in K^n$, $v \neq 0$, mit $gv = \lambda v$ existiert. Also genau dann, falls λ eine Nullstelle des charakteristischen Polynoms (und des Minimalpolynoms) von g ist. g hat genau dann keine Eigenwerte, falls das charakteristische Polynom keine Nullstellen über K hat. Ist p also ein irreduzibler Teiler vom charakteristischen Polynom, so ist p das Minimalpolynom für ein $\lambda \notin K$, das algebraisch über K ist. Insgesamt gilt $\mathbb{F}_q[\lambda] = \mathbb{F}_{q^k}$ (bzw. $\mathbb{F}_{q^2}[\lambda] = \mathbb{F}_{q^{2k}}$ im unitären Fall), wobei $k := \deg p > 1$. Indem wir $X(n,q)$ auf natürliche Weise als Untergruppe von $X(n,q^k)$ auffassen, existiert ein Vektor $v \in K[\lambda]^n$, sodass $gv = \lambda v$ gilt. Neben λ erfüllen auch die anderen Nullstellen von p die gleichen Eigenschaften. Dies sind genau die Galois-Konjugierten von λ, also $\lambda,\ \lambda^q,\ ...,\ \lambda^{q^{k-1}}$. Der Kern von $p(g)$ hat Dimension mindestens k und enthält einen k-dimensionalen, g-invarianten Teilraum von K^n. Insbesondere ist g nicht $k-$satt und höchstens $(k-1)$-satt. Dies führt uns zu en folgenden Definitionen.

Definition 2.29 *Sein $g \in X(n,q)$ und $\lambda \in \bar{K}$.*

- *λ heißt* verallgemeinerter Eigenwert von *g, falls λ eine Nullstelle des charakteristischen Polynoms von g ist. Ist es im Kontext klar, wollen wir einfach verallgemeinerte Eigenwerte als Eigenwerte bezeichnen.*
- *λ heißt* b-sättigender Eigenwert von *g oder* b-sättigend für *g, wenn λ verallgemeinerter Eigenwert von g ist und der Grad der Körpererweiterung $K[\lambda]$ echt größer als b ist.*

Bemerkung 2.30 *Ist λ b-sättigend für g, so ist ein nicht-trivialer, von λ induzierter g-invarianter Teilraum mindestens k-dimensional, denn jeder Eigenwert induziert einen invarianten Untervektorraum als Teilraum des Haupraums. Es gilt also die hilfreiche Äquivalenz*

$$g \in X(n,q) \text{ ist } b\text{-satt} \ \Leftrightarrow\ \text{alle verallgemeinerten Eigenwerte von } g \text{ sind } b\text{-sättigend.}$$

Wir sehen also, dass die Eigenschaft b-satt zu sein, nur von den Eigenwerten abhängt. Die genaue Verteilung der Jordanblöcke in der Jordannormalform ist in diesem Zusammenhang weniger interessant. Die multiplikative Jordanzerlegung, die wir jetzt behandeln wollen, trennt diese beiden Aspekte.

2.2.1 Jordanzerlegung

In diesem Abschnitt sei ausnahmsweise K ein perfekter, nicht unbedingt endlicher Körper.

Definition 2.31

- *Eine Matrix $t \in K^{n\times n}$ heißt* nilpotent, *falls $t^l = 0$ für ein $l \geq 1$, also falls 0 der einzige verallgemeinerte Eigenwert ist.*
- *Ein Element $u \in X(n,K)$ heißt* unipotent, *falls u nur den verallgemeinerten Eigenwert 1 besitzt, also falls $u - 1$ nilpotent ist.*

- *Ein Element $s \in X(n,K)$ heißt* halbeinfach*, falls sein Minimalpolynom separabel ist.*

Ist $s \in X(n,K)$ halbeinfach, so hat das Minimalpolynom nur einfache Nullstellen. Über einem passenden Erweiterungskörper, der alle Eigenwerte enthält, ist g also diagonalisierbar. Insbesondere sind, falls K algebraisch abgeschlossen ist, halbeinfach und diagonalisierbar äquivalent.

Satz 2.32 *(Jordanzerlegung)*
Sei $g \in X(n,K)$.
Dann existieren die

(i) additive Jordanzerlegung $g = s + t$, wobei $s \in X(n,K)$ halbeinfach mit gleichem charakteristischem Polynom wie g und $t \in K^{n\times n}$ nilpotent sind und $st = ts$ gilt.

(ii) multiplikative Jordanzerlegung $g = su = us$, wobei s wie in (i) und $u \in X(n,K)$ unipotent sind, insbesondere gilt $u = 1 + s^{-1}t$.

Die Zerlegungen sind jeweils eindeutig. s,t und u sind als Polynome in g ohne konstanten Term ausdrückbar. Das Element s heißt auch der ***halbeinfache Anteil*** *von g und entsprechend t der* ***nilpotente Anteil*** *und u der* ***unipotente Anteil****.*

Beweis: Für den Beweis vergleiche man auch [1, S. 79] und [12, S. 24-26].

Zu (i): Sei zunächst K algebraisch abgeschlossen. Dann zerfällt das ckarakteristische Polynom $\chi_g(x)$ von g in Linearfaktoren $(x-\lambda_i)$ für die Eigenwerte λ_i von g, d.h.

$$\chi_g(x) = \prod_{i=1}^{s}(x-\lambda_i)^{n_i}, \text{ wobei } \sum n_i = n.$$

Nach dem Chinesischen Restsatz existiert ein Polynom $p(x) \in K[x]$ mit

$$p(x) \equiv \lambda_i \pmod{(x-\lambda_i)^{n_i}} \text{ und } p(x) \equiv 0 \pmod{x}.$$

Wir definieren weiterhin $s := p(g)$ und $o := q - p(g)$.

Beh.: $g = s + t$ ist die additive Jordanzerlegung.

Offensichtlich vertauschen s und t. Das Minimalpolynom von s ist $\prod_{i=1}^{s}(s-\lambda_i)$, also ist s diagonalisierbar. Dies ist wegen $K = \bar{K}$ äquivalent zu halbeinfach. Sei $V = K^n = \bigoplus_{i=1}^{s} V_{\lambda_i}$ mit $V_{\lambda_i} = Kern((g-\lambda_i)^{n_i})$ die Zerlegung in Haupträume. Auf V_{λ_i} ist $(g-\lambda_i)^{n_i} = 0$, also hat s die Form $s = \lambda_i I_{n_i}$. Außerdem hat g auf V_{λ_i} nur den Eigenwert λ_i, also ist $t = g - s$ auf V_{λ_i} nilpotent. Dann ist t aber insgesamt nilpotent. Dies zeigt die Behauptung.

Zum Beweis der Eindeutigkeit sei $g = s' + t'$ eine weitere (additive) Jordanzerlegung. Nun ist s' halbeinfach und somit diagonalisierbar und muss auf V_{λ_i} die Form $\lambda_i I$ haben, also gilt $s = s'$ und damit auch $t = t'$.

Sei nun K nicht algebraisch abgeschlossen. über $\bar{K}$ habe g wieder die Eigenwerte $\lambda_1, ..., \lambda_s$ und es existiert die Jordanzerlegung $g = s + t$ mit $s,t \in X(n,\overline{K})$. Wir wollen $s,t \in X(n,K)$ zeigen. Dazu sei E/K eine Galoiserweiterung, sodass E alle Eigenwerte λ_i enthält. Für alle $\sigma \in Gal(E/K)$ gilt $\sigma(g) = g$ (komponentenweises Anwenden) und andererseits

$$\sigma(g) = \sigma(s) + \sigma(t).$$

Aus der Eindeutigkeit der Jordanzerlegung, $\sigma(s)$ halbeinfach und $\sigma(t)$ nilpotent folgt

$$\sigma(s) = s \text{ und } \sigma(t) = t \ \ \forall\ \sigma \in Gal(E/K),$$

damit gilt $s,t \in GL(n,K)$ nach Galois.

Zu (ii): Sei $g = s+t$ die additive Jordanzerlegung. Definiere $u := I_n + s^{-1}t$. Dann ist $u - I_n = s^{-1}t$ nilpotent, also ist u unipotent und die Eigenschaften der multiplikativen Jordanzerlegung folgen direkt aus denen der additiven. □

2.2.2 Eigenwertpaare und b-Äquivalenz

Eine Matrix g ist genau dann b-satt, wenn der halbeinfache Anteil s b-satt ist. Dies hängt nun wiederum nur von den Eigenwerten oder dem charakteristischen Polynom ab. Es ist in diesem Zusammenhang hilfreich, unsere Begriffe zu erweitern.

Definition 2.33
- *Ein algebraisches Element $\lambda \in \bar{K}$ heißt* b-sättigend*, falls $[K[\lambda] : K] > b$.*
- *Ein Polynom $p(x) \in K[x]$ heißt* b-satt*, falls alle Nullstellen über dem algebraischen Abschluss b-sättigend sind.*

Außerdem können wir eine für uns hilfreiche Äquivalenzrelation definieren.

Definition 2.34 *Seien $g, h \in X(n,q)$. g und h heißen $\chi-$*äquivalent*, Bezeichnung $g \sim_\chi h$, falls die halbeinfachen Anteile von g und h konjugiert sind. Dies gilt natürlich genau dann, wenn die charakteristischen Polynome gleich sind.*

Die Ähnlichkeitsrelation von Matrizen ist eine Verfeinerung von $\sim_\chi$. Die Beschränkung auf halbeinfache Matrizen ist aber nur bedingt hilfreich. Wir wollen Proportionen berechnen und zu verschiedenen halbeinfachen Matrizen ist die Anzahl der unipotenten Matrizen, die jeweils mit der Matrix kommutieren, verschieden. So vertauschen alle unipotenten Matrizen mit

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \text{ aber}$$

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

kommutieren nicht (Zumindest falls die Körpercharakteristik nicht 3 ist, für Charakteristik 3 findet mal leicht ein anderes Beispiel).

Die Aufteilung der Matrizen mit Hilfe der Jordanzerlegung ist trotzdem hilfreich. Im letzten Abschnitt des Kapitels betrachten wir dafür unipotente Matrizen und insbesondere deren Proportion. Zunächst wollen wir aber die $\chi-$Äquivalenz beziehungsweise als Vertreter die halbeinfachen Elemente weiter betrachten. Man kann halbeinfache Elemente nach ihren unterschiedlichen Eigenwerten zerlegen beziehungsweise die Proportionen aufteilen, da sie (block-)diagonalisierbar sind. Interessant sind dann nur halbeinfache Matrizen, die wenige verschiedene Eigenwerte besitzen. Welche Eigenwerte notwendigerweise zusammen auftreten müssen, klärt der nächste Satz.

Satz 2.35 *Sei λ algebraisch über K.*

(i) Sei $g \in GL(n,q)$. Ist λ ein verallgemeinerter Eigenwert, so sind auch alle anderen Galois-Konjugierten λ^{q^i} mit $i \geq 0$ Eigenwerte von g.

(ii) Sei $g \in Sp(n,q)$ oder $g \in O^\epsilon(2m,q)$. Ist λ ein verallgemeinerter Eigenwert, so sind auch alle Galois-Konjugierten und λ^{-1} und alle Galois-Konjugierten von λ^{-1} Eigenwerte von g.

(iii) Sei $g \in U(n,q)$. Ist λ ein verallgemeinerter Eigenwert, so auch λ^{-q} und alle Galois-Konjugierten Eigenwerte von g.

Beweis: Zu (i): Sei λ ein Eigenwert von $g \in X(n,q)$. Dann ist λ eine Nullstelle des charakteristischen Polynoms χ_g von g. Da alle Koeffizienten von χ_g in K liegen, sind auch die Galois-Konjugierten von λ Nullstellen und damit Eigenwerte von g.

Zu (ii), (iii): Wir definieren

$$\lambda^* := \begin{cases} \lambda^{-1} & \text{falls } X \in \{Sp, O^\epsilon\}, \\ \lambda^{-q} & \text{falls } X = U. \end{cases}$$

Es sei Φ die Gram-Matrix, jeweils für die drei klassischen Gruppen. Für ein Element $g \in Sp(n,q)$ oder $g \in O^\epsilon(2m,q)$ gilt dann $g^{tr}\Phi g = \Phi$. Für $g \in U(n,q)$ bezeichne $\overline{g} \in U(n,q)$ die Matrix, die durch Anwenden von $x \mapsto x^q$ auf alle Einträge entsteht. Dann gilt $\overline{g}^{tr}\Phi g = \Phi$. Wir definieren

$$g^* := \begin{cases} g^{-tr} & \text{falls } X \in \{Sp, O\}, \\ \overline{g}^{-tr} & \text{falls } X = U. \end{cases}$$

In den betrachteten Fällen ist Φ invertierbar, also sind g und g^* ähnlich und haben insbesondere die selben Eigenwerte. Ist λ ein Eigenwert von g, so ist λ^* ein Eigenwert von g^* und somit auch von g. □

Für die Orthgonalen Gruppen können wir insbesondere festhalten, dass die Ergebnisse des letzten Satzes unabhängig von der Charakteristik des Körpers richtig sind. Entscheidend ist nur die Eigenschaft der Polarform (dass diese bilinear und nicht-ausgeartet ist). Wir können in unserem weiteren Vorgehen die Orthogonalen Gruppen ähnlich den Symplektischen behandeln. Allerdings gilt die Aussage für Orthogonale Gruppen von ungeradem Grad im Allgemeinen nicht. Diese Gruppen müssen wir aber, wie in Bemerkung 1.3 erwähnt, nicht beachten.

Wir wollen weiterhn die b-sättigenden und nicht-b-sättigenden Eigenwerte untersuchen. Dies liefert eine neue, hilfreiche Äquivalenzrelation. Zunächst eine nützliche Vorüberlegung.

Lemma 2.36 *Sei $g \in X(n,q)$.*
Dann können wir V in g-invariante Teilräume zerlegen,

$$V = V_0 \oplus V_{\leq b},$$

mit $n_0 := \dim V$ und $n_{\leq b} := \dim V_{\leq b}$, sodass die Einschränkung $g_{|_{V_0}} \in GL(n_0, q)$ b-satt ist und alle verallgemeinerten Eigenwerte von $g_{|_{V_{\leq b}}} \in GL(n_{\leq b}, q)$ nicht b-sättigend sind.
Ist $X \in \{Sp, U, O^\epsilon\}$, so ist die Zerlegung orthogonal.

Beweis: Wir definieren das Polynom

$$\Psi_b(x) := \prod_{\lambda \in \bar{K} \text{ nicht } b-\text{sättigend}} (x - \lambda)^n$$

und

$$V_0 := Bild(\Psi_b(g)) \text{ und } V_{\leq b} := Kern(\Psi_b(g)).$$

Auf invarianten Teilräumen hat g genau die gleichen Eigenwerte wie sein halbeinfacher Anteil. Sei also o.B.d.A. g halbeinfach. Alle Eigenvektoren zu einem nicht-b-sättigenden Eigenwert (über einem Erweiterungskörper) liegen dann in $V_{\leq b}$. Entsprechend hat $g_{|_{V_0}}$ ausschließlich b-sättigende Eigenwerte, ist also b-satt.

Sei nun $X \in \{Sp, U, O^\epsilon\}$. Über einem Erweiterungskörper E ist g diagonalisierbar. Es existiert eine direkte Summe $EV = EV_0 \oplus EV_{\leq b}$. Dann ist $EV_{\leq b}$ im orthogonalem Komplement von EV_0 enthalten und umgekehrt. Die Summe ist orthogonal und damit auch $V = V_0 \perp V_{\leq b}$. □

Definition 2.37 *Sei $g \in X(n,q)$. Wir können g wie im Lemma aufteilen. Wir bezeichnen*

- $g_{|_{V_0}}$ *als* b-satter Anteil,

- $g_{|_{V_{\leq b}}}$ *als* nicht-b-satter Anteil *und*
- $\Psi_b(x) := \prod_{\lambda \in \bar{K} \text{ nicht } b-\text{sättigend}} (x-\lambda)^n$.

Wir erkennen sofort, dass ein Element $g \in X(n,q)$ genau dann b-satt ist, wenn das charakteristische Polynom χ_g und Ψ_b teilerfremd sind. Der größte gemeinsame Teiler gibt also den nicht-b-satten Anteil an. Dies liefert eine Äquivalenzrelation.

Definition 2.38 *Seien $g, h \in X(n,q)$. g und h heißen $b-$äquivalent, Bezeichnung $g \sim_b h$, falls*

$$ggT(\Psi_b, \chi_g) = ggT(\Psi_b, \chi_h).$$

Dies ist der Fall, falls die halbeinfachen Anteile von g und h die selben nicht-b-sättigenden Eigenwerte mit selber Vielfachheit haben, also $\chi-$äquivalent sind.

$\sim_\chi$ ist eine Verfeinerung von $\sim_b$. Die b-satten Matrizen bilden eine b-Äquivalenzklasse, deren Proportion wir bestimmen wollen. Dafür berechnen wir die Proportionen aller anderen b-Äquivalenzklassen. Dies muss für jede klassische Gruppe gesondert geschehen und wird jeweils das erste Ziel in den Kapiteln 3 bis 6 sein.

2.2.3 Orthogonale Gruppen II

Die Orthogonalen Gruppen weisen zwar gewisse Ähnlichkeiten mit den Symplektischen auf, wir haben aber auch wesentliche Unterschiede zu beachten. Diese wollen wir in diesem Abschnitt behandeln und einige Vorbereitungen für unsere spätere Arbeit mit den Orthogonalen Gruppen im Kapitel 6 treffen.

In diesem Kapitel sei V ein $n-$dimensionaler $\mathbb{F}_q-$Vektorraum, Q eine quadratische Form auf V und (V,Q) ein Orthogonaler Raum. Die Gruppe $O(n,q)$ sei als Invariantengruppe des Raums aufgefasst. β bezeichne die Polarform von Q. Je nach Witt-Typ ist $O(n,q)$ von der Form $O^+(2m,q),\ O(2m+1,q)$ oder $O^-(2m,q)$.

Die Orthogonalen Gruppen für ungerade Dimension n müssen nicht beachtet werden, wie wir bereits in der Einleitung erwähnten. Alle Elemente besitzen einen Eigenwert. Dies werden wir jetzt beweisen.

Satz 2.39 *Sei $g \in O(2m+1,q)$ mit $m \in \mathbb{N}$.*

(i) Ist q ungerdade, so ist 1 oder -1 Eigenwert von g.

(ii) Ist q gerade, so ist die Polarfom β ausgeartet und das Radikal von V eindimensional. Das Radikal ist in einem Eigenraum von g enthalten.

Insbesondere enthält $O(2m+1,q)$ keine b-satten Elemente für alle $b \in \mathbb{N}$.

Beweis: Zu (i): Es ist, eventuell nach Wahl passender Basen, $g^{-1} = g^{tr}$ und $det(g) = \pm 1$. Ist $\det(g) = 1$, so folgt

$$\det(g - I_n) = \det(g^{tr}g - g^{tr}) = \det(I_n - g)^{tr} = -\det(g - I_n).$$

Somit ist $\det(g - I_n) = 0$ und 1 ist Eigenwert von g. Hat g die Determinante -1, so gilt $\det(-g) = 1$ und $-g$ hat den Eigenwert 1, womit g natürlich den Eigenwert -1 besitzen muss.

Zu (ii): Nach Folgerung 2.26 ist die Polarform β ausgeartet. Das Radikal ist eindimensional und ein nichttrivialer Vektor im Radikal ist damit ein Eigenwert von g. □

Im Folgenden sei n gerade, d.h. $n = 2m$. Die Orthogonalen Gruppen $O^\epsilon(2m,q)$ mit $\epsilon = \pm$ enthalten b-satte Elemente. Allerdings liegen diese alle in einem Normalteiler von Index 2. Diesen weden wir als Spezielle Orthogonale Gruppe bezeichnen.

Nach Bemerkung 2.24 haben alle Elemente der Orthogonalen Gruppen die Determinante 1 oder -1. Ist die Körpercharakteristik gerade, so haben alle offensichtlich Determinante 1, allerdings ist die Komutatorgruppe ein echter Normalteiler. Ist die Charakteristik wiederum ungerade, so ist der Kern der Determinantenabbildung ein Normalteiler von Index 2, denn für $v \in V$ nicht singulär hat die Isometrie

$$v \mapsto -v \text{ und } w \mapsto w \text{ für alle } w \in \langle v \rangle^{\perp}$$

die Determinante 1. Beide Normalteiler treten als Kern von ähnlichen Abbildungen auf.

Definition 2.40

- *Wir definieren die Komutatorgruppe $O(V)'$ der Orthogonalen Gruppe als $\Omega(V)$. Ist $V = \mathbb{F}_q^n$, das heißt $O(V) = O(n,q)$, so schreiben wir auch $\Omega(n,q) := \Omega(\mathbb{F}_q^n)$. Bei gerader Dimension bezeichnen wir $\Omega^+(2m,q) := O^+(2m,q)'$ und $\Omega^-(2m,q) := O^-(2m,q)'$.*
- *Ist die Körpercharakteristik q_0 ungerade, so ist die* Spezielle Orthogonale Gruppe *gegeben durch $SO(V) := O(V) \cap SL(V)$. Im Falle $V = \mathbb{F}_q^n$ schreiben wir $SO(n,q) := SO(\mathbb{F}_q^n)$ und im Falle $n = 2m$ verwenden wir auch die Bezeichnungen $SO^+(2m,q)$ beziehungsweise $SO^-(2m,q)$.*
- *Die* Dickson-Invarante *sei die Abbildung*

$$D : O(V) \to \mathbb{F}_2,\ g \mapsto \dim(Bild(1-g)) \pmod 2.$$

Die Dimension $n = 2m$ ist gerade und somit ist die Dickson-Invariante gleich

$$g \mapsto \dim(Kern(1-g)) \pmod 2.$$

Lemma 2.41 *Die Dickson-Invariante ist ein Homomorphismus. Der Kern ist gegeben durch*

$$Kern(D) = \begin{cases} \Omega(2m,q) & \text{falls } q \text{ gerade,} \\ SO(2m,q) & \text{falls } q \text{ ungerade.} \end{cases}$$

Beweis Siehe [3], Theorem 2 (D ist surjektiver Homomorphismus), [13], S. 160 (Kern für q ungerade) und Theorem 11.51 (für q gerade).

Definition 2.42 *Für die Orthogonalen Gruppen $O^\epsilon(2m,q)$ mit $\epsilon = \pm$ setzen wir, der Notation von Donald Taylor in [13] folgend:*

$$SO^\epsilon(2m,q) := Kern(D) = \begin{cases} \Omega(2m,q) & \text{falle } q \text{ gerade,} \\ SO(2m,q) & \text{falle } q \text{ ungerade.} \end{cases}$$

Den Kern der Dickson-Invariante nennen wir auch Spezielle Orthogonale Gruppe.

Entscheidend ist nun folgender Satz

Satz 2.43 *Sei $g \in O^\epsilon(2m,q)$ 1-satt.*
Dann gilt $g \in SO^\epsilon(2m,q)$.
Insbesondere liegen für alle $b \in \mathbb{N}$ alle $b-$satten Elemente einer Orthogonalen Gruppe bereits in der Speziellen Orthogonalen Gruppe

Beweis: Sei zunächst q ungerade. Da g b-satt ist, liegen alle Eigenwerte insbesondere nicht in $\lambda_i \notin \mathbb{F}_q$. g liegt in der Orthogonalen Gruppe und somit ist nach Satz 2.35 $\lambda \in \bar{K}$ genau dann ein Eigenwert von g, wenn λ^{-1} Eigenwert ist. Alle Eigenwerte treten also in Paaren auf und g hat die Determinante 1.

Ist q gerade, so verweisen wir auf Ergebnisse von Roger Dye 1977, siehe [3] Theorem 3. Nach Dye haben alle invarianten Teilräume genau dann gerade Dimension, wenn die Dimension des Bildes von $I_n - g$ gerade ist. Nach den Definitionen ist also g genau dann 1-satt, wenn g im Kern der Dicksoninvariante liegt, also $g \in SO^\epsilon(2m,q)$. □

2.3 Unipotente Matrizen

In diesem Abschnitt wollen wir die Proportion der Matrizen berechnen, deren charakteristisches Polynom eine Potenz von $p(x)$ ist, wobei p ein (irreduzibles) Minimalpolynom vom Grad $k := \deg p$ mit $1 \leq k \leq b$ ist. Im ersten Teil zeigen wir, dass die Größe einer $\chi-$ beziehungsweise b-Äquivalenzklasse von $p(x)^{n/k}$ in $X(n,q)$ genau die Proportion der unipotenten Matrizen in $X(n/k, q^k)$ ist.

Daher müssen zunächst unipotente Matrizen beziehungsweise deren Proportionen betrachtet werden. Daraus resultiert eine erzeugende Funktion für die Proportionen unipotenter Matrizen. Diese ist für die Generelle Lineare Gruppe identisch mit der Inversen der ganzen Funktion $G(q;z) := \prod_{i=1}^{\infty}(1 - zq^{-i})$, welche bereits Euler untersucht hat. Für die anderen klassischen Gruppen gelten ähnliche Identitäten mit der Euler'schen Funktion. Die Beweise sowie einige hilfreiche Eigenschaften der Euler'schen Funktion werden im 2. Teil behandelt.

Wir gehen allgemein für alle klassischen Gruppen vor, also K gleich $\mathbb{F}_q$ oder $\mathbb{F}_{q^2}$ und n gleich m oder $2m$ (siehe Tabelle 1).

2.3.1 Proportionen unipotenter Matrizen

Definition 2.44 *Sei $f(x) \in K[x]$ vom Grad n und $X(n,q)$ eine klassische Gruppe wie in Tabelle 1 oder $X(n,q) = SO^{\epsilon}(2m,q)$.*

- $\mathcal{X}_{X(n,q)}(f(x)) := \{g \in X(n,q) \mid \chi_g(x) = f(x)\}$ *sei die* Menge aller Matrizen in $X(n,q)$ mit charakteristischem Polynom $f(x)$.
- $\chi_{X(n,q)}(f(x)) := \frac{|\mathcal{X}(f(x))|}{|X(n,q)|}$ *bezeichne die Proportion dieser Matrizen.*
- *Meist wollen wir auf die Nennung von Gruppe und Dimension verzichten, also $\mathcal{X}(f(x)) := \mathcal{X}_{X(n,q)}(f(x))$ und $\chi(f(x)) := \chi_{X(n,q)}(f(x))$.*

$\mathcal{X}(f(x))$ ist genau eine Äquivalenzklasse von $\sim_\chi$ und falls f b-satt ist auch eine b-Äquivalenzklasse.

Im letzten Abschnitt haben wir bereits kurz unipotente Matrizen im Zusammenhang der Jordanzerlegung betrachtet. Unipotente Matrizen waren genau die Matrizen, die als einzigen (verallgemeinerten) Eigenwert 1 besitzen. Jetzt wollen wir die Proportionen der unipotenten Matrizen betrachten. Die Definitionen sind analog zu denen der b-satten Matrizen.

Definition 2.45

- $U(X(n,q)) := \{u \in X(n,q) |\ u \text{ unipotent}\}$ *sei die* Menge der unipotenten Matrizen in $X(n,q)$.
- $u(X(n,q)) := \frac{|U(X(n,q))|}{|X(n,q)|}$ *deren Proportion. Die Festlegungen $u(X(0,q)) := 1$ für $X \in \{GL, Sp, U\}$, $u(SO^+(0,q)) := 2$ und $u(SO^-(0,q)) := 0$ sind hilfreich und werden im Laufe der Arbeit klar.*
- $U(z) := U(X,q;z) := \sum_{m=0}^{\infty} u(X(n,q))z^m$ *für $z \in \mathbb{C}$ sei die erzeugende Funktion, die* unipotente Potenzreihe.

Die Proportion unipotenter Matrizen ist für $GL(n,q)$ einfach die Proportion nilpotenter Matrizen in $M(n,q)$, die Nathan J. Fine und Israel N. Herstein in [4] berechnet haben. Des weiteren gibt es ein Resultat von Robert Steinberg [11] über die Anzahl der unipotenten Elemente einer algebraischen Gruppe.

Lemma 2.46 *(Proportion nilpotenter und unipotenter Matrizen)*
Es gelten folgende Aussagen.

(i) (Fine, Herstein 1958, [4]) $|\chi(x^n)| = q^{-n}$ (in $M(n,q)$).

(ii) (Steinberg 1968, [11]) Sei H eine Untergruppe von $X(n,q)$, die nur aus unipotenten Elementen besteht und maximal mit dieser Eigenschaft ist. Die Anzahl unipotenter Matrizen ist dann $|U(X(n,q))| = |H|^2$. Ein Element ist genau dann unipotent, wenn es ein q_0-Element ist ($charK = q_0$, d.h. die Ordnung ist eine q_0-Potenz). Somit ist H eine $q_0 - Sylowgruppe$.

(iii) $u(GL(n,q)) = \chi((x-1)^n) = \frac{q^{n^2-n}}{|GL(n,q)|}$.

(iv) $u(Sp(2m,q)) = \frac{q^{2m^2}}{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}$.

(v) $u(U(n,q)) = \frac{q^{n^2-n}}{q^{(n^2-n)/2}\prod_{i=1}^{m}(q^i-(-1)^i)}$.

(vi) $u(SO\epsilon(2m,q)) = \frac{1}{2}q^{-2m}(q^m+\epsilon 1)\prod_{i=1}^{m}(1-q^{-2i})^{-1}$.

Beweis: Für (i) siehe [4] und für (ii) siehe [11], Theorem 15.1 (S. 98 - 104). Eine unipotente Matrix hat eine Ordnung von q_0-Potenz - man betrachte zum Beispiel die Jordannormalformen. Als Eigenwerte einer Matrix kommen nur Einheitswurzeln der Ordnung infrage. Hat eine Matrix also q_0-Potenz-Ordnung, so ist 1 der einzige mögliche verallgemeinerte Eigenwert.

(iii) folgt sofort aus (i) (oder (ii)). Wegen $|Sp(2m,q)| = q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$ (siehe Satz 2.17), $|U(n,q)| = q^{(n^2-n)/2}\prod_{i=1}^{m}(q^i-(-1)^i)$ (siehe Satz 2.22) und $|SO^\epsilon(2m,q)| = q^{m(m-1)}(q^m - \epsilon 1)\prod_{i=1}^{m-1}(q^{2i}-1)$ (siehe Sätze 2.28 und 2.41) gelten (iv), (v) und (vi) mit Verwendung von (ii) (Die Anzahl der unipotenten Matrizen ist das Quadrat der maximalen q-Potenz, die die Ordnung teilt).

□

Wir wollen das vorhergehende Lemma für die Bestimmung von $\chi(p(x)^{n/k})$ nutzen. Dafür können wir die Matrizen aus $\mathcal{X}(p(x)^{n/k})$ mit Hilfe von unipotenten Matrizen beziehungsweise der multiplikativen Jordan-Zerlegung darstellen.

Bemerkung 2.47 *Sei $\lambda \in \mathbb{F}_q\backslash\{0\}$. Eine Matrix mit ausschließlich dem Eigenwert λ hat als halbeinfache Anteil die Skalarmatrix $\lambda \cdot I$, mit der offensichtlich alle unipotenten Matrizen vertauschen. Damit sind $\mathcal{X}((x-\lambda)^n)$ und $\mathcal{X}((x-1)^n)$ bijektiv und für die Proportion gilt*

$$\chi((x-\lambda)^n) = u((X(n,q))).$$

Für die anderen Proportionen müssen wir ermitteln, welche unipotenten Matrizen mit den passenden halbeinfachen Anteilen vertauschen.

Satz 2.48 *Es gelte $k|n$. Sei $p(x) \in K[x]$ irreduzibel mit $deg(p) = k$. Matrizen $g \in \mathcal{X}(p(x)^{n/k})$ haben dann einen halbeinfachen Anteil konjugiert zu*

$$s_0 := Diag(M_p, ..., M_p),$$

wobei $M_p \in GL(k,q)$ die Begleitmatrix zu p bezeichnet. Der unipotente Anteil ist entsprechend konjugiert zu einer unipotenten Matrix, die mit s_0 vertauscht.

Es gilt

$$C_{X(n,q)}(s_0) \cong X(n/k, q^k).$$

und damit

$$U(C_{X(n,q)}(s_0)) = U(X(n/k, q^k)).$$

Beweis: Wir definieren das K-Algebraerzeugnis $S := \langle s_o \rangle$. S ist isomorph zum endlichen Körper F mit Körpergrad $[F : K] = k$. Genauer gilt also $F = \mathbb{F}_{q^k}$, falls $K = \mathbb{F}_q$, und $F = \mathbb{F}_{q^{2k}}$, falls wir die Unitären Gruppen untersuchen und damit $K = \mathbb{F}_{q^2}$ gilt.

Für den Zentralisator von S in $K^{n\times n}$ ergibt sich

$$C_{K^{n\times n}}(S) = \{x \in End_K(K^n) \mid xs = sx \ \forall\ s \in S\} \ \cong \ End_S(K^n) \cong End_F(K^n).$$

Wegen $K^n \cong F^{n/k}$ ist dies isomorph zu

$$End_F(F^{n/k}) \cong F^{n/k\times n/k}.$$

Daraus folgt direkt

$$C_{X(n,q)}(s_0) = X(n,q) \cap C_{K^{n\times n}}(S) \cong X(n,q) \cap F^{n/k\times n/k} = X(n/k, q^k).$$

Hierbei seien die F-Endomorphismen von $F^{n/k}$, also die $(n/k \times n/k)-$Matrizen über F als $K-$Endomorphismen von K^n, also als $(n \times n)$-Matrizen über K aufgefasst. Es gelte also $F^{n/k\times n/k} \leq K^{n\times n}$.

□

Folgerung 2.49 *Mit der Notation des vorherigen Satzes gibt es eine Bijektion zwischen*

$$\mathcal{X}(p(x)^{n/k}) \text{ und } s_0^{X(n,q)} \times U(X(n/k, q^k)).$$

Damit gilt für die Proportionen

$$\chi(p(x)^{n/k}) = u(X(n/k, q^k)) \ .$$

Beweis: Der halbeinfach Anteil jeder Matrix aus $\mathcal{X}(p(x)^{n/k})$ ist konjugiert zu s_o. Der unipotente Anteil liegt im Zentralisator und wird somit auf eine Matrix aus $C_{X(n,q)}(s_0) \cong X(n/k, q^k)$ konjugiert. Es folgt die Bijektion. Die Identität der Proportionen ergibt sich aus der Auswertung von $|\mathcal{X}(p(x)^{n/k})| = |s_0^{X(n,q)}||U(X(n/k, q^k)|$. Mit Hilfe des Bahnensatzes gilt dann

$$\chi(p(x)^{n/k})|X(n,q)| \ = \ \frac{|X(n,q)|}{|C_{X(n,q)}(s_0)|}\ u(X(n/k,q))\ |X(n/k,q^k)|.$$

Kürzen mit Hilfe des letzten Satzes liefert

$$\chi(p(x)^{n/k}) \ = \ u(X(n/k, q^k)).$$

□

2.3.2 Unipotente Potenzreihe und Euler'sche Funktion

Wir wollen die unipotente Potenzreihe $U(z) = \sum_{m=0}^{\infty} u(X(n,q))z^m$ untersuchen.

Definition 2.50 *(Euler'sche Funktion)*
Sei $x \in \mathbb{C}$ mit $|x| > 1$. Wir definieren die Funktion $G(x; -) : \mathbb{C} \to \mathbb{C}$ mit

$$G(x; z) := \prod_{i=1}^{\infty}(1 - x^{-i}z), \quad z \in \mathbb{C}.$$

Diese hat bereits Leonard Euler untersucht und wir bezeichnen sie hier als Euler'sche Funktion.

Hilfreich sind die Definitionen der Partialprodukte $c_n(x) := \prod_{i=1}^{\infty}(1 - x^{-i})^{-1}$ und des Grenzwertes $c(x) := \lim_{n\to\infty} c_n(x) = G(x; 1)^{-1}$.

Lemma 2.51 *$G(x;z)$ ist eine ganze Funktion (in der zweiten Komponente holomorph auf ganz $\mathbb{C}$) mit den einzigen Nullstellen $z \in \{x, x^2, ...\}$. Es gelten*

(i) $G(x;z) = \sum_{n=0}^{\infty} g(n)z^n$ *mit* $g(n) = (-1)^n x^{-n(n+1)/2} \prod_{i=1}^{n}(1-x^{-i})^{-1}$ *und* $z \in \mathbb{C}$,

(ii) $G(x;z)^{-1} = \sum_{n=0}^{\infty} h(n)z^n$ *mit* $h(n) = x^{-n} \prod_{i=1}^{n}(1-x^{-i})^{-1}$ *und* $|z| < |x|$,

(iii) sowie die Beziehungen $g(n) = (-1)^n c_n(x) x^{-n(n+1)/2}$ *und* $h(n) = x^{-n} c_n(x)$.

Man beachte, dass $g(n)$ und $h(n)$ von x abhängen.

Beweis: Für einen Beweis der Ganzheit von G siehe [2], S. 104.

G ist ganz, also ist G auf ganz $\mathbb{C}$ als Potenzreihe darstellbar:

$$G(x;z) = \sum_{n=0}^{\infty} g(n)z^n,$$

wobei $g(n)$ von x abhängt. Aus $G(x;xz) = (1-z)G(x;z)$ erhalten wir die Rekursionsgleichung

$$x^n g(n) = g(n) - g(n-1) \text{ d.h. } g(n) = -\frac{g(n-1)}{(x^n-1)} \ .$$

Wegen $g(0) = 1$ folgt $g(n) = (-1)^n c_n(x) x^{-n(n+1)/2}$ mit einem leichten Induktionsbeweis.

$G(x;z)^{-1}$ ist eine meromorphe Funktion mit einfachen Polen bei $x, x^2, ...$. Also ist $G(x;z)^{-1}$ für $|z| < |x|$ holomorph und dort als Potenzreihe entwickelbar:

$$G(x;z)^{-1} = \sum_{n=0}^{\infty} h(n)z^n.$$

Jetzt liefert $(1-z)G(x;xz)^{-1} = G(x;z)^{-1}$ eine Rekursionsgleichung

$$x^n h(n) - x^{n-1} h(n-1) = h(n),$$

aus der wir $h(n)$ berechnen können. □

Die Betrachtung der Euler'schen Funktion können wir mit dem folgenden Hauptsatz dieses Abschnitts begründen. Die Orthogonalen Gruppen wollen wir zunächst nicht behandeln, da der Zusammenhang zwischen unipotenter Potenzreihe und Euler'scher Funktion etwas komplizierter ist. Dies holen wir in einem späteren Kapitel (Lemma 7.9) nach.

Danach folgen noch einige Eigenschaften wie Taylorentwicklung und Abschätzungen, die wir in den folgenden Kapiteln benötigen und hier unkommentiert zusammenfassen wollen.

Satz 2.52 *Für die unipotenten Potenzreihen der verschiedenen klassischen Gruppen gelten folgende Identitäten mt der Euler'schen Funktion.*

(i) $U(GL, q; z) = G(q; z)^{-1}$, $|z| < q$

(ii) $U(Sp, q; z) = G(q^2; qz)^{-1}$, $|z| < q$

(iii) $U(U, q; z) = G(-q; -z)^{-1}$, $|z| < q$

Beweis: Zu (i): nach Lemma 2.46 (ii) gilt

$$u(GL(n,q)) = \frac{q^{n^2-n}}{|GL(n,q)|} = q^{n^2-n} \prod_{i=0}^{n-1} (q^n - q^i)^{-1} =$$

$$q^{n^2-n}q^{-n^2}\prod_{i=0}^{n-1}(1-q^{i-n})^{-1} = q^{-n}\prod_{i=1}^{n}(1-q^{-i})^{-1} = q^{-n}c_n(q)\ .$$

Im letzten Lemma haben wir $q^{-n}c_n(q) = h(n)_{|x=q}$ gezeigt, also stimmen die Koeffizienten der Potenzreihen $U(GL,q;z)$ und $G(q;z)^{-1}$ überein und damit die Potenzreihen.

Die Beweise zu (ii) und (iii) funktionieren analog, man muss nur Lemma 2.46 (iii) beziehungsweise (iv) verwenden.

Siehe auch [7], Theoreme 4.2 (für (i)), 5.2 (für (ii)) und 6.2 (für (iii)).

□

Lemma 2.53 *(i) Seien $f(z) = \sum_{i=1}^{\infty}(-1)^n a_n z^n$ und $g(z) = \sum_{i=1}^{\infty}(-1)^n b_n z^n$ zwei Potenzreihen mit $a_n, b_n \geq 0$. Dann gilt für das Produkt $(f\cdot g)(z) = \sum_{i=1}^{\infty}(-1)^n d_n z^n$ mit nichtnegativen $d_n \in \mathbb{R}$, d.h. die Koeffizienten alternieren.*

(ii) Seien $x \in \mathbb{R}$ mit $x \geq 2$ und $r \geq 1$. Die r-te Potenz der Euler'schen Funktion lässt sich als Potenzreihe entwickeln, $G(x;z)^r = \sum_{n=0}^{\infty}(-1)^n g^{(r)}(n)z^n$. Die Koeffizienten alternieren im Vorzeichen und lassen sich folgendermaßen abschätzen:

$$0 < g^{(r)}(n) < (2+3x^{-1/2})c(x)^r x^{-n(n+r)/2r} < \frac{16^r}{2}x^{-n(n+r)/2r},\ n\in\mathbb{N}\ .$$

Für große n, $n > 5r^2$, sind die Koeffizienten streng monoton fallend. Damit gilt für $N > 5r^2$

$$G(q,1)^r - \sum_{n=0}^{N}(-1)^n g^{(r)}(n) = (-1)^{N+1}\epsilon_N \text{ für ein } 0 < \epsilon_N < (-1)^{N+1}g^{(r)}(N+1).$$

Beweis: Zu (i): Die Koeffizienten des Produkts sind nach der Produktregel von Cauchy gegeben durch

$$\sum_{i=0}^{n}(-1)^i a_i (-1)^{n-i} b_{n-i} = (-1)^n \underbrace{\sum_{i=0}^{n} a_i\ b_{n-i}}_{=:\ d_n \geq 0}\ .$$

Zu (ii): Nach (i) alternieren die Koeffizienten im Vorzeichen. Für den Beweis der Abschätzungen und der Monotonie verweisen wir auf [7], Theorem 2.4.

□

Lemma 2.54 *(i) Die Euler'sche Funktion mit Parameter $x \in \mathbb{R}_{>0}$ kann an der Stelle $z = 1$ näherungsweise als Exponentialfunktion ausgedrückt werden, genauer gilt*

$$G(x;1) = \exp\left(\ -(x^{-1} + \frac{3}{2}x^{-2} + \frac{4}{3}x^{-3} + \frac{7}{4}x^{-4} + \frac{6}{5}x^{-5} + O(x^{-6}))\ \right)$$

(ii) $\exp(x) = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + O(x^4)$

Beweis: Zu (i): Indem wir den Logarithmus auf $G(x;1)$ anwenden, erhalten wir

$$\log G(x;1) = \sum_{i=1}^{\infty}\log(1-x^{-i}).$$

Die Potenzreihenentwicklung des Logarithmus, $\log(1-y) = -\sum_{j=1}^{\infty}\frac{1}{j}y^j$, ergibt dann

$$\log G(x;1) = -\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\frac{1}{j}x^{-ij} = -\sum_{i=1}^{\infty}\sum_{j|i}^{\infty}\frac{1}{j}x^{-i} = -(x^{-1}+\frac{3}{2}x^{-2}+\frac{4}{3}x^{-3}+\frac{7}{4}x^{-4}+\frac{6}{5}x^{-5}+O(x^{-6})).$$

Die Potenzreihenentwicklung der Exponentialfunktion (Taylorentwicklung um $x = 0$) liefert sofort (ii).

□

Satz 2.55 *Es gelten folgenden Näherungen.*

(i) $G(q;1)^{q-1} = e^{-1}(1 - \frac{1}{2}q^{-1} + \frac{7}{24}q^{-2} - \frac{25}{48}q^{-3} + O(q^{-4}))$.

(ii) $G(q^k;1)^{\frac{q^k-1}{k}} = e^{-1/k}(1 - \frac{1}{2k}q^{-k} + \frac{4k+3}{24k^2}q^{-2k} + O(q^{-3k}))$.

(iii) $G(q^k;1)^{-\frac{q^{k/p}-1}{k}} = 1 + \frac{1}{k}q^{-d} + O(q^{-(d+1)})$, *wobei* $d := k - k/p$ *mit* p *als kleinster Primteiler von* k. *Anders ausgedrückt ist* d *also gleich „*k *minus den größten Teiler von* k*“. Es gilt* $d \geq \frac{k}{2}$. *Für kleine* k *ist* d *folgendermaßen gegeben:*

k	2	3	4	5	6	7	8	9	10	11	12
d	1	2	2	4	3	6	4	6	5	10	6

(iv) $G(q^{4k};q^{2k})^{\frac{q^k}{k}} = (1 - \frac{1}{k}q^{-k} + O(q^{-2k}))$.

(v) $G(q^k;1)^{\frac{q^k-q^{k/p}}{2k}} = e^{-1/2k}(1 - \frac{1}{4k}q^{-d} + O(q^{-(d+1)}))$, *wobei* p *wieder der kleinste Primteiler von* k *sei.*

(vi) $G(-q^k;-1)^{\frac{q^k}{k}} = e^{-1/k}(1 + \frac{1}{2k}q^{-k} + O(q^{-2k}))$.

(vii) $G(q^k;1) \geq e^{-\frac{q^k}{(q^k-1)^2}}$.

Beweis: Zu (i): Teil (i) des Lemmas liefert

$$\begin{aligned} G(q,1)^{q-1} &= \exp(-(q-1)(q^{-1} + \frac{3}{2}q^{-2} + \frac{4}{3}q^{-3} + \frac{7}{4}q^{-4} + \frac{6}{5}q^{-5} + O(q^{-6})) \\ &= \exp(-1 - \frac{1}{2}q^{-1} + \frac{1}{6}q^{-2} - \frac{5}{12}q^{-3} + \frac{11}{20}q^{-4} + O(q^{-5})). \end{aligned}$$

Mit dem 2. Teil ist dies gleich

$$e^{-1}(1 - \frac{1}{2}q^{-1} + \frac{7}{24}q^{-2} - \frac{25}{48}q^{-3} + \frac{4583}{5760}q^{-4} + O(q^{-5})).$$

Zu (ii): Teil (i) des Lemmas liefert jetzt

$$\begin{aligned} G(q^k,1)^{\frac{q^k-1}{k}} &= \exp(-\frac{q^k-1}{k}(q^{-k} + \frac{3}{2}q^{-2k} + \frac{4}{3}q^{-3k} + O(q^{-4k})) \\ &= \exp(-\frac{1}{k} - \frac{1}{2k}q^{-k} + \frac{1}{6k}q^{-2k} + O(q^{-3k})) \end{aligned}$$

Mit dem 2. Teil des Lemmas ($x := -\frac{1}{2k}q^{-k} + \frac{1}{6k}q^{-2k} - O(q^{-3k})$) ist dies gleich

$$e^{-1/k}(1 - \frac{1}{2k}q^{-k} + \frac{1}{6k}q^{-2k} + \frac{1}{2}(\frac{-1}{2k}q^{-k})^2 + O(q^{-3k})) = e^{-1/k}(1 - \frac{1}{2k}q^{-k} + \frac{4k+3}{24k^2}q^{-2k} + O(q^{-3k}))$$

Zu (iii): Nach dem Lemma gilt

$$\begin{aligned} (G(q^k,1)^{-\frac{d-1}{k}}) &= \exp\left(\frac{1}{k}(d-1)(q^{-k} + \frac{3}{2}q^{-2k} + \frac{4}{3}x^{-3k} + O(x^{-4k}))\right) \\ &= \exp(\frac{1}{k}(q^{-d} - O(q^{-d-1}))) = 1 + \frac{1}{k}q^{-d} + O(q^{-(d+1)}). \end{aligned}$$

Zu (iv): Wir verwenden

$$G(q^{4k};q^{2k}) = \prod_{i=1}^{\infty}(1 - q^{-4ki}q^{2k}) = \prod_{i=1}^{\infty}(1 - q^{-2k(2i-1)}) = \frac{G(q^{2k};1)}{G(q^{4k};1)}.$$

Damit erhalten wir

$$G(q^{4k};q^{2k})^{q^k/k} = \exp\left(-\frac{q^k}{k}(q^{-2k}+O(q^{-4k}))+\frac{q^k}{k}(q^{-4k}+O(q^{-8k}))\right) = 1-\frac{1}{k}q^{-k}+O(q^{-2k}).$$

Für (v) vergleiche den Beweis zu (ii).

Zu (vi): Wir verfahren ähnlich wie im letzten Lemma. Der Wert $G(-q^k,-1)$ ist für alle $k \geq 2$ reell und positiv. Damit können wir Logarithmus und Exponentialfunktion anwenden.

$$\begin{aligned} G(-q^k,-1) &= \exp\left(\sum_{i=1}^{\infty}\log(1-(-1)^{i-1}q^{-ik})\right) \\ &= \exp\left(-\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\frac{1}{j}(-1)^{j(i-1)}q^{-ijk}\right) \\ &= \exp\left(-\frac{1}{k}+\frac{1}{2k}q^{-k}+O(q^{-2k})\right) \\ &= e^{-\frac{1}{k}}\left(1+\frac{1}{2k}q^{-k}+O(q^{-2k})\right). \end{aligned}$$

Damit folgt mit (ii) aus dem Lemma

$$G(-q^k;-1)^{\frac{q^k}{k}} = e^{-1/k}(1-O(q^{-k})).$$

Zu (vii): Mit $\log(1-q^{-ki}) > \frac{-q^{-ik}}{1-q^{-ik}} = -\frac{1}{q^{-ik}-1}$ für alle $i \geq 1$ erhalten wir

$$\log G(q^k;1) = \sum_{i=1}^{\infty}\log(1-q^{-ki}) \geq \sum_{i=1}^{\infty}-\frac{1}{q^{-ik}-1} = -\frac{q^k}{(q^k-1)^2}.$$

□

Kapitel 3

Generelle Lineare Gruppen

In diesem Kapitel wollen wir unsere gewonnenen Erkenntnisse nutzen, um die Proportion b-satter Matrizen in der Generellen Linearen Gruppe zu berechnen. Wir gehen in der bereits angedeuteten Strategie von Neumann und Praeger vor.

3.1 Die Operation auf b-Haupträumen

Seien $b, n \in \mathbb{N}$ mit $b < n$. Wir betrachten die Gruppe $GL(n,q)$ über dem Körper $K := \mathbb{F}_q$ und deren natürliche Operation auf dem n-dimensionalen K-Vektorraum $V := K^n$. Man siehe auch Tabelle 1.

Wir können $GL(n,q)$ in die b-Äquivalenzklassen der b-Äquivalenz (s. Definition 2.38) aufteilen. Im Folgenden wollen wir die Kardinalitäten der Klassen berechen.

Dafür werden wir verwenden, dass jede Matrix konjugiert zu einer Matrix mit „schöner“ Hauptraumzerlegung (bzw. Blockdiagonalgestalt) ist. Die Anzahl der Matrizen in $GL(n,q)$ mit gleicher Hauptraumzerlegung bzw. b-Hauptraumzerlegung (siehe Def. 3.1) lässt sich dann als Produkt berechnen. Die Faktoren sind dann die Anzahl von Matrizen kleinerer Dimension, mit charakteristischem Polynom $f(x)$, das nur einen irreduziblen Teiler $p(x)$ besitzt. Deren Anzahl haben wir bereits in Abschnitt 2.3 berechnet. Wir erhalten eine nützliche Summenformel von Proportionen, siehe Satz 3.10, und eine Gleichung für Potenzreihen, siehe Satz 3.11.

Die b-satten Matrizen bilden eine Äquivalenzklasse. Außerdem kommt, wie wir noch sehen werden, in der Proportion jeder Äquivanzklasse als Faktor die Proportion der b-satten Matrizen vom Grad n_0 vor, wobei n_0 der Grad der b-satten Anteile der Matrizen aus der Äquivalenzrelation ist. Wir wiederholen die Erkenntnisse des Lemmas 2.36:

$$g \in GL(n,q) \quad \Rightarrow \quad V = V_0 \oplus V_{\leq b},\ n_0 := \dim V_0,\ n_{\leq b} := \dim V_{\leq b} \qquad \text{(I)}$$
$$\text{mit } g_{|_{V_0}}\ b-\text{satt und } n_{\leq b} = \deg\left(ggT(\chi_g, \Psi_b)\right).$$

Ψ_b war als Polynom definiert als das Produkt über alle $(x-\lambda)^n$ für alle nicht-b-sättigenden $\lambda \in \bar{\mathbb{F}}_q$.

Sei $g \in GL(n,q)$. Wir können dann den Vektorraum in die Haupträume zerlegen. Seien p_1, ..., $p_l \in \mathbb{F}_q[x]$ die irreduziblen Teiler des charakteristischen Polynoms von g. Die Hauptraumzerlegung ist

$$V = \bigoplus_{i=1}^{l} H(p_i)$$

mit den Haupträmen $H(p_i) := Kern(p_i(g)^n) = Kern(p_i(g)^{e_i})$, wobei e_i die geometrische Vielfachheit ist, also die maximale Potenz, mit der p_i das charakteristische Polynom teilt.

Wenn wir außerdem $V = V_0 \oplus V_{\leq b}$ wie in der Gleichung 2.36 zerlegen, dann ist V_0 offensichtlich die Summe aller Haupträume von b-sättigenden Polynomen. Da es uns nicht interessiert, wie sich g auf V_0 verhält, solange es b-satt ist, ist es sinnvoll, die Haupträume zu V_0 zusammenzufassen. Dies führt uns zur folgenden Definition.

Definition 3.1 *Sei $g \in GL(n,q)$. Dann lässt sich V zerlegen in*

$$V = V_0 \oplus \bigoplus H(p_i) \ ,$$

wobei V_0 wie in (I) so gewählt ist, dass die Einschränkung von g b-satt ist und die Summe über alle irreduziblen Teiler p_i des charakteristischen Polynoms von g, die nicht-b-satt sind, summiert (d.h. es gilt $V_{\leq b} = \bigoplus H(p_i)$). So eine Zerlegung nennen wir b-Hauptraumzerlegung. *Die Teilräume $H(p_i)$ und V_0 heißen* b-Haupträume, *V_0 der* satte b-Hauptraum.

Wir bezeichnen $H(\lambda) := H(p)$, wo p das Minimalpolynom von λ ist, falls λ ein nicht-b-sättigender Eigenwert von g ist, und $H(\lambda) := \{0\}$, falls λ nicht-b-sättigend ist, aber kein Eigenwert von g.

Ein nicht-satter b-Hauptraum ist gegeben durch $H(\lambda)$, wobei λ ein nicht-b-sättigender Eigenwert ist. Gleichzeitig definiert jeder Galois-Konjugierte von λ in der Körpererweiterung $\mathbb{F}_q[\lambda]/\mathbb{F}_q$ den gleichen Hauptraum, es gilt also

$$H(\lambda) = H(\lambda^{q^i})$$

füer alle $i \geq 0$. Wir müssen ein Vertretersystem definieren, in dem nur ein Galois-Konjugierter vorkommt.

Definition 3.2 *Sei $k \leq b$.*

- *Definiere*
$$i_q(k) := |\{\lambda \in \mathbb{F}_{q^k} \mid \lambda = 0 \text{ oder } \mathbb{F}_q[\lambda] \neq \mathbb{F}_{q^k} \}|$$
als die Anzahl aller nicht-primitiven Elemente. *$i_q(k)$ kann über eine Siebformel berechnet werden.*

- *Weiterhin definieren wir eine Vertretermenge der primitiven Elemente. Sei* Frob : $\mathbb{F}_{q^k} \to \mathbb{F}_{q^k}$, $x \mapsto x^q$ *der (Standard-)Frobeniusautomorphismus. Θ_k sei eine Vertretermenge der Bahnen der Operation des Frobeniusautomorphismus auf der Menge der primitiven Elemente von $\mathbb{F}_{q^k}$, d.h.*
$$\sum_{i=0}^{k-1} \Theta_k^{q^i} = \mathbb{F}_{q^k} \setminus \bigcup_{l|k,\ l<k} \mathbb{F}_{q^k}, \quad \Theta_k^{q^i} := \{\lambda_k^{q^i} \mid \lambda_k \in \Theta_k\}.$$

- *Zur Abkürzung definieren wir*
$$\Theta := \bigcup_{k=1}^{b} \Theta_k.$$

Bemerkung 3.3 *Die Kardinalität von Θ_k ist*

$$|\Theta_k| = \frac{q^k - i_q(k)}{k}.$$

Dies ist auch die Anzahl aller normierten, irreduziblen Polynome vom Grad k, häufig auch mit $I_k(q)$ bezeichnet. Hervorheben wollen wir, dass das Polynom $|\Theta_k|(q) \in \mathbb{Q}[q]$ den Grad k hat.

Für kleine k sind die Kardinalitäten der $|\Theta_k|$ gegeben durch

k	$\lvert\Theta_k\rvert$
1	$q-1$
2	$\frac{q^2-q}{2}$
3	$\frac{q^3-q}{3}$
4	$\frac{q^4-q^2}{4}$
5	$\frac{q^5-q}{5}$
6	$\frac{q^6-q^3-q^2+q}{6}$
7	$\frac{q^7-q}{7}$
8	$\frac{q^8-q^4}{8}$
9	$\frac{q^9-q^3}{9}$
10	$\frac{q^{10}-q^5-q^2+q}{10}$
11	$\frac{q^{11}-q}{11}$
12	$\frac{q^{12}-q^6-q^4+q^2}{12}$

Nun wollen wir die b-Hauptraumzerlegung genauer betrachten und den Zusammenhang zur b-Äquivalenz untersuchen. Eine b-Hauptraumzerlegung ist eine Zerlegung von V in maximal $1+|\Theta|$ b-Haupträume.

Definition 3.4

- *Wir definieren eine Menge von $(1+|\Theta|)$-Tupeln von Untervektorräumen, deren Einträge als direkte Summe eine Zerlegung von V bilden.*

$$\mathcal{M} := \{(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1},\ \dots,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b})\ \mid V_0, V_{\lambda_i} \leq V,\ \ V\ =\ V_0\ \oplus\ \bigoplus_{\lambda\in\Theta} V_\lambda\}$$

- *Die Abbildung, die jedes Tupel von Untervektorräumen auf das Tupel der Dimensionen schickt, sei*

$$\dim : \mathcal{M}\ \to\ \mathbb{N}^{1+|\Theta|},\ (V_0,\ (V_\lambda)_{\lambda\in\Theta})\ \mapsto\ (\dim(V_0),\ (\dim(V_\lambda))_{\lambda\in\Theta})\,.$$

- *Außerdem definieren wir die Abbildung, die jeder Matrix ihre b-Hauptraumzerlegung beziehungsweise das Tupel der b-Hauptraumzerlegung zuweist:*

$$\pi : GL(n,q)\ \to\ \mathcal{M},\ g \mapsto\ (V_0,\ (H(\lambda))_{\lambda\in\Theta})$$

mit V_0 dem satten b-Hauptraum und den anderen b-Haupträumen $H(\lambda)$ für Eigenwerte von g. Ist λ kein Eigenwert von g, so haben wir $H(\lambda) := \{0\}$ definiert.

Es ist ein direkter Zusammenhang zwischen $\mathcal{M}$ und der b-Äquivalenz gegeben.

Lemma 3.5 *Für $g, h \in GL(n,q)$ gilt:*

$$g \sim_b h\ \Leftrightarrow \dim(\pi(g)) = \dim(\pi(h)).$$

Beweis: Nach Gleichung (I) können wir V bezüglich g in $V = V_0 \oplus V_{\leq b}$ und bezüglich h in $V = V_0' \oplus V_{\leq b}'$ zerlegen, sodass g eingeschränkt auf V_0 und h eingeschränkt auf V_0' b-satt sind und g auf $V_{\leq b}$ und h auf $V_{\leq b}'$ keine b-sättigenden Eigenwerte haben.

Angenommen, es gilt $g \sim_b h$, das heißt $ggT(\chi_g, \Psi_b) = ggT(\chi_h, \Psi_b)$. Damit gilt $\dim V_0 = \dim V_0'$ und g und h haben die selben nicht-b-sättigenden Eigenwerte. Außerdem haben diese jeweils die selben geometrischen Vielfachheiten, also die Potenz, mit der das Minimalpolynom

eines Eigenwerts die charakteristischen Polynome von g und h teilt. Die Dimensionen der b-Haupträume sind gleich und somit $\dim(\pi(g)) = \dim(\pi(h))$.

Gilt andererseits $\dim(\pi(g)) = \dim(\pi(h))$, so haben g und h wiederum die selben nicht-b-sättigenden Eigenwerte mit den selben geometrischen Vielfachheiten. Damit gilt $ggT(\chi_g, \Psi_b) = ggT(\chi_h, \Psi_b)$ und somit $g \sim_b h$. □

Die natürliche Operation von $GL(n,q)$ auf $\mathcal{M}$ erhält die b-Äquivalenzklassen. Dies liefert uns das folgende Lemma.

Lemma 3.6 *$GL(n,q)$ operiere auf $\mathcal{M}$ komponentenweise, also via*

$$g \cdot (V_0, (V_\lambda)\lambda \in \Theta) \ := \ (gV_0, (gV_\lambda)\lambda \in \Theta).$$

Dann trennt dim *die Bahnen und ist somit eine trennende Invariante. Für $g, h \in GL(n,q)$ gilt*

$$g \sim_b h \ \Leftrightarrow \pi(g) \in GL(n,q) \cdot \pi(h).$$

Beweis: Die natürliche Operation von $GL(n,q)$ auf V bildet Zerlegungen auf Zerlegungen ab. Auf Untervektorräumen gleicher Dimension operiert $GL(n,q)$ transitiv, also ist dim eine trennende Invariante. Die zweite Aussage folgt sofort mit dem letzten Lemma. □

Ist $g \in GL(n,q)$, so ist die Kardinalität der b-Äquivalenzklasse von g das Produkt der Bahnenlänge von $\pi(g)$ und der Anzahl der Elemente, die die gleiche b-Hauptraumzerlegung haben wie g. Anders ausgedrückt gilt

$$|[g]_{\sim_b}| \ = \ |\ GL(n,q) \cdot \pi(g)| \cdot |\pi^{-1}(\pi(g))|. \qquad \text{(II)}$$

Diese beiden Faktoren wollen wir ermitteln. Zunächst ist es noch hilfreich, die Bilder von π und $\dim \pi$ zu bestimmen.

Bemerkung 3.7

- $(V_0,\ (V_\lambda)_{\lambda\in\Theta}) \in \mathcal{M}$ *ist genau dann im Bild von π, wenn* $\dim V_0 = 0$ *oder* $\dim V_0 > b$. *Und für alle $\lambda \in \Theta$ gilt $k | \dim V_\lambda$, wobei $k := [\mathbb{F}_q[\lambda] : \mathbb{F}_q]$.*

- $(N_0,\ (N_\lambda)_{\lambda\in\Theta}) \in \mathbb{N}^{1+|\Theta|}$ *liegt andererseits genau dann im Bild von* $\dim \pi$, *wenn ein Element des Bildes von π darauf abgebildet wird. Also genau dann, wenn $N_0 + \sum N_\lambda = n$, also wenn $(N_0,\ (N_\lambda)_{\lambda\in\Theta})$ eine Partition von n ist, außerdem $N_0 = 0$ oder $N_0 > b$ gilt und für alle $\lambda \in \Theta$ gilt $k | N_\lambda$, wobei $k := [\mathbb{F}_q[\lambda] : \mathbb{F}_q]$. $(N_0,\ (N_\lambda)_{\lambda\in\Theta})$ hat also die Form*

$$(n_0,\ (n_{\lambda_1})_{\lambda_1\in\Theta_1},\ (2n_{\lambda_2})_{\lambda_2\in\Theta_2}, ...,\ (bn_{\lambda_b})_{\lambda_b\in\Theta_b}).$$

Wir bestimmen den ersten Faktor in Gleichung (II), der Stabilisator eines Tupels von Untervektorräumen, die V zerlegen.

Lemma 3.8 *Sei $(V_0,\ (V_\lambda)_{\lambda\in\Theta}) \in \mathcal{M}$ mit Dimension* $\dim((V_0,\ (V_\lambda)_{\lambda\in\Theta})) =: (n_0,\ (n_\lambda)_{\lambda\in\Theta})$.
Dann gilt für den Stabilisator

$$Stab_{GL(n,q)}((V_0,\ (V_\lambda)_{\lambda\in\Theta})) \ \cong \ GL(n_0,q) \times \prod_{\lambda\in\Theta} GL(n_\lambda, q).$$

($GL(0,q) := \{1\}$.)

Beweis: Sei $g \in GL(n,q)$. Für $\lambda \in \Theta \cup \{0\}$ sei B_λ eine Basis von V_λ. Dann ist $B := \bigcup_\lambda B_\lambda$ eine Basis von V. g stabilisiert genau dann $(V_0,\ (V_\lambda)_{\lambda\in\Theta})$, wenn für alle $\lambda \in \Theta$ auch $g(B_\lambda)$ eine Basis für V_λ ist. Also genau dann, wenn g bezüglich B eine Blockdiagonalmatrix ist. Jeder Block

entspricht $g_{|V_\lambda}$ bezüglich der Basis B_λ. Damit ist der Grad des Blocks gleich $\dim V_\lambda = n_\lambda$. Der Homomorphismus

$$g \mapsto \left(g_{|V_0}, (g_{|V_\lambda})_{\lambda\in\Theta}\right)$$

ist dann bijektiv auf

$$GL(n,q) \to GL(n_0,q) \times \prod_{\lambda\in\Theta} GL(n_\lambda, q).$$

□

Das folgende Lemma liefert den zweiten Faktor von (II).

Lemma 3.9 *Sei* $(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1}, ...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b}) \in \mathcal{M}$ *mit Dimension*

$$\dim\left((V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1}, ...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b})\right) =: (n_0,\ (n_{\lambda_1})_{\lambda_1\in\Theta_1},\ (2n_{\lambda_2})_{\lambda_2\in\Theta_2}, ...,\ (bn_{\lambda_b})_{\lambda_b\in\Theta_b})$$

im Bild von π.

Dann ist die Kardinalität des Urbildes $\pi^{-1}((V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1}, ...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b}))$ *gleich*

$$v^b(GL(n_0,q))|GL(n_0,q)| \cdot \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k} u(GL(n_{\lambda_k}, q^k))|GL(k\cdot n_{\lambda_k}, q)|\ ,$$

wobei $v^b(GL(n_0,q))$ *die Proportion b-satter Elemente der* $GL(n_0,q)$ *und* $u(GL(n_{\lambda_k},q^k))$ *die Proportion unipotenter Elemente der* $GL(n_{\lambda_k},q^k)$ *sind, siehe Definitionen* 1.2 *bzw.* 2.45.

Beweis: Wir schreiben $(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1}, ...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b})$ auch als $(V_0,\ (V_\lambda)_{\lambda\in\Theta})$. Nach Bemerkung 3.7 liegt $(V_0,\ (V_\lambda)_{\lambda\in\Theta})$ im Bild von π. Sei $g \in GL(n,q)$ im Urbild. Dann ist das charakteristische Polynom von g gegeben durch

$$\chi_g(x) = f_0(x) \prod_{\lambda\in\Theta} \mu_\lambda(x)^{n_\lambda},$$

wobei μ_λ jeweils das Minimalpoynom von λ über $\mathbb{F}_q$ und $f_0 \in \mathbb{F}_q[x]$ ein b-sattes Polynom ist. V_0 und die V_λ sind $g-$invariante Untervektorräume, die V zerlegen. g ist also durch das Abbildungsverhalten auf V_0 und den V_λ festgelegt. Die Abbildung

$$g \mapsto \left(g_{|V_0},\ (g_{|V_{\lambda_1}})_{\lambda\in\Theta_1}, ...,\ (g_{|V_{\lambda_b}})_{\lambda_b\in\Theta_b},\right)$$

soll dann eine Bijektion liefern.

Wir bestimmen das Bild. Der b-satte Anteil $g_{|V_0} \in GL(n_0,q)$ liegt in

$$g_{|V_0} \in S^b(GL(n_0,q)).$$

($S^b(GL(n_0,q))$ ist die Menge der b-satten Elemente der $GL(n_0,q)$, siehe Definition 1.2.)

Für $k \in \{1, ..., b\}$ ist $g_{|V_{\lambda_k}} \in GL(kn_{\lambda_k}, q)$. Das charakteristische Polynom der Einschränkung ist $\mu_{\lambda_k}(x)^{n_{\lambda_k}}$. Damit gilt

$$g_{|V_{\lambda_k}} \in \mathcal{X}(\mu_{\lambda_k}(x)^{n_{\lambda_k}}).$$

($\mathcal{X}(\mu_{\lambda_k}(x)^{n_{\lambda_k}})$ bezeichnet hier die Menge der Elemente der $GL(kn_{\lambda_k},q)$, die charakteristisches Polynom $\mu_{\lambda_k}(x)^{n_{\lambda_k}}$ haben, siehe Definition 2.44.)

Umgekehrt haben alle Elemente von $GL(n,q)$, die auf V_0 und allen V_λ diese Gestalt haben, die b-Hauptraumzerlegung

$$V = V_0 \oplus \bigoplus_{\lambda\in\Theta} V_\lambda.$$

Sie werden von π also auf $(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1},...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b})$ abgebildet.

Damit ist also $\pi^{-1}((V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1},...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b}))$ bijektiv zum kartesischen Produkt

$$S^b(GL(n_0,q)) \times \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k} \mathcal{X}\left(\mu_{\lambda_k}(x)^{n_{\lambda_k}}\right).$$

Die Kardinalitäten der zweiten Mengen sind bekannt. Mit

$$|S^b(GL(n_0,q))| = v^b(GL(n_0,q))|GL(n_0,q)| \quad (\text{ s. Definition 1.2})$$

und

$$|\mathcal{X}\left(\mu_{\lambda_k}(x)^{n_{\lambda_k}}\right)| = u\left(GL(n_{\lambda_k},q^k)\right)|GL(k\cdot n_{\lambda_k},q)| \ (\text{ s. Folgerung 2.49})$$

folgt die Behauptung. □

Jetzt haben wir die Kardinalität einer beliebigen b-Äquivalenzklasse bestimmt. Wir können also über alle Äquivalenzklassen summieren und damit eine Gleichung für die $v^b_{n_0}$ finden, $n_0 \in \{0, b+1, b+2, ..., n\}$.

Satz 3.10 *Es gilt*

$$1 = \sum_{\mathfrak{p}\in\ \dim\pi(GL(n,q))} v^b(GL(n_0,q)) \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k} u(GL(n_{\lambda_k},q^k)).$$

Wir summieren über alle Partitionen von n der Form

$$\mathfrak{p} = (n_0,\ (n_{\lambda_1})_{\lambda_1\in\Theta_1},\ (2n_{\lambda_2})_{\lambda_2\in\Theta_2},...,\ (bn_{\lambda_b})_{\lambda_b\in\Theta_b}),$$

wobei $n_0 = 0$ oder $n_0 > b$ und $n_{\lambda_k} \geq 0$ für $\lambda_k \in \Theta_k$ und $k = 1, ..., b$ gelten.

Θ_k ist eine Vertretermenge der primitiven Elemente der Körpererweiterung $\mathbb{F}_{q^k}/\mathbb{F}_q$ bezüglich der Operation der Galois-Gruppe (siehe Definition 3.2), $v^b(GL(n_0,q))$ ist die Proportion b-satter Matrizen in $GL(n_o,q)$ (siehe Definition 1.2) und $u(GL(n_{\lambda_k},q^k))$ ist die Proportion unipotenter Matrizen in $GL(n_{\lambda_k},q^k)$ (siehe Definition 2.45).

Beweis: Gleichung II liefert für alle $g \in GL(n,q)$

$$|[g]_{\sim_b}| \ = \ |\ GL(n,q)\cdot\pi(g)|\cdot|\pi^{-1}(\pi(g))|.$$

Sei $g \in GL(n,q)$ mit

$$(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1},...,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b}) := \pi(g)$$

und

$$\dim\pi(g) =: (n_0,\ (n_{\lambda_1})_{\lambda_1\in\Theta_1},\ (2n_{\lambda_2})_{\lambda_2\in\Theta_2},...,\ (bn_{\lambda_b})_{\lambda_b\in\Theta_b}).$$

Nach Lemma 3.8 ist die Bahnenlänge gegeben durch

$$\frac{|GL(n,q)|}{|GL(n_0,q)|\cdot\ \prod_{k=1}^{b}\ \prod_{\lambda_k\in\Theta_k}|GL(kn_{\lambda_k},q)|}.$$

Lemma 3.9 liefert

$$|\pi^{-1}(\pi(g))| = v^b(GL(n_0,q))|GL(n_0,q)|\cdot\ \prod_{k=1}^{b}\ \prod_{\lambda_k\in\Theta_k} u(GL(n_{\lambda_k},q^k))|GL(k\cdot n_{\lambda_k},q)|.$$

Kürzen mit $|GL(n,q)|$ liefert dann die Proportion

$$\frac{|[g]_{\sim_b}|}{|GL(n,q)|} \;=\; v^b(GL(n_0,q)) \cdot \prod_{k=1}^{b} \prod_{\lambda_k \in \Theta_k} u(GL(n_{\lambda_k}, q^k)).$$

Wir können nun über alle b-Äquivalenzklassen summieren, also über ein Transversale der b-Äquivalenz. Die Abbildung $\dim \circ \pi$ trennt nach Lemma 3.5 die b-Äquivalenzklassen. Wir können somit über das Bild von $\dim \circ \pi$ summieren. Dies sind aber genau die Partitionen der Form $\mathfrak{p}$, wie sie im Satz angegeben sind. □

Die im Satz bewiesene Identität werden wir jetzt verwenden. Wir wollen eine Variable z^n einfügen, die in der Gleichung des Satzes vorkommenden Proportionen als Koeffizienten ihrer erzeugenden Potenzreihen auffassen und über alle Dimensionen n summieren. Auf der einen Seite erhalten wir dann die geometrische Reihe $\sum_{n=0}^{\infty} z^n \;=\; \frac{1}{1-z}$ und auf der anderen ein Produkt von $V^b(z)$ und verschiedener unipotenter Potenzreihen, also Euler'scher Funktionen (s. Satz 2.52(i)). $V^b(z)$ ist die erzeugende Funktion der Proportionen der b-satten Matrizen (s. b-satte Potenzreihe, Definition 1.4).

Satz 3.11 *Es gilt*

$$(1-z)^{-1} \;=\; V^b(GL,q;z)\; U(GL,q;z)^{q-1} \prod_{k=2}^{b} U(GL,q^k;z^k)^{(q^k - i_q(k))/k}.$$

Beweis: In der im letzten Satz gegebene Gleichung multiplizieren wir mit z^n und summieren über n auf beiden Seiten, n läuft von Null bis Unendlich. Wir erhalten

$$(1-z)^{-1} = \sum_{n=0}^{\infty} \sum_{\mathfrak{p}} v_{n_0}^2 \prod_{k=1}^{b} \prod_{\lambda_k \in \Theta_k} u(GL(n_{\lambda_k}, q^k)) \cdot z^n$$

für z betragsmäßig kleiner als 1. Die Summe läuft über alle Partitionen

$$\mathfrak{p} = (n_0,\; (n_{\lambda_1})_{\lambda_1 \in \Theta_1},\; (2n_{\lambda_2})_{\lambda_2 \in \Theta_2}, ...,\; (bn_{\lambda_b})_{\lambda_b \in \Theta_b}) \in \dim \pi(GL(n,q)).$$

Unter Ausnutzung von $n = n_0 + \sum_{k=1}^{b} \sum_{\lambda_k} k \cdot n_{\lambda_k}$ erhalten wir für die rechte Seite

$$\sum_{n=0}^{\infty} \sum_{\mathfrak{p}} v_{n_0}^2 z^{n_0} \prod_{k=1}^{b} \prod_{\lambda_k \in \Theta_k} u(GL(n_{\lambda_k}, q^k)) z^{k n_{\lambda_k}}$$

$$= V^b(GL,q;z) \prod_{k=1}^{b} U(GL,q^k;z^k)^{|\Theta_k|}.$$

Man beachte, dass wir $v^b(GL(0,q)) = u(GL(0,q^k)) = 1$ definierten und dass $v^b(GL(n,q)) = 0$ für alle $1 \le n \le b$ gilt. Mit $|\Theta_k| = \frac{q^k - i_q(k)}{k}$ (siehe Definition 3.2) folgt die Behauptung.

□

Wir wollen die b-satte Potenzreihe weiter untersuchen. Zuerst betrachten wir als Spezialfall die Proportion 2-satter Matrizen. Für diese können wir bessere Aussagen treffen, als für eine allgemeine Schranke b. Die Proportionen b-satter Matrizen (b beliebig) behandeln wir im darauf folgendem Abschnitt.

3.2 Proportionen 2-satter Matrizen

In diesem Abschnitt ist $b = 2$. Die in Satz 3.11 bewiesene Gleichung für Potenzreihen lautet in diesem Fall

$$V^2(z) = (1-z)^{-1}U(GL, q^2; z^2)^{-(q^2-q)/2}\ U(GL, q; z)^{-(q-1)}. \tag{III}$$

Wir nutzen, dass wir in Satz 2.49 gezeigt haben, dass die unipotente Potenzreihe gerade die Inverse der Euler'schen Funktion ist. Genauer gilt

$$U(GL, q; z)^{-1} = G(q; z) \text{ und damit } U(GL, q^2; z^2)^{-1} = G(q^2; z^2).$$

Also gilt für die 2-satte Potenzreihe

$$V^2(z) = (1-z)^{-1}\ G(q, z)^{(q-1)}\ G(q^2, z^2)^{(q^2-q)/2}. \tag{IV}$$

Satz 3.12 *Die Folge* $(v^2(GL(n, q)))_{n\in\mathbb{N}}$ *konvergiert gegen*

$$v^2(GL, \infty, q) = G(q, 1)^{q-1}G(q^2, 1)^{(q^2-q)/2}.$$

Beweis: Definiere $f(z) := G(q, z)^{q-1}G(q^2, z^2)^{(q^2-q)/2}$. f ist eine ganze Funktion nach Lemma 2.51. Die Taylorentwicklung hat die Form $f(z) = \sum_{n=0}^{\infty}(-1)^n a_n z^n$, $a_n := |\frac{f^{(n)}(0)}{n!}|$ (die Taylorkoeffizienten alternieren, siehe Lemma 2.53), also gilt

$$(1-z)^{-1}f(z) = \sum_{n=0}^{\infty}\sum_{i=0}^{n}(-1)^i a_i z^n.$$

Der n-te Koeffizient von $V^2(z)$ ist v_n^2. Ein Koeffizientenvergleich ergibt $v_n^2 = \sum_{i=0}^{n}(-1)^i a_i$, also gilt

$$v^2(GL, \infty, q) = \sum_{n=0}^{\infty}(-1)^n a_n = f(1).$$

□

Wir suchen nun eine Näherung für $v^2(GL, \infty, q) = G(q, 1)^{q-1}G(q^2, 1)^{(q^2-q)/2}$. Dafür teilen wir $G(q^2, 1)^{(q^2-q)/2}$ in $G(q^2, 1)^{(q^2-1)/2}$ und $G(q^2, 1)^{-(q-1)/2}$ auf. In Satz 2.55 haben wir diese Werte schon berechnet.

Satz 3.13 *Es gilt* $v^2(GL; \infty, q) = e^{-3/2}\ (1 - \frac{7}{12}q^{-2} + \frac{1}{3}q^{-3} + \frac{77}{1440}q^{-4} + O(q^{-5}))$.

Beweis: Mit Satz 2.55 gilt

$$v^2(GL; \infty, q) = G(q^2, 1)^{(q^2-1)/2}G(q^2, 1)^{-(q-1)/2}G(q, 1)^{q-1}$$

$$= e^{-1/2}(1 - \frac{1}{4}q^{-2} + \frac{11}{96}q^{-4} + O(q^{-6})) \cdot (1 + \frac{1}{2}q^{-1} - \frac{3}{8}q^{-2} + \frac{25}{48}q^{-3} - \frac{119}{384}q^{-4} + O(q^{-5}))\cdot$$
$$e^{-1}(1 - \frac{1}{2}q^{-1} + \frac{7}{24}q^{-2} - \frac{25}{48}q^{-3} + \frac{4583}{5760}q^{-4} + O(q^{-5}))$$
$$= e^{-1-1/2}(1 - \frac{7}{12}q^{-2} + \frac{1}{3}q^{-3} + \frac{77}{1440}q^{-4} + O(q^{-5})).$$

□

Das Ergebnis des letzten Satzes war das Ziel dieses Abschnitts. Jetzt wollen wir ähnliche Resultate auch für beliebige $b \in \mathbb{N}$ finden. Die zwei Sätze lassen sich übertragen, Produkte, Summen und vor allem Abschätzungen werden nur komplizierter und einige Schritte der beiden Sätze deutlich schwieriger.

3.3 Proportionen b-satter Matrizen

Satz 3.14 *Die Folge* $(v^b(GL(n,q)))_n$ *konvergiert gegen*

$$v^b(GL;\infty,q) = \prod_{k=1}^{b} G(q^k,1)^{(q^k-i_q(k))/k}.$$

Beweis: Mit Satz 3.11 und den Identitäten

$$U(GL,q;z) = G(q,z)^{-1} \text{ und damit } U(GL,q^k;z^k) = G(q^k,z^k)$$

(s. Satz 2.52) gilt

$$V^b(z) \;=\; (1-z)^{-1} \prod_{k=1}^{b} G(q^k,1)^{(q^k-i_q(k))/k}.$$

Definiere $f(z) := \prod_{k=1}^{b} G(q^k,z)^{(q^k-i_q(k))/k}$. Dann ist f nach 2.51 eine ganze Funktion und die Taylorentwicklung hat die Form $f(z) = \sum_{n=0}^{\infty}(-1)^n a_n z^n$, $a_n := |\frac{f^{(n)}(0)}{n!}|$ (die Taylorkoeffizienten alternieren, s. Lemma 2.53), also gilt

$$(1-z)^{-1}f(z) = \sum_{n=0}^{\infty}\sum_{i=0}^{n}(-1)^i a_i z^n.$$

Der n-te Koeffizient von $V^b(z)$ ist v_n^b. Ein Koeffizientenvergleich ergibt $v_n^b = \sum_{i=0}^{n}(-1)^i a_i$, also gilt

$$v^b(GL,\infty,q) = \sum_{n=0}^{\infty}(-1)^n a_n = f(1).$$

□

Der folgende Satz gibt nun das wichtigste Resultat dieser Arbeit an.

Satz 3.15 *Die Proportion b-satter Matrizen ist circa* $e^{-\sum_{k=1}^{b}\frac{1}{k}}$ *und genauer gilt*

$$v^b(GL,\infty,q) = e^{-\sum_{k=1}^{b}1/k}(1+O(q^{-1})).$$

Beweis: Für $b=1$ siehe [7].

$v^b(GL,\infty,q)$ war das Hauptresultat des letzten Abschnitts, siehe Satz 3.13.

Der letzte Satz lieferte

$$v^b(GL;\infty,q) = \prod_{k=2}^{b} G(q^k,1)^{(q^k-i_q(k))/k} \;\cdot\; G(q,1)^{q-1} = v^{b-1}(GL,\infty,q)G(q^b,1)^{(q^b-p_b(q))/b}$$

Den letzten Faktor können wir aufteilen in

$$G(q^b,1)^{(q^b-i_q(b))/b} = G(q^b,1)^{(q^b-1)/b}\cdot G(q^b,1)^{-(i_q(b)-1)/b}.$$

Für diese Werte haben wir in Kapitel 2, Satz 2.55, bereits Näherungen angegeben. Für $b=3$ liefern diese

$$v^3(GL;\infty,q) = \underbrace{e^{-3/2}\;(1-\frac{7}{12}q^{-2}+\frac{1}{3}q^{-3}+\frac{77}{1440}q^{-4}+O(q^{-5}))}_{=v^2(GL;\infty,q)}\cdot$$

$$\underbrace{e^{-1/3}(1-\frac{1}{6}q^{-3}+O(q^{-6}))}_{=G(q^3,1)^{(q^3-1)/3}}\cdot\underbrace{(1+\frac{1}{3}q^{-2}-\frac{1}{3}q^{-3}+\frac{1}{18}q^{-4}+O(q^{-5}))}_{=G(q^3,1)^{-(q-1)/3}}$$

$$= e^{-11/6}\ (1 - \frac{1}{4}q^{-2} + \frac{1}{6}q^{-3} + \frac{41}{480}q^{-4} + O(q^{-5}))$$

Allgemein gilt für $b \geq 2$ mit Satz 2.55

$$G(q^b,1)^{\frac{q^b - q^{b/p}}{b}} = e^{-1/b}(1 + \frac{1}{2b}q^{-b} + O(q^{-2b}))(1 + \frac{1}{b}q^{-d} + O(q^{-d-1}))$$

wobei p die kleinste Primzahl, die b teilt, und $d = b - b/p$, also „k minus den größten Teiler von k“, seien. Nun ist $deg(i_q(b)) = b/p$ und damit gilt auch

$$G(q^b,1)^{\frac{q^b - i_q(b)}{b}} = e^{-1/b}(1 + \frac{1}{2b}q^{-b} + O(q^{-2b}))(1 + \frac{1}{b}q^{-d} + O(q^{-d-1})).$$

Insbesondere gilt $d \geq 2$ und damit weicht $G(q^b,1)^{(q^b - i_q(b))/b}$ mit einem von q abhängigen Fehler von $e^{-1/b}$ ab. Mit der oben schon erwähnten Rekursionsgleichung haben wir dann den Limes der Proportionen, $v^b(GL,\infty,q)$, berechnet:

$$v^b(GL,\infty,q) = e^{-\sum_{k=1}^{b} 1/k}(1 + O(q^{-1})).$$

□

Für kleine Schranken b können wir mit Maple genauerte Näherungen mit höheren Termen in q^{-1} angeben. Man siehe Anhang A für eine genauere Ausfürung.

b	$v^b(GL,\infty,q)$	
1	e^{-1}	$(1 - \frac{1}{2}q^{-1} + \frac{7}{24}q^{-2} - \frac{25}{48}q^{-3} + \frac{4583}{5760}q^{-4} - \frac{13907}{11520}q^{-5} + O(q^{-6}))$
2	$e^{-1-1/2}$	$(1 - \frac{7}{12}q^{-2} + \frac{1}{3}q^{-3} + \frac{77}{1440}q^{-4} - \frac{59}{180}q^{-5} + \frac{26371}{362880}q^{-6} + O(q^{-7})))$
3	$e^{-1-1/2-1/3}$	$(1 - \frac{1}{4}q^{-2} - \frac{1}{6}q^{-3} - \frac{41}{480}q^{-4} + \frac{49}{120}q^{-5} - \frac{17009}{40320}q^{-6} + O(q^{-7}))$
4	$e^{-1-\ldots-1/4}$	$(1 - \frac{1}{6}q^{-3} - \frac{59}{120}q^{-4} + \frac{11}{30}q^{-5} - \frac{37}{504}q^{-6} + \frac{1133}{5040}q^{-7} + O(q^{-8}))$
5	$e^{-1-\ldots-1/5}$	$(1 - \frac{1}{6}q^{-3} - \frac{7}{24}q^{-4} + \frac{1}{15}q^{-5} - \frac{37}{504}q^{-6} + \frac{193}{1008}q^{-7} + O(q^{-8}))$
6	$e^{-1-\ldots-1/6}$	$(1 - \frac{1}{8}q^{-4} - \frac{1}{10}q^{-5} - \frac{85}{252}q^{-6} + \frac{1}{7}q^{-7} - \frac{97}{1920}q^{-8} + O(q^{-9}))$
7	$e^{-1-\ldots1/7}$	$(1 - \frac{1}{8}q^{-4} - \frac{1}{10}q^{-5} - \frac{7}{36}q^{-6} - \frac{1}{14}q^{-7} - \frac{97}{1920}q^{-8} + O(q^{-9}))$
8	$e^{-1-\ldots-1/8}$	$(1 - \frac{1}{10}q^{-5} - \frac{7}{36}q^{-6} - \frac{1}{14}q^{-7} - \frac{59}{240}q^{-8} + O(q^{-9}))$
9	$e^{-1-\ldots-1/9}$	$(1 - \frac{1}{10}q^{-5} - \frac{1}{12}q^{-6} - \frac{1}{14}q^{-7} - \frac{59}{240}q^{-8} + O(q^{-9}))$
10	$e^{-1-\ldots-1/10}$	$(1 - \frac{1}{12}q^{-6} - \frac{1}{14}q^{-7} - \frac{7}{48}q^{-8} + O(q^{-9}))$
11	$e^{-1-\ldots-1/11}$	$(1 - \frac{1}{12}q^{-6} - \frac{1}{14}q^{-7} - \frac{7}{48}q^{-8} + O(q^{-9}))$
12	$e^{-1-\ldots-1/12}$	$(1 - \frac{1}{14}q^{-7} - \frac{1}{16}q^{-8} + O(q^{-9}))$

Man sieht, dass bei geraden b der nicht-konstante Term größten Grades verschwindet. Außerdem wissen wir wegen

$$G(q^k,1)^{\frac{q^k - i_q(k)}{k}} = e^{-1/b}(1 + \frac{1}{2b}q^{-b} + O(q^{-2b}))(1 + \frac{1}{b}q^{-d} + O(q^{-d-1}))$$

und $d \geq 2$ für $k > 2$, dass gilt

$$v^b(Gl\infty,q) = e^{-\sum_{k=1}^{b} 1/k}(1 + O(q^{-2})).$$

Denn für $b = 2$ ist dies richtig und für größere b enthalten die Faktoren $G(q^k,1)^{\frac{q^k - i_q(k)}{k}}$ mit $2 < k \leq b$ in der entwicklung nach q keinen Term vom Grad -1, sodass das Produkt $v^b(Gl\infty,q)$

auch keinen enthält. Entsprechende Aussagen können wir auch für größere SChranken b treffen, also etwa

$$v^b(Gl\infty, q) = e^{-\sum_{k=1}^{b} 1/k}(1 + O(q^{-3})) \text{ für alle } b \geq 4, \text{ etc.}$$

Vermutlich gilt diese Entwicklung auch allgemein für alle $b \in \mathbb{N}$. Genauer definieren wir

$$b^* := \lfloor \frac{b}{2} \rfloor + 1.$$

Wir stellen folgende Vermutungen auf.

Vermutung 3.16 *Der Limes der Proportionen b-satter Matrizen für $b > 2$ ist nähernungsweise*

$$v^b(GL, \infty, q) = e^{-\sum_{k=2}^{b} 1/k}(1 - \frac{1}{2b^*}q^{-b^*} + O(q^{-(b^*+1)})).$$

Wir konnten dies leider nicht exakt beweisen. Eine andere Möglichkeit ist es, $v^b(GL, \infty, q)$ abzuschätzen. Eine zufriedenstellende Abschätzung nach unten konnten wir aber nicht finden.

Satz 3.17 *Es gilt*

(i) (Obere Schranke) $v^b(GL, \infty, q) \leq e^{-\sum_{k=1}^{b} 1/k}$,

(ii) (Untere Schranke) $v^b(GL, \infty, q) \geq e^{-\sum_{k=1}^{b} 1/k} \cdot (1 - \frac{1}{2}q^{-1} + O(q^{-2}))$.

Beweis: Die obere Schranke ist am leichtesten mit Quokkatheorie zu finden. Wir verweisen daher auf Kapitel 8 und speziell Satz 8.15.

Wegen $\frac{q^k - iq(k)}{q^k - 1} \leq \frac{q^k - q}{q^k - 1}$ (denn $k \geq 2$) und $G(q^k; 1) \geq e^{-\frac{q^k}{(q^k-1)^2}}$ (siehe Satz 2.55(vii)) ist

$$\begin{aligned} G(q^k; 1)^{(q^k - i_q(k))/k} &\geq \exp(-\frac{q^k}{(q^k-1)^2})^{(q^k - i_q(k))/k} \\ &\geq \exp\left(-\frac{1}{k}\frac{q^k(q^k - q)}{(q^k-1)^2}\right). \end{aligned}$$

Es ist $\frac{q^k(q^k-q)}{(q^k-1)^2} < 1$ und damit

$$G(q^k; 1)^{(q^k - i_q(k))/k} > e^{-1/k}.$$

□

Kapitel 4

Matrixring

In diesem Kurzen Einschub wollen wir die Proportion b-satter Elemente des Matrixrings $M(n,q) = \mathbb{F}_q^{n\times n}$ angeben. Wie in der Bemenrkung 1.3 (i) erwähnt, lässt sich diese sofort aus den Proportionen der b-satten Elemente der Generellen Linearen Gruppe folgern. Nach der Bemerkung gilt für die Proportion b-satter Matrizen

$$v^b(M(n,q)) = \prod_{i=1}^{n}(1-q^{-i})v^b(GL(n,q)).$$

Als Grenzwert ergibt sich somit

$$v^b(M,\infty,q) = G(q;1)v^b(GL\infty,q).$$

Interessant ist nun, dass wir für $v^b(M,\infty,q)$ genauere Näherungen, für alle $b \in \mathbb{N}$, angeben können. Gewisse Terme im von q abhängigen Fehlerterm verschwinden nähmlich gerade nicht. Genau Näherungen für $b \in \{1,...,12\}$ sind in Anhang B angegeben.

Satz 4.1 *Sei $b \in \mathbb{N}$ beliebig. Der Grenzwert der Proportionen b-satter Matrizen ist circa*

$$e^{-\sum_{k=1}^{b}\frac{1}{k}}.$$

Genauer gelten folgende Näherungen

$b = 1$

$$e^{-1}\cdot\left(1-\frac{3}{2}q^{-1}+O\left(q^{-2}\right)\right),$$

$b \geq 2$

$$e^{-\sum_{k=1}^{b}\frac{1}{k}}\cdot\left(1-q^{-1}+O\left(q^{-2}\right)\right).$$

Beweis: Die Näherung für $b = 1$ haben Neumann und Praeger in [7], Theorem 4.5 angegeben. Man vergleiche auch Anhang B. Man erhält den Wert durch eine Entwicklung von $G(q;1)$ nach q, d.h.

$$G(q;1) = (1-q^{-1}+O\left(q^{-2}\right)),$$

und der Multiplikation mit der Entwicklung von $v^1(GL,\infty,q)$, man siehe Satz 3.15.

Für $b = 2$ geht man genau gleich vor. Für $b > 2$ kann sich der Term von q^{-1}, wie wir am Ende des letzten Kapitels erwähnten, nicht verändern. (Für $k \geq 2$ gilt $v^b(GL,\infty,q) = e^{-\sum_{k=1}^{b}\frac{1}{k}}\cdot(1+O\left(q^{-2}\right)))$

□

Kapitel 5

Symplektische Gruppen

In diesem Kapitel wollen wir die Proportion b-satter Matrizen einer Symplektischen Gruppe bestimmen. Die Symplektische Gruppe sei mit $Sp(n,q)$ oder $Sp(2m,q)$ bezeichnet.

- $\beta : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ sei die nicht-ausgeartete, alternierende Bilinearform, die durch die Dimension $n = 2m$ eindeutig festgelegt ist (bis auf Isometrie).
- Die klassische Gruppe $Sp(2m,q)$ ist definiert als Invariantengruppe von β, d.h. $Sp(2m,q) := \{g \in GL(2m,q) \mid \beta(g(u).g(v)) = \beta(u,v) \ \forall\ u,v \in \mathbb{F}_q^n\}$.
- Der natürliche Modul von $Sp(2m,q)$ ist $V = \mathbb{F}_q^n$. Dieser hat gerade Dimension, $n = 2m$, über dem endlichen Körper $K = \mathbb{F}_q$.
- Der Witt-Index von (V,β) ist dann m, also die Dimension der maximalen, total isotropen Untervektorräume.
- Φ bezeichne eine Grammatrix.

Schreiben wir die Elemnte von $GL(2m,q)$ als Matrizen, so ist $g \in GL(2m,q)$ genau dann ein Element von $Sp(2m,q)$, wenn $g^{tr}\Phi g = \Phi$ gilt.

Die Proportion b-satter Matrizen wird mit $v_n^b = v^b(Sp(n,q))$ bezeichnet. Wir wollen, wie bei den Generellen Linearen Gruppen, die erzeugende Funktion als Potenzreihe betrachten und den Limes der Proportionen bestimmen. Für die Symplektischen Gruppen sind dies

$$V^b(z) = V^b(Sp,q;z) = \sum_{m=0}^{\infty} v_{2m}^b z^m \text{ und } v^b(Sp,\infty,q) = \lim_{m\to\infty} v_{2m}^b.$$

(man beachte die Summantion über m!)

Wir verwenden wieder die b-Äquivalenz und im Besonderen die Zerlegung des Lemmas 2.36:

$$\begin{aligned} g \in Sp(n,q) \quad \Rightarrow \quad & V = V_0 \perp V_{\leq b},\ n_0 := \dim V_0,\ n_{\leq b} := \dim V_{\leq b} \\ & \text{mit } n_0,\ n_{\leq b} \text{ gerade, } g_{|_{V_0}}\ b-\text{satt und } n_{\leq b} = \deg\left(ggT(\chi_g, \Psi_b)\right). \end{aligned} \tag{I}$$

($\Psi_b(x) := \prod_{\lambda \in \bar{K}\ nicht-b-sättigend} (x-\lambda)^n$).

In den ersten drei Kapiteln haben wir eine Operation auf b-Hauptraumzerlegungen betrachtet und Matrizen im wesentlichen nach ihren (verallgemeinerten) Eigenwerten aufgeteilt und so eine Summenformel erhalten. Dann mussten wir nur Matrizen mit möglichst einfachem charakteristischem Polynom betrachten. Für die Eigenwerte aus $\mathbb{F}_q$ waren dies Matrizen, die nur diesen Eigenwert besitzen. Für Eigenwerte über einem Erweiterungskörper war dies etwas komplizierter, da diese nicht alleine auftreten können, sondern eine Matrix über $\mathbb{F}_q$ immer auch alle q-Potenzen, also die Galois-Konjugierten, als Eigenwerte haben muss.

In den weiteren klassischen Gruppen können nun auch einige Eigenwerte nicht alleine vorkommen und verallgemeinerte Eigenwerte nicht nur mit ihren Galois-Konjugierten zusammen. Dies haben wir in Satz 2.35 gezeigt. Genauer gilt $g^{tr}\Phi g = \Phi$ für $g \in Sp(2m, q)$, da g β invariant lässt. Damit ist g ähnlich zu g^{-tr}. Wir halten fest:

λ ist verallgemeinerter Eigenwert von $g \Leftrightarrow \lambda^{-1}$ ist verallgemeinerter Eingewert von g. (II)

Jedes Element der symplektischen Gruppe hat zu jedem Eigenwert auch das multiplikativ Inverse als Eigenwert. Es ist also nur dann möglich, einen Eigenwert λ beziehungsweise die Proportionen der Matrizen, die nur diesen Eigenwert besitzen, alleine zu betrachten, falls $\lambda = \lambda^{-1}$ gilt. Dies trifft nur bei $\lambda \in \{1, -1\}$ beziehungsweise $\lambda = 1$, falls q gerade ist, zu. Ist λ ein verallgemeinerter Eigenwert, so ist die interessante Frage, ob λ^{-1} Galois-konjugiert zu λ ist. Falls dies nicht gilt, müssen λ und λ^{-1} und alle Galois-Konjugierten zusammen betrachtet werden. Wir untersuchen die Eigenwerte mit dieser Eigenschaft.

Lemma 5.1 *Seien $k \geq 1$ und $\lambda \in \mathbb{F}_{q^k}$ primitiv über $\mathbb{F}_q$.*

Gilt $\lambda = \lambda^{-1}$ oder sind λ und λ^{-1} Galois-konjugiert (d.h. sie haben das selbe Minimalpolynom), dann gilt einer der drei folgenden Fälle.

(i) q ist ungerade, $k = 1$ und $\lambda = \pm 1$.

(ii) q ist gerade, $k = 1$ und $\lambda = 1$.

(iii) q beliebig, k gerade und $\lambda^{-1} = \lambda^{q^{\frac{k}{2}}}$

Beweis: Angenommen $k > 1$. Insbesondere gilt damit $\lambda \neq \lambda^{-1}$. λ und λ^{-1} sind Galois-konjugiert, also existiert ein $0 < i < k$, mit $\lambda^{q^i} = \lambda^{-1}$. Daraus folgt

$$\lambda = \lambda^{-q^i} = \lambda^{q^i q^i} = \lambda^{q^{2i}}.$$

λ ist Element von $\mathbb{F}_{q^k}$, also gilt $\lambda^{q^k} = \lambda$. λ liegt in keinem echten Teilkörper, also wird q^{2i} von q^k geteilt. Wir haben $i < k$ vorausgesetzt, also gilt $2i = k$. Insbesondere ist k gerade.

□

Wir wollen Vertretermengen der Typen von Eigenwerten definieren und dann deren Kardinalitäten bestimmen. Dabei betrachten wir nur Erzeuger der Erweiterungskörper $\mathbb{F}_{q^k}$ für $k \leq b$.

Definition 5.2 *Sei $k \leq b$.*

- Θ_k *war als Vertretermenge der primitiven Elemente definiert, wobei jeweils nur ein Galois-Konjugierter enthalten ist, siehe Definition* 3.2.
- *Wir definieren die Vertretermenge der primitiven Elemente, die Galois-konjugiert zu ihren Inversen sind,*
$$\Theta_k^1 := \{\lambda \in \Theta_k | \lambda^{-1} = \lambda^{q^{\frac{k}{2}}}\}.$$
- Θ_k^2 *sei definiert als Teilmenge von $\Theta_k \backslash \Theta_k^1$, die von $\lambda \in \Theta_k \backslash \Theta_k^1$ und λ^{-1} und deren Galois-konjugierten nur eines enthält. Für $\lambda \in \Theta_k^2$ gelte also*
$$\lambda^{-q^i} \notin \Theta_k^2 \quad \text{für alle} \quad i = 0, ..., k-1.$$
- *Zur Vereinfachung $\Theta^1 := \bigcup_{k=1}^b \Theta_k^1$ und $\Theta^2 := \bigcup_{k=1}^b \Theta_k^2$.*

Θ_k^1 ist Vertretermenge von primitiven Elementen, die Galois-konjugiert zu ihren Inversen sind. Dies kann aber für ungerade $k \neq 1$ nicht auftreten. Insbesondere ist also für $k \neq 1$ ungerade $\Theta_k^1 = \emptyset$ und $|\Theta_k^2| = \frac{1}{2}|\Theta_k|$. Wir wollen die Mächtigkeiten auch für die anderen Fälle berechnen. Für $k = 1$ gilt $\Theta_1^1 = \{\pm 1\}$ und

$$|\Theta_1^2| = \begin{cases} \frac{q-2}{2} & \text{falls } q \text{ gerade,} \\ \frac{q-3}{2} & \text{falls } q \text{ ungerade.} \end{cases}$$

Für $k = 2$ haben die Elemente in Θ_k^1 gerade Norm 1, sind also Elemente, deren Minimalpolynome konstanten Term 1 haben. Denn für $\lambda \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ gilt $\lambda^{-1} = \frac{\lambda}{\mu_\lambda(0)}$. Die Kardinalitäten sind

$$|\Theta_2^1| = \begin{cases} \frac{q}{2} & \text{falls } q \text{ gerade,} \\ \frac{q-1}{2} & \text{falls } q \text{ ungerade,} \end{cases}$$

und

$$|\Theta_2^2| = \begin{cases} \frac{q^2-2q}{4} & \text{falls } q \text{ gerade,} \\ \frac{q^2-2q+1}{4} & \text{falls } q \text{ ungerade.} \end{cases}$$

Für größere k wollen wir zwei Berechnungsmöglichkeiten angeben. Dazu zunächst folgendes Lemma.

Lemma 5.3 *Sei $1 \leq k \leq b$ gerade.*

(i) $\Theta_k^1 = \{\lambda \in \Theta |\ \lambda^{q^{k/2}+1} = 1\}$. Θ_k^1 ist also Vertretermenge der $(q^{k/2}+1)$-ten Einheitswurzeln, die primitiv in $\mathbb{F}_{q^k}$ sind.

(ii) Die im maximalen Teilkörper $\mathbb{F}_{q^{k/2}}$ von $\mathbb{F}_{q^k}$ enthaltenen $(q^{k/2}+1)$-ten Einheitswurzeln sind 1 und -1, nur 1 falls q gerade. Insbesondere gilt $\Theta_k^1 \cap \mathbb{F}_{q^{k/2}} = \emptyset$.

Beweis: (i) klar nach Definition. Für (ii) müssen wir nur den größten gemeinsamen Teiler der Ordnungen der beiden zyklischen Gruppen bestimmen:

$$ggT(q^{k/2}+1, q^{k/2}-1) = \begin{cases} 1 & \text{falls } q \text{ gerade,} \\ 2 & \text{falls } q \text{ ungerade.} \end{cases}.$$

Außerdem sind 1 und -1 sicher $(q^{k/2}+1)$-te Einheitswurzeln. □

Um $|\Theta_k^1|$ zu berechnen wollen wir von der Ordnung der Gruppe der $(q^{k/2}+1)$-ten Einheitswurzeln die Anzahl aller Einheitswurzeln, die nicht primitiv für $\mathbb{F}_{q^k}$ über $\mathbb{F}_q$ sind, abziehen. Wir erhalten die Anzahl der primitiven Elemente unter den $(q^{k/2}+1)$-ten Einheitswurzeln (primitiv über dem Körper $\mathbb{F}_q$, nicht unbedingt als Einheitswurzel primitiv). Jedes $k-$te solcher Elemente liegt dann in der Vertretermenge Θ_k^1.

Satz 5.4 *Sei $1 \leq k \leq b$ gerade mit $k = 2^\alpha k'$, 2 teilt nicht k' und $\alpha \in \mathbb{N}$.*

(i) (Siebformel) Wir gehen die Untergruppen der Gruppe der $(q^{k/2}+1)$-ten Einheitswurzeln, die als Untergruppe einer Einheitengruppe eines Zwischenkörpers von $\mathbb{F}_{q^k}/\mathbb{F}_q$ vorkommen, durch. Damit gilt

$$k \cdot |\Theta_k^1| \ = \ q^{k/2} + 1 - \sum_{p \ Pz.,\ p|k} (q^{k/2p}+1) + \sum_{p,r \ \ Pz.,\ pr|k} (q^{k/2pr}+1) - \ldots \pm |\Theta_1^1|.$$

(ii) (Rekursiv) Alle $(q^{k/2}+1)$-ten Einheitswurzeln haben einen Vertreter in $\Theta_{2^\alpha l'}^1$ für genau ein $l'|k'$. Somit gilt

$$k \cdot |\Theta_k^1| \ = \ q^{k/2} + 1 - \sum_{l'|k',\ l' \neq k'} 2^\alpha l' \cdot |\Theta_{2^\alpha l'}^1| - |\Theta_1^1|.$$

(iii) Insbesondere ist $k/2$ der Grad von $|\Theta_k^1|(q) \in \mathbb{Q}[x]$, als Polynom in q betrachtet.

Beweis: Sei p ein Primzahl, die k' teilt. Wir wollen die $(q^{k/2}+1)$-ten Einheitswurzeln, die im maximalen Teilkörper $\mathbb{F}_{q^{k/p}}$ liegen, bestimmen. Diese bilden eine zyklische Untergruppe und wir wollen den größten gemeinsamen Teiler von $q^{k/2}+1$ und $q^{k/p}-1$ berechnen. Es ist $q^{k/p}-1 = (q^{k/2p}-1)(q^{k/2p}+1)$ und

$$q^{k/2}+1 = (q^{k/2p}+1)\sum_{i=0}^{p-1}(-q^{\frac{k}{2p}})^i \quad \text{(p ist ungerade und damit ist } (-1)^{p-1}=1\text{)}.$$

Da außerdem

$$\sum_{i=0}^{p-1}(-q^{\frac{k}{2p}})^i = 1+(q^{\frac{k}{2p}}-1)(q^{\frac{k}{2p}}+q^{\frac{k+3}{2p}}+...+q^{\frac{k(p-2)}{2p}})$$

eine Linearkombination der 1 ist, gilt insgesamt

$$ggT(q^{k/2}+1, q^{k/p}-1) = q^{k/2p}+1.$$

Hieraus ergibt sich sofort Möglichkeit (i). Für (ii) ist zu beachten, dass eine $(q^{k/2}+1)$-te Einheitswurzel primitiv in einem Körper $\mathbb{F}_{q^l}$ mit $l|k$ ist. Ist $\lambda \neq \pm 1$, so wird l von 2^α geteilt. Die Überlegungen oben liefern insbesondere, dass λ eine $(q^{l/2}+1)$-te Einheitswurzel ist. Damit ist λ aber Galois-konjugiert zu einem Element aus Θ_l nach Definition der Vertretermenge.

(iii) folgt sofort aus (i) oder (ii). □

Für die zweite Berechnungsmöglichkeit ist es notwendig, die Anzahl der Elemente in Θ_k^1 zu kennen, wenn k eine 2-Potenz ist. Alle anderen Kardinalitäten können aus diesen berechnet werden.

Bemerkung 5.5 *(i) Sei $k = 2^\alpha \leq b$, $\alpha \in \mathbb{N}$. Mit Lemma 5.3 (ii) gilt*

$$|\Theta_k^1| = \begin{cases} \frac{1}{k}q^{2^{\alpha-1}} & \text{falls } q \text{ gerade,} \\ \frac{1}{k}(q^{2^{\alpha-1}}-1) & \text{falls } q \text{ ungerade.} \end{cases}$$

Die Kardinalitäten der zweiten Vertretermenge sind jetzt leicht anzugeben.

(ii) Für k gerade gilt

$$|\Theta_k^2| = \frac{1}{2}(|\Theta_k| - |\Theta_k^1|) \;=\; \frac{1}{2}(\frac{q^k - i_q(k)}{k} \;-\; |\Theta_k^1|).$$

($i_q(k)$: siehe Definition 3.2).

(iii) Für $k \neq 1$ ungerade gilt

$$|\Theta_k^2| = \frac{1}{2}|\Theta_k| = \frac{q^k - i_q(k)}{2k}.$$

(iv) Wir geben die Werte für kleine k an.

q gerade:

k	$\lvert\Theta_k^1\rvert$	$\lvert\Theta_k^2\rvert$
1	1	$\frac{q-2}{2}$
2	$\frac{q}{2}$	$\frac{q^2-2q}{4}$
3	0	$\frac{q^3-q}{6}$
4	$\frac{q^2}{4}$	$\frac{q^4-2q^2}{8}$
5	0	$\frac{q^5-q}{10}$
6	$\frac{q^3-q}{6}$	$\frac{q^6-2q^3-q^2+2q}{12}$
7	0	$\frac{q^7-q}{14}$
8	$\frac{q^4}{8}$	$\frac{q^8-2q^4}{16}$
9	0	$\frac{q^9-q^3}{18}$
10	$\frac{q^5-q}{10}$	$\frac{q^{10}-2q^5-q^2+2q}{20}$
11	0	$\frac{q^{11}-q}{22}$
12	$\frac{q^6-q^2}{12}$	$\frac{q^{12}-2q^6-q^4+2q^2}{24}$

q ungerade:

k	$\lvert\Theta_k^1\rvert$	$\lvert\Theta_k^2\rvert$
1	2	$\frac{q-3}{2}$
2	$\frac{q-1}{2}$	$\frac{q^2-2q+2}{4}$
3	0	$\frac{q^3-q}{6}$
4	$\frac{q^2-1}{4}$	$\frac{q^4-2q^2+1}{8}$
5	0	$\frac{q^5-q}{10}$
6	$\frac{q^3-q}{6}$	$\frac{q^6-2q^3-q^2+2q}{12}$
7	0	$\frac{q^7-q}{14}$
8	$\frac{q^4-1}{8}$	$\frac{q^8-2q^4+1}{16}$
9	0	$\frac{q^9-q^3}{18}$
10	$\frac{q^5-q}{10}$	$\frac{q^{10}-2q^5-q^2+2q}{20}$
11	0	$\frac{q^{11}-q}{22}$
12	$\frac{q^6-q^2}{12}$	$\frac{q^{12}-2q^6-q^4+2q^2}{24}$

Wie im letzen Kapitel wollen wir jetzt b-Hauptraumzerlegungen für Elemente der $Sp(n,q)$ betrachten. Man vergleiche dazu die Definitionen 3.1 und 3.4.

Definition 5.6 *Sei $g \in Sp(n,q)$.*

- *Der in Gleichung (I) gegebene Untervektorraum V_0, auf dem g b-satt ist und der maximal mit dieser Eigenschaft ist, heißt b-satter Hauptraum.*
- *Für $\lambda \in \Theta^1$ ist der b-Hauptraum von g bezüglich λ gegeben durch*

$$H(\lambda) := Kern(\mu_\lambda(g)^n).$$

(μ_λ bezeichne das Minimalpolynom von λ.)

- *Für $\lambda \in \Theta^2$ ist der b-Hauptraum von g bezüglich λ gegeben durch*

$$H(\lambda) := Kern((\mu_\lambda(g)\mu_{\lambda^{-1}}(g))^n).$$

- *Die orthogonale Zerlegung*

$$V = V_0 \perp \coprod_{\lambda\in\Theta^1} H(\lambda) \perp \coprod_{\lambda\in\Theta^2} H(\lambda)$$

heißt b-Hauptraumzerlegung von g.

- *Die Menge von $(1 + |\Theta^1| + |\Theta^2|)-$ Tupeln von Untervektorräumen, die eine orthogonale Zerlegung von V angeben, ist hier gegeben durch*

$$\mathcal{M} := \{\Big(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (V_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (V_{\lambda_b})_{\lambda_b\in\Theta_b^2}\Big) \mid V_0, V_{\lambda_i} \le V,\ V = V_0 \perp \coprod V_\lambda\}.$$

- *Die Dimensionsabbildung ist*

  $$\dim : \mathcal{M} \to \mathbb{N}^{1+|\Theta^1|+|\Theta^2|},\ (V_0,\ (V_\lambda)_{\lambda\in\Theta^1},\ (V_\lambda)_{\lambda\in\Theta^2}) \mapsto (\dim(V_0),\ (\dim(V_\lambda))_{\lambda\in\Theta^1},\ (\dim(V_\lambda))_{\lambda\in\Theta^2}).$$

- $\pi : Sp(n,q) \to \mathcal{M},\ g \mapsto (V_0,\ (H(\lambda))_{\lambda\in\Theta^1},\ (H(\lambda))_{\lambda\in\Theta^2})$ *weist jeder Matrix ihre b-Hauptraumzerlegung zu.*

Viele Aussagen gelten jetzt genauso wie bei der Generellen Linearen Gruppe. Die wesentlichen Unterschiede gibt das folgende Lemma an.

Lemma 5.7 *Sei $g \in Sp(2m,q)$.*

(i) Die Dimension eines $b-Hauptraums$ von g ist gerade.

(ii) Sei $\lambda \in \Theta^2$ ein Eigenwert von g und $m_\lambda := \frac{\dim H(\lambda)}{2}$. Dann existiert eine nicht-orthogonale Zerlegung

$$H(\lambda) = W \oplus W^*$$

in total isotrope, g-invariante Teilräume, jeweils der Dimension m_λ. Ist B eine Basis für W, so ist die Dualbasis B^* eine Basis für W^*. Die Einschränkung $g_{|_{W^*}}$ als Matrix bzgl. B^* ist gegeben durch $g_{|_W}^{-tr}$ (bzgl. B). Damit ist $g_{|_{W^*}} \in GL(m_\lambda, q)$ insbesondere durch $g_{|_W} \in GL(m_\lambda, q)$ festgelegt.

Beweis: Zu (i): Die Zerlegung in Haupträume ist orthogonal. Ist also λ ein nicht-b-sättigender Eigenwert von g, so ist

$$(H(\lambda), \beta_{|_{H(\lambda)\times H(\lambda)}})$$

ein Symplektischer Raum. Insbesondere ist die Dimension gerade. Der b-satte Hauptraum muss dann auch gerade Dimension haben (gleiches Argument oder über die Summe der Dimensionen).

Zu (ii): $\lambda \in \Theta^2$ ist ein Eigenwert von g, also auch λ^{-1} und λ und λ^{-1} haben verschiedene Minimalpolynome. Wir setzen

$$W := Kern(\mu_\lambda(g)^n) \text{ und } W^* := Kern(\mu_{\lambda^{-1}}(g)^n).$$

W, W^* sind dann g-invariante Teilräume. Diese haben jeweils Dimension m_λ. Sei $s \in Sp(m_\lambda, q)$ der halbeinfache Anteil der Einschränkung von g auf W. Über $K[\lambda]$ ist s dann diagonalisierbar und besitzt eine Eigenvektorbasis. Seien v, w zwei Eigenvektoren. Die Eigenwerte sind Galois-konjugiert zu λ, sagen wir λ^{q^i} bzw. λ^{q^j}. Damit gilt

$$\beta(v,w) = \beta(sv, sw) = \lambda^{q^i+q^j}\beta(v,w).$$

λ liegt aber in Θ^2 und somit sind Galois-Konjugierte nicht invers zueinander. Es muss also $\beta(v,w) = 0$ gelten. Insgesamt sind damit $K[\lambda]W$ und insbesondere auch W total isotrop. Gleiches gilt für $W^\perp$.

Da $H(\lambda)$ nicht degeneriert ist (d.h. $H(\lambda) \cap H(\lambda)^\perp = \emptyset$), ist die Summe insbesondere nicht orthogonal. Eine Basis von W^* ist als Dualbasis einer Basis von W gegeben.

□

Wir erhalten wie bei der generellen linearen Gruppe folgende Resultate.

Lemma 5.8 *(i) Für $g, h \in Sp(n,q)$ gilt*

$$g \sim_b h \Leftrightarrow \dim(\pi(g)) = \dim(\pi(h)).$$

(ii) Ein Tupel $(V_0,\ (V_\lambda)_{\lambda\in\Theta^1},\ (V_\lambda)_{\lambda\in\Theta^2}) \in \mathcal{M}$ liegt genau dann im Bild von π, wenn alle Dimensionen gerade sind und außerdem folgende Bedingungen gelten:

(a) $\dim V_0 = 0$ *oder* $\dim V_0 > b$,

(b) $\forall\ k \leq b\ \forall\ \lambda \in \Theta_k^1$*:* $2k$ *teilt* $\dim V_\lambda$,

(c) $\forall\ k \leq b\ \forall\ \lambda \in \Theta_k^2$*:* $2k$ *teilt* $\dim V_\lambda$.

(iii) Ein Tupel in $\mathbb{N}^{1+|\Theta^1|+|\Theta^2|}$ *liegt entsprechend genau dann im Bild von* $\dim \circ \pi$*, wenn es die Form*

$$\left(2m_0,\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (2m'_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \ldots\ ,\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m'_{\lambda_b})_{\lambda_b\in\Theta_b^2}\right)$$

hat, wobei $m_0 = 0$ *oder* $m_0 > \frac{b}{2}$ *gilt.*

(iv) $Sp(n,q)$ *operiert auf* $\mathcal{M}$ *durch komponentenweises Anwenden.* dim *ist eine trennende Invariante und der Stabilisator eines* $\pi(g)$ *für* $g \in Sp(n,q)$ *ist dann isomorph zu*

$$Sp(2m_0,q) \times \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k^1} Sp(2k\cdot m_{\lambda_k},q) \times \prod_{\lambda_k\in\Theta_k^2} GL(k\cdot m'_{\lambda_k},q).$$

(v) Für $g \in Sp(n,q)$ *ist die Menge aller Matrizen, die* π *gleich wie* g *abbildet, bijektiv zu*

$$S^b(Sp(2m_0,q)) \times \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k^1} \mathcal{X}\left(\mu_{\lambda_k}^{2m_{\lambda_k}}\right) \times \prod_{\lambda_k\in\Theta_k^2} \mathcal{X}\left((\mu_{\lambda_k}\mu_{\lambda_k^{-1}})^{m_{\lambda_k}}\right).$$

$S^b(Sp(2m_0,q))$ *bezeichnet die Menge der b-satten Matrizen in der* $Sp(2m_0,q)$*,* $\mathcal{X}(...)$ *die Menge der Matrizen, die das angegebene charakteristische Polynom haben. Die Mengen*

$$\mathcal{X}\left((\mu_{\lambda_k}\mu_{\lambda_k^{-1}})^{m_{\lambda_k}}\right)_{Sp(2km_{\lambda_k},q)} \text{ und } \mathcal{X}\left(\mu_{\lambda_k}^{m_{\lambda_k}}\right)_{GL(km_{\lambda_k},q)}$$

sind bijektiv. Die Dimensionen bzw. Potenzen sind gegeben durch

$$\dim(\pi(g)) = \left(2m_0,\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (2m'_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \ldots\ ,\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m'_{\lambda_b})_{\lambda_b\in\Theta_b^2}\right).$$

Beweis: Wie bei der Generellen Linearen Gruppe, siehe Lemmata und Bemerkungen 3.5 bis 3.9.

Das folgende Lemma gibt die Proportionen zu den Mengen in (v) im letzten Lemma an.

Lemma 5.9 *Sei* k *ein Teiler von* m *mit* $n = 2m$.
Dann gelten folgende Aussagen über Proportionen von bestimmten Matrizen in $Sp(n,q)$.

(i) $\chi((x-1)^n) = \chi((x+1)^n) = u(Sp(n,q))$.

(ii) Für alle $\lambda \in \Theta_1^2$ *gilt* $\chi\left(((x-\lambda)(x-\lambda^{-1}))^m\right) = u(GL(m,q))$.

(iii) Für alle $\lambda \in \Theta_k^1$ *gilt* $\chi\left(\mu_\lambda(x)^{\frac{n}{k}}\right) = u(Sp(n/k,q^k))$.

(iv) Für alle $\lambda \in \Theta_k^2$ *gilt* $\chi\left((\mu_\lambda(x)\cdot\mu_{\lambda^{-1}}(x))^{m/k}\right) = u(GL(m/k,q^k))$.

Beweis: (i) und (ii) haben Neumann und Praeger in [7], Abschnitt 3 und Theorem 5.1, bewiesen.

(i) und (iii) sind direkte Anwendungen von Satz 2.48 beziehungsweise der Folgerung daraus. Alle Matrizen mit charakteristischem Polynom $\mu_\lambda(x)^{\frac{n}{k}}$ haben in der multiplikativen Jordanzerlegung einen halbeinfachen Anteil, dessen Minimalpolynom μ_λ ist. Alle halbeinfachen Anteile sind konjugiert. Die Menge der unipotenten Matrizen, die mit einem halbeinfachen Anteil vertauschen, ist nach Satz 2.48 bijektiv zu $U(GL(n,q^k))$, der Menge der unipotenten Matrizen in

der $GL(n,q^k)$. Der Zentralisator eines halbeinfachen Anteils ist isomorph zur $GL(n,q^k)$. Durch Kürzen (siehe Folgerung 2.49) erhält man die behaupteten Proportionen.

Zu (ii) und (iv): Sei $\lambda \in \Theta_k^2$ für k teilt m und gerade oder $k=1$. Eine Matrix mit Eigenwert λ muss nach (II) auch λ^{-1} als Eigenwert besitzen. Sei also $g \in \mathcal{X}\left((\mu_a(x)\cdot\mu_{a^{-1}}(x))^{\frac{m}{k}}\right)$. Der Vektorraum $V=\mathbb{F}_q^n$ lässt sich nach Lemma 5.7(ii) in eine direkte, bzgl. β nicht-orthogonale Summe zerlegen.

$$V = W \oplus W^*,$$

$W = Kern(\mu_\lambda(g))$ und $W^* = Kern(\mu_{\lambda^{-1}}(g))$. Die Dimensionen von W und W^* sind jeweils m (Witt-Index). Sei B eine Basis von W. Dann ist die Dualbasis B^* eine Basis von W^* und $g_{|_W}$ legt $g_{|_{W^*}}$ fest. Nach Konstruktion besitzt $g_{|_W}$ genau die Eigenwerte $\lambda,\ \lambda^q, ...,\ \lambda^{q^{k-1}}$, hat das charakteristische Polynom $\mu_\lambda(x)^{m/k}$ und es gilt $g_{|_W} \in \mathcal{X}(\mu_\lambda(x)^{m/k})$, diese Menge ist als Teilmenge von $GL(W) \cong GL(m,q)$ aufzufassen. Satz 2.49 liefert jetzt wiederum

$$\chi(\mu_\lambda(x)^{m/k})_{GL(m,q)} = u(GL(m/k,q^k))$$

und damit

$$\chi((\mu_\lambda(x)\cdot\mu_{\lambda^{-1}}(x))^{m/k})_{Sp(2m,q)} = \chi(\mu_\lambda(x)^{m/k})_{GL(m,q)} = u(GL(m/k,q^k)).$$

□

Damit haben wir alle Unterschiede aufgelistet und können nun einen Zusammenhang zwischen b-satter Potenzreihe und unipotenten Potenzreihen für die Symplektische Gruppen formulieren. Für die Generellen Linearen Gruppen haben wir diesen in den Sätzen 3.10 und 3.11 entwickelt.

Satz 5.10 *Es gilt*

$$(1-z)^{-1} \;=\; V^b(Sp,q;z)\ \prod_{k=1}^{b} U(Sp,q^k;z^k)^{|\Theta_k^1|}\ U(GL,q^k;z^{2k})^{|\Theta_k^2|}.$$

Beweis: Im Beweis zum Satz 3.10 bestimmten wir zunächst die Länge einer Bahn von b-Hauptraumzerlegungen. Sei dazu $g\ in Sp(n,q)$ mit

$$\dim \pi(g) = \left(2m_0,\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (2m'_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots\ ,\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m'_{\lambda_b})_{\lambda_b\in\Theta_b^2}\right).$$

Damit hat die Bahn $Sp(n,q)\cdot\pi(g)$ nach Lemma 5.8(iv) die Länge

$$\frac{|Sp(n,q)|}{|Sp(2m_0,q)|\prod_{k=1}^b\prod_{\lambda_k\in\Theta_k^1}|Sp(2k\cdot m_{\lambda_k},q)|\prod_{\lambda_k\in\Theta_k^2}|GL(k\cdot m'_{\lambda_k},q)|}.$$

Zum zweiten interessierte uns die Anzahl der Matrizen mit der selben b-Hauptraumzerlegung. Diese ist jetzt nach Lemma 5.8 (v) und Lemma 5.9 gegeben durch

$$v^b(Sp(2m_0,q))|Sp(2m_0,q)|\prod_{k=1}^{b}\prod_{\lambda_k\in\Theta_k^1}|Sp(2m_{\lambda_k},q^k)|\chi\left((\mu_{\lambda_k}(x))^{2m_{\lambda_k}}\right)\cdot$$

$$\prod_{\lambda_k\in\Theta_k^2}|GL(km'_{\lambda_k},q^k)|\chi\left((\mu_{\lambda_k}(x)\mu_{\lambda_k^{-1}}(x))^{m'_{\lambda_k}}\right).$$

Summieren über alle Bahnen und Kürzen liefert

$$1 = \sum v^b(Sp(2m_0,q))\ \prod_{k=1}^{b}\prod_{\lambda_k\in\Theta_k^1}u(Sp(2m_{\lambda_k},q^k))\ \prod_{\lambda_k\in\Theta_k^2}u(GL(m'_{\lambda_k},q^k)),$$

wobei wir über das Bild von $\dim \circ \pi$ summieren, also über alle Tupel der Form

$$\Big(2m_0,\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (2m'_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots\ ,\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m'_{\lambda_b})_{\lambda_b\in\Theta_b^2}\Big)$$

mit $m_0 = 0$ oder $m_0 > \frac{b}{2}$.

Schlussendlich multiplizieren wir beide Seiten mit z^{2m} und summieren über m. Wir erhalten die oben angegebene Gleichung für die Potenzreihen.

□

Wegen $U(Sp,q;z) = G(q^2;qz)^{-1}$ (s. Satz 2.52) gilt folgende Folgerung.

Folgerung 5.11 $V^b(Sp,q;z) = (1-z)^{-1}\ \prod_{k=1}^{b}\ G(q^{2k};q^kz^k)^{|\Theta_k^1|}G(q^k;z^{2k})^{|\Theta_k^2|}$.

Wir betrachten wiederum den Grenzwert für $m\to\infty$. Eine genaue Aussage über die Konvergenz können wir leider nicht liefern.

Satz 5.12 *Der Limes der Proportionen b-satter Matrizen in der Symplektischen Gruppe ist*

$$v^b(Sp;\infty,q) = \prod_{k=1}^{b} G(q^{2k};q^k)^{|\Theta_k^1|}G(q^k;1)^{|\Theta_k^2|}$$

Beweis: Man betrachte analog zu Satz 3.14 die Laurrententwicklung um 1 der Funktion, die auf der rechten Seite der Gleichung in der Folgerung angegeben ist. □

Der nächste Satz liefert eine Abschätzung für $v^b(Sp;\infty,q)$. Genauere Werte für $b\in\{1,...,24\}$ sind im Anhang C angegeben.

Satz 5.13 *Es gilt für $b\geq 1$ beliebig*

$$v^b(Sp;\infty,q) = \begin{cases} e^{-\sum_{k=1}^{b}\frac{1}{2k}}(1-\frac{3}{4}q^{-1}+O(q^{-2})) & \textit{falls } q \textit{ gerade,}\\ e^{-\sum_{k=1}^{b}\frac{1}{2k}}(1-\frac{5}{4}q^{-1}+O(q^{-2})) & \textit{falls } q \textit{ ungerade.}\end{cases}$$

Beweis: Der Satz 2.55 gibt an, wie wir Abschätzungen für $G(q^{2k};q^k)^{|\Theta_k^1|}$ und $G(q^k;1)^{|\Theta_k^2|}$ berechnen können:

$$G(q^{2k};q^k)^{\frac{1}{k}q^{k/2}} = (1-\frac{1}{k}q^{-k/2}+O(q^{-k})) \text{ und } G(q^k;1)^{\frac{q^k-q^{\deg(i_q(k))}}{2k}} = e^{-\frac{1}{2}k}(1-\frac{1}{4k}q^{-d}+O(q^{-d-1})),$$

wobei wieder $d = k-\deg(i_q(k))$ („k minus größten Teiler“) sei. In den Potenzen werden nur die Terme größeren Grades von $|\Theta_k^1|(q)$ und $|\Theta_k^2|(q)$ betrachtet, dies ist aber für die Näherungen

$$G(q^{2k};q^k)^{|\Theta_k^1|}\approx 1 \text{ und } G(q^k;1)^{|\Theta_k^2|}\approx e^{-1/2k}$$

ausreichend. Damit gilt

$$v^b(Sp;\infty,q) = e^{-\sum_{k=1}^{b}\frac{1}{2k}}(1+O(q^{-1})).$$

Um den zweiten Faktor genauer zu berechen, müssen nur die Werte für $k=1$ und $k=2$ ausgewertet werden. Nach Neumann und Praeger [7] gilt

$$v^1(Sp;\infty,q) = G(q^2;q)^{|\Theta_1^1|}G(q;1)^{|\Theta_1^2|} = \begin{cases} e^{-\frac{1}{2}}(1-\frac{3}{4}q^{-1}+O(q^{-2})) & \text{falls } q \text{ gerade,}\\ e^{-\frac{1}{2}}(1-\frac{5}{4}q^{-1}+O(q^{-2})) & \text{falls } q \text{ ungerade.}\end{cases}$$

und mit Maple

$$G(q^2;q)^{|\Theta_1^1|}G(q;1)^{|\Theta_1^2|} = \begin{cases} e^{-\frac{1}{2}}(1-\frac{3}{8}q^{-2}+O(q^{-3})) & \text{falls } q \text{ gerade,}\\ e^{-\frac{1}{2}}(1-\frac{1}{8}q^{-2}+O(q^{-3})) & \text{falls } q \text{ ungerade.}\end{cases}$$

Für $k\geq 3$ gilt bereits $k/2>1$ und $d>1$. Damit verschwindet für alle k der Term $1-\frac{3}{4}q^{-1}$ beziehungsweise $1-\frac{5}{4}q^{-1}$ nicht.

□

Kapitel 6

Unitäre Gruppe

Die Proportionen b-satter Matrizen in den Unitären Matrizen zu bestimmen ist jetzt nicht weiter schwierig, da wir wie bei den Symplektischen Gruppen vorgehen können. Wir wollen nur die wesentlichen Unterschiede auflisten.

- $\beta : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ sei die (bis auf Isometrie) eindeutige nicht-ausgeartete, hermitsche Form.
- β ist $(^-)$-Sesquilinearform, wobei $(^-)$ der Körperautomorphismus $\mathbb{F}_{q^2} \to \mathbb{F}_q,\ \lambda \mapsto \overline{\lambda}$ ist.
- Die Unitäre Gruppe $U(n,q)$ ist definiert als Invariantengruppe von β, d.h.

$$U(n,q) := \{g \in GL(n,q^2) \mid \beta(g(u).g(v)) = \beta(u,v)\ \forall\ u,v \in \mathbb{F}_q^n\}.$$

- Der natürliche Modul von $U(n,q)$ ist $V = \mathbb{F}_q^n$ über dem endlichen Körper $K = \mathbb{F}_q$.
- Der Witt-Index, die Dimension der maximalen, total isotropen Untervektorräume, ist $\frac{n}{2}$ beziehungsweise $\frac{n-1}{2}$, je nachdem, ob n gerade oder ungerade ist.
- Φ bezeichne eine Grammatrix.

Für $g \in U(n,q)$ bezeichne $\overline{g}$ die Isometrie $(^-) \circ g$, wobei $(^-)$ eintragsweise auf die Elementen von $V = \mathbb{F}_q^n$ angewendet werde. Schreiben wir die Elemente von $GL(n,q^2)$ als Matrizen, so ist $g \in GL(n,q^2)$ genau dann ein Element von $U(n,q)$, wenn $\overline{g^{tr}}\Phi g = \Phi$ gilt.

Die Proportion b-satter Matrizen wird mit $v_n^b = v^b(U(n,q))$ bezeichnet. Wir wollen wieder die erzeugende Funktion als Potenzreihe betrachten und den Limes der Proportionen bestimmen. Für die Unitäre Gruppe sind dies

$$V^b(z) = V^b(U,q;z) = \sum_{n=0}^{\infty} v_n^b z^n \text{ und } v^b(U,\infty,q) = \lim_{n\to\infty} v_n^b.$$

Lemma 2.36 liefert wieder

$$g \in U(n,q) \quad \Rightarrow \quad V = V_0 \perp V_{\leq b},\ n_0 := \dim V_0,\ n_{\leq b} := \dim V_{\leq b} \quad \text{(I)}$$
$$\text{mit } g_{|_{V_0}}\ b-\text{satt und } n_{\leq b} = \deg\left(ggT(\chi_g, \Psi_b)\right).$$

$(\Psi_b(x) := \prod_{\lambda \in \bar{K}\ \textit{nicht b-sättigend}} (x-\lambda)^n)$.

Satz 2.35 liefert hier

$$\lambda \text{ ist verallgemeinerter Eigenwert von } g \ \Leftrightarrow\ \overline{\lambda}^{-1} = \lambda^{-q} \text{ ist verallg. Eingewert von } g \quad \text{(II)}$$

Wir müssen Bedingungen für die algebraischen Elemente $\lambda \in \bar{\mathbb{F}}_{q^2}$ finden, die Galois-konjugiert zu λ^{-q} sind. Dies heißt im unitären Fall, dass $\lambda^{-q} = \lambda^{q^{2i}}$ für ein $i \geq 0$ ist.

Lemma 6.1 *Seien $k \geq 1$ und $\lambda \in \mathbb{F}_{q^{2k}}$ primitiv über $\mathbb{F}_{q^2}$.*

Gilt $\lambda = \lambda^{-q}$ oder sind λ und λ^{-q} Galois-konjugiert (d.h. sie haben das selbe Minimalpolynom), dann gilt einer der zwei folgenden Fälle.

(i) $\lambda \in \mathbb{F}_{q^2}$ und λ ist $(q+1)$-te Einheitswurzel.

(ii) k ist ungerade und $\lambda^{-q} = \lambda^{q^{k+1}}$. λ ist dann (q^k+1)-te Einheitswurzel.

Beweis: Ist $\lambda \in \mathbb{F}_{q^2}$, so gilt $\lambda^{-q} = \lambda$ und damit $\lambda^{q+1} = 1$. Wegen $|\mathbb{F}_{q^2}^*| = (q-1)(q+1)$ liegen die $(q+1)$-ten Einheitswurzeln in $\mathbb{F}_{q^2}$.

Seien nun $k > 1$ angenommen. Insbesondere gilt damit $\lambda \neq \lambda^{-q}$. λ und λ^{-q} sind Galois-konjugiert, also existierte ein $0 < i < k$, mit $\lambda^{q^{2i}} = \lambda^{-q}$. Daraus folgt

$$\lambda^{q^2} = \lambda^{(-q)(-q)} = \lambda^{q^{2i}q^{2i}} = \lambda^{q^{4i}}$$

und damit $4i - 2 = 2k$. Umformen ergibt $i = \frac{k+1}{2}$ und k muss insbesondere ungerade sein. Damit gilt

$$\lambda^{-q} = \lambda^{q^{k+1}} \Leftrightarrow 1 = \lambda^{q(q^k+1)} = \overline{\lambda^{q^k+1}}.$$

Dann muss aber bereits $\lambda^{q^k+1} = 1$ gelten.

□

Umgekehrt erfüllen natürlich für ungerades $1 \leq k \leq b$ alle $(q^k+1)-$ten Einheitswurzeln, die primitiv für die Körpererweiterung $\mathbb{F}_{q^{2k}}/\mathbb{F}_{q^2}$ sind, die Bedingung, dass λ und λ^{-q} Galois-konjugiert sind. Wir definieren nun wie im letzten Kapitel passende Vertretermengen. Dabei verwenden wir die selben Bezeichnungen.

Definition 6.2 *Sei $k \leq b$.*

- *Θ_k war als Vertretermenge der primitiven Elemente definiert, wobei jeweils nur ein Galois-Konjugierter enthalten ist, siehe Definition 3.2.*
- *Wir definieren Θ_k^1, die Menge der $\lambda \in \Theta_k$, die Galois-Konjugiert zu λ^{-q} sind,*

$$\Theta_k^1 := \{\lambda \in \Theta_k | \lambda^{-q} = \lambda^{q^{k+1}}\}.$$

- *Θ_k^2 sei definiert als Teilmenge von $\Theta_k \backslash \Theta_k^1$, die von $\lambda \in \Theta_k \backslash \Theta_k^1$ und λ^{-q} und deren Galois-konjugierten nur eines enthält. Es gelte also für $\lambda \in \Theta_k^2$*

$$\lambda^{-q^{2i}} \notin \Theta_k^2 \quad \text{für alle} \quad i = 0, ..., k-1.$$

- *Zur Vereinfachung $\Theta^1 := \bigcup_{k=1}^b \Theta_k^1$ und $\Theta^2 := \bigcup_{k=1}^b \Theta_k^2$.*

Für k gerade ist $\Theta_k^1 = \emptyset$ und $|\Theta_k^2| = \frac{1}{2}|\Theta_k|$. Wir wollen die Anzahl der Elemente für ungerade k berechnen. Für $k = 1$ gilt $|\Theta_1^1| = q+1$ und entsprechend $|\Theta_1^2| = \frac{q^2-q-2}{2}$.

Für größere k müssen wir die Anzahl der (q^k+1)-ten Einheitswurzeln, die primitiv für $\mathbb{F}_{q^{2k}}/\mathbb{F}_{q^2}$ sind, berechnen.

Lemma 6.3 *Seien $1 < k \leq b$ ungerade und C die Gruppe der (q^k+1)-ten Einheitswurzeln in $\mathbb{F}_{q^{2k}}$.*

(i) Es gilt $\Theta_1^1 \subseteq C$.

(ii) Sei p ein Primteiler von k. Dann gilt

$$|C \cap \mathbb{F}_{q^{2k/p}}| \;=\; q^{\frac{k}{p}} + 1.$$

Alle (q^k+1)-ten Einheitswurzeln, die Elemente des maximalen Teilkörpers $\mathbb{F}_{q^{2k/p}}$ und primitiv für die Körpererweiterung $\mathbb{F}_{q^{2k/p}}/\mathbb{F}_{q^2}$ sind, haben einen Vertreter in $\Theta^1_{k/p}$.

Beweis: Zu (i): Sei $\lambda \in \Theta^1_1$, d.h. $\lambda^q = \lambda^{-1}$. Damit gilt

$$\lambda^{q^k} = \lambda^{(-1)^k} = \lambda^{-1},$$

denn k ist ungerade. Damit ist λ aber (q^k+1)-te Einheitswurzel.

Zu (ii): Wir müssen den größten gemeinsamen Teiler von (q^k+1) und $(q^{\frac{2k}{p}}-1)$ bestimmen (diesen haben wir im wesentlichen bereits im Beweis zu Lemma 5.3 bestimmt). Der größte gemeinsame Teiler ist $q^{\frac{k}{p}}+1$, denn es gilt $q^{\frac{2k}{p}}-1 = (q^{\frac{k}{p}}+1)(q^{k/p}-1)$ und

$$q^k + 1 = (q^{\frac{k}{p}}+1)\sum_{i=0}^{p-1}(-q^{\frac{k}{p}})^i \quad \text{(p ist ungerade und damit ist } (-1)^{p-1}=1)$$

und es gibt eine Linearkombination der 1 durch die beiden weiteren Faktoren:

$$\sum_{i=0}^{p-1}(-q^{\frac{k}{p}})^i = 1 + (q^{\frac{k}{p}}-1)(q^{\frac{k}{p}} + q^{\frac{k3}{p}} + ... + q^{\frac{k(p-2)}{p}}).$$

Somit sind die Elemente, die im Schnitt von C und $\mathbb{F}_{q^{2k/p}}$ liegen, $(q^{\frac{k}{p}}+1)$-te Einheitswurzeln. Die primitiven Elemente sind also nach Definition von $\Theta^1_{k/p}$ Galois-konjugiert zu einem Vertreter aus $\Theta^1_{k/p}$.

□

Nun sehen wir leicht, dass für alle ungeraden $1 \le k \le b$ jede (q^k+1)-te Einheitswurzel einen Vertreter in genau einer Menge Θ^1_l für einen Teiler l von k hat. Mit anderen Worten liegt genau jede k-te (q^k+1)-te Einheitswurzel, die primitiv für die Körpererweiterung $\mathbb{F}_{q^{2k/p}}/\mathbb{F}_q$ ist, in Θ^1_k (ist also ein Vertreter). Wir können die Anzahl der Vertreter wie im symplektischen Fall auf zwei Arten bestimmen.

Satz 6.4 *Sei $1 \le k \le b$ ungerade.*

(i) (Siebformel) Wir gehen die Untergruppen der Gruppe der (q^k+1)-ten Einheitswurzeln, die als Untergruppe einer Einheitengruppe eines Zwischenkörpers von $\mathbb{F}_{q^{2k}}/\mathbb{F}_{q^2}$ vorkommen, durch.

$$k \cdot |\Theta^1_k| \;=\; q^k + 1 - \sum_{p \text{ Pz., } p|k}(q^{k/p}+1) + \sum_{p,r \text{ Pz., } pr|k}(q^{k/pr}+1) - ... \pm |\Theta^1_1|.$$

(ii) (Rekursiv) Alle (q^k+1)-ten Einheitswurzeln haben einen Vertreter in Θ^1_l für genau einen echten Teiler l von k.

$$k \cdot |\Theta^1_k| \;=\; q^k + 1 - \sum_{l|k,\ l\neq k} l \cdot |\Theta^1_l|.$$

(iii) Insbesondere ist k der höchste Grad von $|\Theta^1_k|(q) \in \mathbb{Q}[x]$, als Polynom in q betrachtet.

Beweis: Im wesentlichen folgen die Behauptungen aus den vorangestellten Bemerkungen und Lemmata. Man vergleiche auch den Beweis zum Satz 5.4.

Für die zweite Berechnungsmöglichkeit ist es notwendig, die Anzahl der Elemente in Θ_k^1 zu kennen, wenn k eine Primzahl ist. Wir geben die Kardinalitäten für Primzahlpotenzen an. Alle anderen Kardinalitäten können aus diesen berechnet werden.

Bemerkung 6.5 *(i) Sei $k \leq b$ mit $k = p^\alpha$, p eine ungerade Primzahl und $\alpha \in \mathbb{N}$. Dann gilt*

$$|\Theta_k^1| = \frac{1}{k}(q^{p^\alpha} - q^{p^{\alpha-1}}).$$

Die Kardinalitäten der zweiten Vertretermenge sind jetzt leicht anzugeben.

(ii) Für $1 \leq k \leq b$ ungerade gilt

$$|\Theta_k^2| = \frac{1}{2}(|\Theta_k| - |\Theta_k^1|) \;=\; \frac{1}{2}(\frac{q^k - i_q(k)}{k} \;-\; |\Theta_k^1|).$$

(Für $i_q(k)$ siehe Definition 3.2) .

(iii) Für $2 \leq k \leq b$ gerade gilt

$$|\Theta_k^2| = \frac{1}{2}|\Theta_k| = \frac{q^k - i_q(k)}{2k}.$$

(iv) Wir geben die Werte für kleine k an.

k	$\lvert\Theta_k^1\rvert$	$\lvert\Theta_k^2\rvert$
1	$q+1$	$\frac{q^2-q-2}{2}$
2	0	$\frac{q^4-q^2}{4}$
3	$\frac{q^3-q}{3}$	$\frac{q^6-q^3-q^2+q}{6}$
4	0	$\frac{q^8-q^4}{8}$
5	$\frac{q^5-q}{5}$	$\frac{q^{10}-q^5-q^2+q}{10}$
6	0	$\frac{q^{12}-q^6-q^4+q^2}{12}$
7	$\frac{q^7-q}{7}$	$\frac{q^{14}-q^7-q^2+q}{14}$
8	0	$\frac{q^{16}-q^8}{16}$
9	$\frac{q^9-q^3}{9}$	$\frac{q^{18}-q^9-q^6+q^3}{18}$
10	0	$\frac{q^{20}-q^{10}-q^4+q^2}{20}$
11	$\frac{q^{11}-q}{11}$	$\frac{q^{22}-q^{11}-q^2+q}{22}$
12	0	$\frac{q^{24}-q^{12}-q^8+q^4}{24}$

Wie im letzen Kapitel könnten wir jetzt b-Hauptraumzerlegungen für Elemente der $U(n,q)$ betrachten. Uns interressieren wieder nur Matrizen, deren charakteristisches Polynom höchstens zwei irreduzible Teiler hat. Das nächste Lemma gibt die Proportionen dieser Matrizen an. Die Bezeichnungen der Definition 5.6 und die Aussagen der Lemmata und Sätze 5.7, 5.8 und 5.10 können einfach übertragten werden und gelten entsprechend für die Unitären Gruppen (in den jeweiligen Definitionen und Sätzen haben wir nie die genauen Kardinalitäten der $|\Theta_k^1|$ und $|\Theta_k^2|$ verwendet). Wir wollen auf eine genaue Ausführung verzichten.

Lemma 6.6 *Sei $n \in \mathbb{N}$.*

Dann gelten folgende Aussagen über Proportionen von bestimmten Matrizen in $U(n,q)$.

(i) Für alle $\lambda \in \Theta_1^1$ gilt $\chi((x-\lambda)^n) = u(U(n,q))$.

(ii) Sei zusätzlich n gerade. Für alle $\lambda \in \Theta_1^2$ gilt $\chi\left(((x-\lambda)(x-\lambda^{-q}))^{n/2}\right) = u(GL(\frac{n}{2},q^2))$.

(iii) Sei k ein ungerader Teiler von n. Für alle $\lambda \in \Theta_k^1$ gilt $\chi\left(\mu_\lambda(x)^{\frac{n}{k}}\right) = u(U(\frac{n}{k},q^k))$.

(iv) Seien zusätzlich n gerade und k ein Teiler von $\frac{n}{2}$. Für alle $\lambda \in \Theta_k^2$ gilt $\chi\left((\mu_\lambda(x)\cdot\mu_{\lambda^{-q}}(x))^{\frac{n}{2k}}\right) = u(GL(\frac{n}{2k},q^{2k}))$.

Beweis: (i) und (ii) haben Neumann und Praeger in [7], Abschnitte 3 und 6 bewiesen.

(i) und (iii) sind direkte Anwendungen von Satz 2.48 beziehungsweise der Folgerung daraus.

(iv) ist wie Lemma 5.9 (iv) zu beweisen (eine Matrix ist durch das Abbildungsverhalten auf einem total isotropen Teilraum der halben Dimension festgelegt).

Man beachte für (ii) und (iv), dass wir $U(n,q)$ als Untergruppe der $GL(n,q^2)$ betrachten.

□

Damit erhalten wir eine Gleichung von Potenzreihen, aus der wir die b-satte Potenzreihe für die Unitären Gruppen ablesen können.

Satz 6.7 *Es gilt*

$$(1-z)^{-1} \;=\; V^b(U,q;z)\;\prod_{k=1}^{b}\; U(U,q^k;z^k)^{|\Theta_k^1|}\; U(GL,q^{2k};z^{2k})^{|\Theta_k^2|}.$$

Beweis: Man vergleiche die Beweise zu den Sätzen 3.10 und 3.11 für die Generellen Linearen Gruppen und Satz 5.10 für die Symplektischen Gruppen. Man kann die Proportionen der b-Äquivalenzklassen berechnen und über die Summe der Proportionen die Gleichung für die Potenzreihen erhalten.

□

Nun verwenden wir $U(U,q;z) = G(-q;-z)^{-1}$ und $U(GL,q^2;z) = G(q^2,z)^{-1}$ (siehe Satz 2.52).

Folgerung 6.8 $V^b(U,q;z) \;=\; (1-z)^{-1}\;\prod_{k=1}^{b}\; G(-q^k;-z^k)^{|\Theta_k^1|}\; G(q^{2k};z^{2k})^{|\Theta_k^2|}$.

Zum Abschluss wolle wir noch $v^b(U;\infty,q)$ berechnen und eine Näherung angeben.

Satz 6.9 *Der Limes der Proportionen b-satter Matrizen in der Unitären Gruppe ist*

$$v^b(U;\infty,q) = \prod_{k=1}^{b}\; G(-q^k;-1)^{|\Theta_k^1|}\; G(q^{2k};1)^{|\Theta_k^2|}.$$

Beweis: Wie die Beweise zu den Sätzen 3.14 und 5.12.

□

Satz 6.10 *Es gilt*

$$v^b(U;\infty,q) = e^{-\frac{3}{2}\sum_{k=1,\ k\ ung.}^{b}\frac{1}{k}-\frac{1}{2}\sum_{k=1,\ k\ ger.}^{b}\frac{1}{k}}\;(1+O(q^{-1}))$$

Beweis: Der Satz 2.55 gibt an, wie wir Abschätzungen für $G(-q^k;-1)^{\frac{1}{k}q^k}$ und $G(q^{2k};1)^{\frac{1}{2k}q^{2k}}$ berechnen können:

$$G(-q^k;-1)^{\frac{q^k}{k}} = e^{-1/k}(1+\frac{1}{2k}q^{-k}+O(q^{-2k})) \text{ und } G(q^{2k};1)^{\frac{q^{2k}}{2k}} = e^{-1/2k}(1-\frac{1}{4k}q^{-2k}+O(q^{-4k})).$$

Hierbei sind die Potenzen jeweils die höchsten q-Potenzen der Kardinalitäten von Θ_k^1, falls k ungerade ist, beziehungsweise Θ_k^2 (siehe Satz 6.4 und Bemerkung 6.5). Damit gilt aber bestimmt für k ungerade

$$G(-q^k;-1)^{|\Theta_k^1|} = e^{-1/k}(1+O(q^{-1}))$$

und für k ungerade oder gerade

$$G(q^{2k};1)^{|\Theta_k^2|} = e^{-1/2k}(1+O(q^{-1})).$$

Insgesamt ist die gesuche Näherung dann

$$\begin{aligned} v^b(U;\infty,q) &= \prod_{k=1}^{b} G(q^k;-1)^{|\Theta_k^1|}\ G(q^{2k};1)^{|\Theta_k^2|} \\ &= \prod_{k=1,\ k\ ung.}^{b} e^{-1/k}e^{-1/2k}\ (1+O(q^{-1})) \prod_{k=1,\ k\ ger.}^{b} e^{-1/2k}\ (1+O(q^{-1})) \\ &= e^{-\frac{3}{2}\sum_{k=1}^{b}\frac{1}{k}}\ (1+O(q^{-1})). \end{aligned}$$

□

Für $b \in \{1,...,24\}$ haben wir $v^b(U;\infty,q)$ genauer berechnet. Die Werte sind im Anhang D angegeben. Es ist ein Verschwinden der Grade in q mit steigender Schranke b, ähnlich wie bei den Generellen Linearen Gruppen, zu erkennen.

Kapitel 7

Orthogonale Gruppe

Die letzten Gruppen, die wir betrachten wollen, sind die Orthogonalen Gruppen gerader Dimension. Wie wir in Bemerkung 1.3 zeigten, haben alle Elemente der Orthogonalen Gruppen von ungerader Dimension der Eigenwert 1 oder -1, sind also im Kontext dieser Arbeit nicht interessant. Die relevanten Orthogonalen Gruppen seien mit $O^+(2m,q)$ und $O^-(2m,q)$ bezeichnet.

- Sei $Q : \mathbb{F}_q^n \to \mathbb{F}_q$ eine nicht-ausgeartete quadratische Form.
- $\beta : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ sei die Polarform von Q, d.h. für $u, v \in V$ gilt

  $$\beta(u,v) := Q(u+v) - Q(u) - Q(v).$$

  Ist q ungerade, so ist β eine symmetrische, nicht-ausgeartete Bilinarform, die q eindeutig festlegt. Ist aber q gerade, so gilt dies im Allgemeinen nicht. β ist dann eine alternierende (und symmetrische) Bilinearform.
- Die klassische Gruppe $O(2m,q)$ ist definiert als Invariantengruppe von Q (für ungerade Charakteristik dann auch für β), d.h.

  $$O(2m,q) := \{g \in GL(2m,q) \mid Q(g(v)) = Q(v) \ \forall\ v \in \mathbb{F}_q^n\}.$$

- Wir schreiben auch $O^\epsilon(2m,q)$ mit $\epsilon = +$, falls V eine Basis aus hyperbolischen Paaren besitzt und $\epsilon = -$ sonst. Man siehe zum Vergleich auch die Definition 2.27.
- Der natürliche Modul von $O^\epsilon(2m,q)$ ist $V = \mathbb{F}_q^n$. Dieser hat gerade Dimension, $n = 2m$, über dem endlichen Körper $K = \mathbb{F}_q$.
- Für $O^+(2m,q)$ ist m der Witt-Index von (V,β), also die Dimension eines maximalen Untervektorraums, der nur singuläre Vektoren enthält. Der Witt-Index bei $O^-(2m,q)$ ist $m-1$.
- Φ bezeichne eine Grammatrix von $O^+(2m,q)$ oder $O^-(2m,q)$.

Die Proportion b-satter Matrizen wird mit $v^b(O^\epsilon(2m,q))$ bezeichnet. Wir wollen eigentlich wie zuvor die erzeugende Funktion als Potenzreihe betrachten und den Limes der Proportionen bestimmen. Dies sind die Potenzreihen $V^b(O^\epsilon,q;z) = \sum_{m=0}^{\infty} v^b(O^\epsilon(2m,q))z^m$ und die Grenzwerte $v^b(O^\epsilon,\infty,q) = \lim_{m\to\infty} v^b(O^\epsilon(2m,q))$ (man beachte die Summation über m).

Unser Verfahren, eine Summenformel über die b-Äquivalenzklassen und b-Hauptraumzerlegungen herzuleiten, können wir wieder anwenden, müssen es aber etwas variieren. Dazu definieren wir Folgendes.

Definition 7.1
- *Wir bezeichnen die Summe und Differenz der Proportionen b-satter Matrizen mit* $v^{b+}(O,m,q) := v^b(O^+(2m,q)) + v(O^-(2m,q))$ *und* $v^{b-}(O,m,q) := v^b(O^+(2m,q)) - v(O^-(2m,q))$.
- *In der Definition 1.2 haben wir* $v^b(O^+(0,q)) := 1$ *und* $v^b(SO^-(0,q)) := 0$ *gesetzt.*
- *Die erzeugenden Funktionen von* $v^{b+}(O,m,q)$ *und* $v^{b-}(O,m,q)$ *seien mit* $V^{b+}(O,q;z) = \sum_{m=0}^{\infty} v^{b+}(O,m,q)z^m$ *und* $V^{b-}(O,q;z) = \sum_{m=0}^{\infty} v^{b-}(O,m,q)z^m$ *bezeichnet.*

Wir werden im Folgenden Eigenschaften der beiden letzten Potenzreihen bestimmen und daraus diese für die b-satten Potenzreihen der O^+ und O^- folgern.

Wir verwenden die Zerlegung des Lemmas 2.36:

$$g \in O^\epsilon(n,q) \quad \Rightarrow \quad V = V_0 \perp V_{\leq b},\ n_0 := \dim V_0,\ n_{\leq b} := \dim V_{\leq b} \quad \text{mit } n_0,\ n_{\leq b} \text{ gerade, } g_{|V_0}\ b-\text{satt und } n_{\leq b} = \deg\left(ggT(\chi_g, \Psi_b)\right). \tag{I}$$

($\Psi_b(x) := \prod_{\lambda \in \bar{K}\ nicht-b-sättigend} (x-\lambda)^n$.)

Satz 2.35 liefert für $g \in O^\epsilon(2m,q)$:

$$\lambda \text{ ist verallgemeinerter Eigenwert von } g \ \Leftrightarrow\ \lambda^{-1} \text{ ist verallgemeinerter Eingewert von } g. \tag{II}$$

Man hat den Eindruck, dass sich Orthogonale Gruppen und Symplektische nur wenig unterscheiden. Konsequenterweise sind die Vertretermengen der nicht-b-sättigenden Elemente die selben wie bei den Symplektischen Gruppen. Man siehe Definitionen und Sätze 5.2 bis 5.5 für die Definitionen und Eigenschaften von Θ_k^1 (Vertretermenge der primitiven Elemente von $\mathbb{F}_{q^k}$, die Galois-konjugiert zu ihren Inversen sind) und Θ_k^2 (Vertretermenge der restlichen primitiven Elemente von $\mathbb{F}_{q^k}$). Wir setzen $\Theta^1 := \bigcup_{k=1}^b \Theta_k^1$ und $\Theta^2 := \bigcup_{k=1}^b \Theta_k^2$.

Eine weitere Besonderheit der Orthogonalen Gruppen ist aber, dass alle b-satten Elemente im Normalteiler $SO^\epsilon(2m,q)$, dem Kern der Dickson-Invariante

$$D : O(V) \to \mathbb{F}_2,\ g \mapsto\ \dim(Bild(1-g)) \pmod 2$$

liegen müssen. Dies haben wir in Satz 2.43 gezeigt.

Eigentlich müssen also nur die Speziellen Orthogonalen Gruppen betrachtet werden. Wir wollen zwar die Proportionen b-satter Matrizen in den Orthogonalen Gruppen berechnen, dies ist aber gerade die Hälfte der Proportionen in den Speziellen Orthogonalen Gruppen. Die Proportionen unipotenter Matrizen haben wir in Lemma 2.46(vi) auch nur in den Speziellen Orthogonalen Gruppen berechnet, denn Steinbergs Methode zählt für $q = 2$ nur die unipotenten Elemente in der $SO\epsilon(2m,q)$ (siehe das Lemma oder [11]).

Definition 7.2 *Für die Proportionen unipotenter Matrizen in der* $SO^\epsilon(2m,q)$ *definieren wir entsprechend*

- $u^+(SO,m,q) := u(SO^+(2m,q)) + u(SO^-(2m,q))$ *und* $u^-(SO,m,q) := u(SO^+(2m,q)) - u(SO^-(2m,q))$.
- *In der Definition 2.45 haben wir* $u(SO^+(0,q)) := 2$ *und* $u(SO^-(0,q)) := 0$ *gesetzt.*
- *Die erzeugenden Funktionen von* $u^+(SO,m,q)$ *und* $u^-(SO,m,q)$ *sind dann* $U^+(SO,q;z) = \sum_{m=0}^{\infty} u^+(SO,m,q)z^m$ *und* $U^-(O,q;z) = \sum_{m=0}^{\infty} v^-(O,m,q)z^m$.

Die b-Hauptraumzerlegungen von Elementen der $O\epsilon(2m,q)$ beziehungsweise $SO\epsilon(2m,q)$ werden wir wieder etwas ausführlicher als bei den Unitären Gruppen betrachten. Man vergleiche für die nächste Definition die entsprechende Definition 5.6.

Definition 7.3 *Sei $g \in O^\epsilon(2m,q)$.*

- *Der in Gleichung (I) gegebene Untervektorraum V_0, auf dem g b-satt ist und der maximal mit dieser Eigenschaft ist, heißt b-satter Hauptraum.*
- *Für $\lambda \in \Theta^1$ ist der b-Hauptraum von g bezüglich λ gegeben durch*

$$H(\lambda) := Kern(\mu_\lambda(g)^n).$$

  (μ_λ bezeichne das Minimalpolynom von λ.)
- *Für $\lambda \in \Theta^2$ ist der b-Hauptraum von g bezüglich λ gegeben durch*

$$H(\lambda) := Kern((\mu_\lambda(g)\mu_{\lambda^{-1}}(g))^n).$$

- *Die orthogonale Zerlegung*

$$V = V_0 \perp \coprod_{\lambda\in\Theta^1} H(\lambda) \perp \coprod_{\lambda\in\Theta^2} H(\lambda)$$

  heißt b-Hauptraumzerlegung von g.
- *Die Menge von $(1 + |\Theta^1| + |\Theta^2|)-$ Tupeln von Untervektorräumen, die eine orthogonale Zerlegung von V angeben, ist hier gegeben durch*

$$\mathcal{M} := \{\Big(V_0,\ (V_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (V_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots\ ,\ (V_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (V_{\lambda_b})_{\lambda_b\in\Theta_b^2}\Big) \mid V = V_0 \perp \coprod V_\lambda\}$$

- *Die Abbildung $\pi : O^\epsilon(2m,q) \to \mathcal{M},\ g \mapsto (V_0,\ (H(\lambda))_{\lambda\in\Theta^1},\ (H(\lambda))_{\lambda\in\Theta^2})$ weist jeder Matrix ihre b-Hauptraumzerlegung zu.*

Ein weiterer Unterschied ist, dass sich die verschieden Haupträume unterscheiden.

Lemma 7.4 *Sei $g \in O^\epsilon(2m,q)$.*

(i) Die Dimension eines $b-$Hauptraums von g, mit Ausnahme der Haupträume zu den Eigenwerten 1 und -1, ist gerade. Liegt g in der $SO^\epsilon(2m,q)$, so liefert die Determinante, dass die Dimensionen aller b-Haupträume gerade sind.

(ii) Sei $\lambda \in \Theta^1$ ein Eigenwert von g dann kann der b-Hauptraum $H(\lambda)$ mit der Einschränkung der Quadratischen Form Q vom Witt-Typ $+$ oder $-$ seien.

(iii) Der b-satte Hauptraum V_0 kann mit der Einschränkung von Q vom Witt-Typ $+$ oder $-$ seien.

(iv) Sei $\lambda \in \Theta^2$ ein Eigenwert von g und $m_\lambda := \frac{\dim H(\lambda)}{2}$. Dann existiert eine nicht-orthogonale Zerlegung

$$H(\lambda) = W \oplus W^*$$

in total isotrope, g-invariante Teilräume, jeweils der Dimension m_λ. Ist B eine Basis für W, so ist die Dualbasis B^* eine Basis für W^*. Die Abbildungsmatrix von $g_{|W^*}$ bezüglich B^* ist gegeben durch die von $g_{|W}^{-tr}$ bezüglich B. $g_{|W^*} \in GL(m_\lambda,q)$ ist also insbesondere durch $g_{|W} \in GL(m_\lambda,q)$ festgelegt. Der Witt-Typ von $H(\lambda)$ ist $+$.

(v) Sein $\lambda_1,...,\lambda_s$ die Eigenwerte von g und ϵ_{λ_i} der Witt-Index des b-Hauptraums $H(\lambda_i)$ für $1 \le i \le s$. Der Witt-Index des b-satten Hauptraums von g sei ϵ_0. Dann gilt

$$\epsilon = (\epsilon_0)\prod_{i=1}^{s}(\epsilon_{\lambda_i}).$$

Beweis: (i) bis (iii) sind klar. Für (iv) vergleiche man den Beweis zu Lemma 5.7 (iii). Der Witt-Index ist +, denn der b-Hauptraum besitzt total isotrope Teilräume von halber Dimension.

Zu (v): Wir müssen nur zeigen, dass das orthogonale Produkt zweier Untervektorräume mit Witttyp − vom Witt-Typ + sind. Ohne Einschränkung seien U, U' Untervektorräume der Dimension 2 und von Witt-Typ −. Dann ist

$$U \perp U' = \langle e, f \rangle \perp W,$$

wobei (e, f) ein hyperbolisches Paar sei. Angenommen $U \perp U'$ hätte Witt-Typ −, d.h. W enthält keine singulären Vektoren. Dann sind W und U' isometrisch. Sei $f : W \to U'$ so eine Isometrie. Nach dem Satz von Witt (2.10) setzt f zu einer Isometrie $g : U \perp U' \to U \perp U'$ fort. Dann würde aber $g(U) = \langle e, f \rangle$ gelten, ein Widerspruch.

□

Eine Konsequenz der letzten Aussage des Lemmas ist, dass in b-Hauptraumzerlegungen auch die Verteilung der Witttypen beachtet werden muss.

Definition 7.5 *Die Dimensions-Witttyp-Abbildung definieren wir als*

$$\begin{aligned} \dim^* : \ & \mathcal{M} \ \to \ (\mathbb{N} \times \{+,-\})^{1+|\Theta^1|} \times \mathbb{N}^{|\Theta^2|}, \\ & (V_0,\ (V_\lambda)_{\lambda\in\Theta^1},\ (V_\lambda)_{\lambda\in\Theta^2}) \ \mapsto \ \big((\dim(V_0), \epsilon_0),\ ((\dim(V_\lambda), \epsilon_\lambda))_{\lambda\in\Theta^1}\,,\ (\dim(V_\lambda))_{\lambda\in\Theta^2}\big)\,. \end{aligned}$$

Es bezeichne ϵ_0 den Witt-Typ von V_0 mit der Einschränkung von Q und für $\lambda \in \Theta^1$ sei ϵ_λ der Witt-Typ von V_λ.

Wir erhalten wie bei den bereits betrachteten Gruppe folgende Resultate, die mit denen aus Lemma 5.8 übereinstimmen.

Lemma 7.6 *(i) Für $g, h \in O^\epsilon(2m, q)$ gilt*

$$Zg \sim_b h \Leftrightarrow \dim^*(\pi(g)) = \dim^*(\pi(h)).$$

(ii) Ein Tupel $(V_0,\ (V_\lambda)_{\lambda\in\Theta^1},\ (V_\lambda)_{\lambda\in\Theta^2}) \in \mathcal{M}$ liegt genau dann im Bild von π, wenn alle Dimensionen gerade sind und außerdem folgende Bedingungen gelten:

- *(a) $\dim V_0 = 0$ oder $\dim V_0 > b$,*
- *(b) $\forall\ k \le b\ \forall\ \lambda \in \Theta^1_k$: $2k$ teilt $\dim V_\lambda$,*
- *(c) $\forall\ k \le b\ \forall\ \lambda \in \Theta^2_k$: $2k$ teilt $\dim V_\lambda$.*

(iii) Ein Tupel liegt entsprechend genau dann im Bild von $\dim \circ \pi$, wenn es die Form

$$\Big((2m_0, \epsilon_0),\ ((2m_{\lambda_1}, \epsilon_{\lambda_1}))_{\lambda_1\in\Theta^1_1}\,,\ (2m_{\lambda_1})_{\lambda_1\in\Theta^2_1},\ \ldots\ ,\ (2b\cdot m_{\lambda_b}, \epsilon_{\lambda_b})_{\lambda_b\in\Theta^1_b},\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta^2_b}\Big)$$

hat, wobei $m_0 = 0$ oder $m_0 > \frac{b}{2}$ und $\epsilon = \epsilon_0 \prod \epsilon_{\lambda_1}$ gelten.

(iv) $O^\epsilon(2m, q)$ operiert auf $\mathcal{M}$ durch komponentenweises Anwenden. dim *ist eine trennende Invariante und der Stabilisator eines $\pi(g)$ für $g \in O^\epsilon(2m, q)$ ist dann isomorph zu*

$$O^{\epsilon_0}(2m_0, q) \times \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta^1_k} O^{\epsilon_{\lambda_k}}(2k\cdot m_{\lambda_k}, q) \times \prod_{\lambda_k\in\Theta^2_k} GL(k\cdot m_{\lambda_k}, q).$$

(ϵ_0 bezeichnet den Witt-Typ von V_0 und ϵ_{λ_k} den von $H(\lambda_k)$, $\lambda_k \in \Theta^1_k$.)

(v) Für $g \in SO^\epsilon(2m,q)$ ist die Menge aller Matrizen in $SO^\epsilon(2m,q)$, die π gleich wie g abbildet, bijektiv zu

$$S^b(O^{\epsilon_0}(2m_0,q)) \times \prod_{k=1}^{b} \prod_{\lambda_k \in \Theta_k^1} \mathcal{X}\left(\mu_{\lambda_k}^{2m_{\lambda_k}}\right) \times \prod_{\lambda_k \in \Theta_k^2} \mathcal{X}\left((\mu_{\lambda_k}\mu_{\lambda_k^{-1}})^{m_{\lambda_k}}\right).$$

$S^b(O^\epsilon(2m_0,q))$ bezeichnet die Menge der b-satten Matrizen in der $O^\epsilon(2m_0,q)$ oder $SO^\epsilon(2m_0,q)$, $\mathcal{X}(...)$ die Menge der Matrizen in der Orthogonalen Gruppe und damit auch in der Speziellen Orthogonalen Gruppe, die das angegebene charakteristische Polynom haben. Die Grade der Matrizen bzw. die Potenzen der Polynome sind gegeben durch

$$\dim(\pi(g)) = \left(2m_0,\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (2m'_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots,\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m'_{\lambda_b})_{\lambda_b\in\Theta_b^2}\right).$$

Beweis: Man siehe Lemma 7.6 und die Lemmata und Bemerkungen 3.5 bis 3.9.

Das folgende Lemma gibt die Proportionen zu den Mengen in 7.6 (v) an.

Lemma 7.7 *Sei k ein Teiler von m, $n = 2m$.*
Dann gelten folgende Aussagen über Proportionen von bestimmten Matrizen in $SO^\epsilon(2m,q)$.

(i) $\chi((x-1)^n) = \chi((x+1)^n) = u(SO^\epsilon(2m,q))$

(ii) Für alle $\lambda \in \Theta_1^2$ gilt $\chi\left(((x-\lambda)(x-\lambda^{-1}))^m\right) = u(GL(m,q))$

(iii) Für alle $\lambda \in \Theta_k^1$ gilt $\chi\left(\mu_\lambda(x)^{\frac{n}{k}}\right) = u(SO^\epsilon(2m/k,q^k))$

(iv) Für alle $\lambda \in \Theta_k^2$ gilt $\chi\left((\mu_\lambda(x)\cdot\mu_{\lambda^{-1}}(x))^{m/k}\right) = u(GL(m/k,q^k))$

Beweis: Man vergleiche Lemma 7.7.

Im nächsten Satz können wir mit Hilfe unserer Vorbereitungen eine Gleichung für interessante Potenzreihen herleiten.

Satz 7.8 *Es gelten folgende Aussagen.*

(i)

$$2^{|\Theta_1|-1} = \sum v^b(O^{\epsilon_0}(2m_0,q)) \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k^1} u(SO^{\epsilon_{\lambda_k}}(2m_{\lambda_k},q^k)) \prod_{\lambda_k\in\Theta_k^2} u(GL(m'_{\lambda_k},q^k)),$$

wobei wir über das Bild von $SO^\epsilon(2m,q)$ unter $\dim^* \circ \pi$ summieren. Dies sind alle Tupel der Form

$$\left((2m_0,\epsilon_0),\ ((2m_{\lambda_1},\epsilon_{\lambda_1}))_{\lambda_1\in\Theta_1^1},\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots,\ (2b\cdot m_{\lambda_b},\epsilon_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^2}\right)$$

mit $m_0 = 0$ oder $m_0 > \frac{b}{2}$.

(ii)

$$2^{|\Theta_1|} = \sum v^{b+}(O,m_0,q) \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k^1} u^+(SO,m_{\lambda_k},q^k)) \prod_{\lambda_k\in\Theta_k^2} u(GL(m'_{\lambda_k},q^k))$$

und für $m > 0$

$$0 = \sum v^{b-}(O,m_0,q) \prod_{k=1}^{b} \prod_{\lambda_k\in\Theta_k^1} u^-(SO,m_{\lambda_k},q^k) \prod_{\lambda_k\in\Theta_k^2} u(GL(m'_{\lambda_k},q^k)).$$

Ist $m = n = 0$, so ist die untere Summe auch gleich $2^{|\Theta_1|}$. Wir summieren jeweils über alle Tupel der Form

$$\Big(2m_0,\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^1},\ (2m'_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots\ ,\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m'_{\lambda_b})_{\lambda_b\in\Theta_b^2}\Big)$$

mit $m_0 = 0$ oder $m_0 > \frac{b}{2}$.

(iii)

$$2^{|\Theta_1|}\cdot(1-z)^{-1} \ = \ V^{b+}(O,q;z)\ \prod_{k=1}^{b}\ U^+(SO,q^k;z^k)^{|\Theta_k^1|}\ U(GL,q^k;z^{2k})^{|\Theta_k^2|}$$

und

$$2^{|\Theta_1|} = \ V^{b-}(O,q;z)\ \prod_{k=1}^{b}\ U^-(SO,q^k;z^k)^{|\Theta_k^1|}\ U(GL,q^k;z^{2k})^{|\Theta_k^2|}.$$

Beweis: Zu (i): Wir summieren über das Bild von $SO^\epsilon(2m,q)$ unter $\dim^*\pi$. Sei $g\in SO^\epsilon(2m,q)$ mit

$$\dim^*\pi(g) = \Big((2m_0,\epsilon_0),\ ((2m_{\lambda_1},\epsilon_{\lambda_1}))_{\lambda_1\in\Theta_1^1},\ (2m_{\lambda_1})_{\lambda_1\in\Theta_1^2},\ \dots\ ,\ (2b\cdot m_{\lambda_b},\epsilon_{\lambda_b})_{\lambda_b\in\Theta_b^1},\ (2b\cdot m_{\lambda_b})_{\lambda_b\in\Theta_b^2}\Big).$$

Bahnenlänge von $\pi(g)$ sind gleich unter $O^\epsilon(2m,q)$ und $O^\epsilon(2m,q)$. Diese ist nach Lemma 7.6(iv) gleich

$$\frac{|O^\epsilon(2m,q)|}{|O^{\epsilon_0}(2m_0,q)|\prod|O^{\epsilon_{\lambda_k}}(2k\cdot m_{\lambda_k},q)|\prod|GL(km'_{\lambda_k},q)|}.$$

Das Urbild von $\dim^*\pi(g)$ hat nach Lemmata 7.6(v) und 7.7 die Kardinalität

$$v^b(O^{\epsilon_0}(2m_0,q))|O^{\epsilon_0}(2m_0,q)|\cdot\prod_{k=1}^{b}\prod_{\lambda_k\in\Theta_k^1}u(SO^{\epsilon_{\lambda_k}}(2m_{\lambda_k},q^k))|SO^{\epsilon_{\lambda_k}}(2km_{\lambda_k},q)|\cdot$$

$$\prod_{\lambda_k\in\Theta_k^2}u((GL(m_{\lambda_k},q^k))|(GL(km_{\lambda_k},q)|.$$

Kürzen liefert die Kardinalität der b-Äquivalenzklasse von g:

$$2^{-|\Theta_1|}\cdot|O^\epsilon(2m,q)|\cdot v^b(O^{\epsilon_0}(2m_0,q))\cdot\prod_{k=1}^{b}\prod_{\lambda_k\in\Theta_k^1}u(SO^{\epsilon_{\lambda_k}}(2m_{\lambda_k},q^k))\cdot\prod_{\lambda_k\in\Theta_k^2}u(GL(m_{\lambda_k},q^k)).$$

Nun wird auch klar, warum wir $u(SO^+(0,q)) = 2$ und $u(SO^-(0,q)) = 0$ setzten. Ersteres, um für alle $\lambda_k\in\Theta_k^1$ zu erreichen, dass

$$u(SO^{\epsilon_{\lambda_k}}(2m_{\lambda_k},q^k))\frac{|SO^{\epsilon_{\lambda_k}}(2km_{\lambda_k},q)|}{|O^{\epsilon_{\lambda_k}}(2km_{\lambda_k},q)|} = u(SO^{\epsilon_{\lambda_k}}(2m_{\lambda_k},q^k))\frac{1}{2}$$

auch für $m_{\lambda_k} = 0$ gilt, und zweiteres, da Orthogonale Räume von Dimension 0 mit Witttyp $-$ nicht existieren. Wir summieren über alle b-Äquivalenzklassen der $SO^\epsilon(2m,q)$ und erhalten

$$\frac{1}{2} = 2^{-|\Theta_1|}\sum v^b(O^{\epsilon_0}(2m_0,q))\cdot\prod_{k=1}^{b}\prod_{\lambda_k\in\Theta_k^1}u(SO^{\epsilon_{\lambda_k}}(2m_{\lambda_k},q^k))\cdot\prod_{\lambda_k\in\Theta_k^2}u(GL(m_{\lambda_k},q^k)).$$

Eine Addition beziehungsweise Subtraktion der Summen für $SO^+(2m,q)$ und $SO^-(2m,q)$ liefert die in (ii) angegebenen Summenformeln der $v^{b+}(...)$ und $u^+(...)$ beziehungsweise der $v^{b-}(...)$ und $u^-(...)$.

(iii) folgt sofort aus (ii). □

Die Potenzreihen $U^+(SO,q:z)$ und $U^-(SO,q:z)$ können wir wie die unipotenten Potenzreihen der anderen klassischen Gruppen durch die Euler'sche Funktion ausdrücken.

Lemma 7.9 *Es gilt* $U^+(SO, q : z) = G(q^2 : qz)^{-1}$ *und* $U^-(SO, q : z) = G(q^2 : z)^{-1}$.

Beweis: Wir gehen wie im Beweis zum Satz 2.52 vor. Die Ordnung der Speziellen Orthogonalen Gruppen ist nach den Sätzen 2.28 und 2.41 für $m \geq 1$ gleich

$$|SO^\epsilon(2m, q)| = q^{m(m-1)}(q^m - \epsilon 1) \prod_{i=1}^{m-1} (q^{2i} - 1).$$

Der $q-$Anteil ist somit $q^{m(m-1)}$ und nach Steinbergs Satz über die Anzahl unipotenter Elemente (siehe Lemma 2.46 (iv)) ist die Proportion der unipotenten Matrizen in der $SO^\epsilon(2m, q)$ genau

$$u(SO^\epsilon(2m, q)) = \frac{q^{2m(m-1)}}{|O^\epsilon(2m, q)|} = \frac{1}{2} q^{-2m}(q^m + \epsilon 1) \prod_{i=1}^{m} (1 - q^{-2i})^{-1}.$$

Addieren und subtrahieren liefert

$$u^+(SO, m, q) = q^{-m} \prod_{i=1}^{m} (1 - q^{-2i})^{-1} = q^{-m} c_m(q^2)$$

und

$$u^-(SO, m, q) = q^{-2m} \prod_{i=1}^{m} (1 - q^{-2i})^{-1} = q^{-2m} c_m(q^2).$$

Nach Definition 2.50 ist $c_m(q^2)$ das m-te Partialprodukt von $c(q^2) = G(q^2; 1) = \prod_{i=1}^{\infty}(1 - q^{-2i})$. Nach Lemma 2.51 ist $G(q^2; z) = \sum_{m=1}^{\infty} h(m) z^m$ mit $z \in \mathbb{N}$ und $h(m) = q^{-2m} c_m(q^2)$. Es folgt nach Definition der unipotenten Potenzreihen

$$U^+(SO, q : z) = G(q^2 : qz)^{-1} \text{und } U^-(SO, q : z) = G(q^2 : z)^{-1}.$$

□

Folgerung 7.10 *Es gelten*

$$V^{b+}(O, q; z) \;=\; (1 - z)^{-1} \prod_{k=1}^{b} G(q^{2k}; q^k z^k)^{|\Theta_k^1|} G(q^k; z^{2k})^{|\Theta_k^2|}$$

und

$$V^{b-}(O, q; z) \;=\; \prod_{k=1}^{b} G(q^{2k}; z^k)^{|\Theta_k^1|} G(q^k; z^{2k})^{|\Theta_k^2|}.$$

Wir betrachten wiederum den Grenzwert für $m \to \infty$.

Satz 7.11 *Der Limes der Proportionen b-satter Elemente in den Orthogonalen Gruppen ist unabhängig vom Witt-Typ gegeben durch*

$$v^b(O^\epsilon; \infty, q) = \frac{1}{2} \prod_{k=1}^{b} G(q^{2k}; q^k)^{|\Theta_k^1|} G(q^k; 1)^{|\Theta_k^2|}.$$

Beweis: Ähnlich wie in Satz 3.14 liefert die letzte Folgerung, dass gilt

$$v^{b+}(O, m, q) \to \prod_{k=1}^{b} G(q^{2k}; q^k 1)^{|\Theta_k^1|} G(q^k; 1)^{|\Theta_k^2|}$$

und $v^{b-}(O,m,q) \to 0$ für $m \to \infty$. Wegen $v^b(O^+(2m,q)) = \frac{1}{2}(v^{b+}(O,m,q) + v^{b-}(O,m,q))$ und $v^b(O^-(2m,q)) = \frac{1}{2}(v^{b+}(O,m,q) - v^{b-}(O,m,q))$ sind die Grenzwerte gleich, genauer gilt

$$v^b(O^\epsilon;\infty,q) = \lim_{m\to\infty} \frac{1}{2} v^{b+}(O,m,q) = \frac{1}{2} \prod_{k=1}^{b} G(q^{2k};q^k 1)^{|\Theta_k^1|} G(q^k;1)^{|\Theta_k^2|}.$$

□

Mit Ausnahme des Vorfaktors $\frac{1}{2}$ ist dies genau der selbe Wert wie bei den Symplektischen Gruppen, man siehe Satz 5.12 zum Vergleich. Der nächste Satz liefert eine Abschätzung für $v^b(O^\epsilon;\infty,q)$, die natürlich der der Symplektischen Gruppen entspricht. Genauere Werte für $b \in \{1,...,24\}$ sind im Anhang C angegeben.

Satz 7.12 *Es gilt für $b \geq 1$ beliebig*

$$v^b(O;\infty,q) = \begin{cases} \frac{1}{2} e^{-\sum_{k=1}^{b} \frac{1}{2k}} (1 - \frac{3}{4} q^{-1} + O(q^{-2})) & \textit{falls } q \textit{ gerade,} \\ \frac{1}{2} e^{-\sum_{k=1}^{b} \frac{1}{2k}} (1 - \frac{5}{4} q^{-1} + O(q^{-2})) & \textit{falls } q \textit{ ungerade.} \end{cases}$$

Beweis: Wie in Satz 5.13.

Kapitel 8

Quokka-Mengen

Wie in der Einleitung angedeutet, haben wir zunächst versucht, eine andere Methode anzuwenden, um die Proportionen b-satter Matrizen zu berechnen. Wir wollten einen anderen Ansatz betrachten und so eventuell bessere Abschätzungen finden. Die Idee war die Verwendung von Quokkamengen, die Alice Niemeyer und Cheryl Praeger 2010 in [8] vorgestellt hatten, man siehe auch [6] von Frank Lübeck, Alice Niemeyer und Cheryl Praeger (2009). Die Methode hat vielseitige Anwendung in der Berechnung beziehungsweise Abschätzung von Proportionen gefunden, siehe zum Beispiel wieder [8].

Eine bessere obere Schranke können wir in Abschnitt 8.2 angeben, genauer gilt für die Proportionen b-satter Matrizen in der Generellen Linearen Gruppe:

$$v^b(GL, \infty, q) \leq e^{-\sum_{k=1}^{b} \frac{1}{k}}.$$

(Siehe Satz 8.15.)

Beim Versuch, eine gute untere Schranken zu finden, treten aber Schwierigkeiten auf, die ich nicht lösen konnte. Ich werden argumentieren, dass gewisse Abschätzungen nach unten nicht genau genug durchgeführt werden können. Diese Abschätzungen sind aber notwendig, um die Proportionen b-satter Matrizen von großem Grad n näherungweise zu berechnen. Hier wollen wir uns auf den Fall von Eigenwert-freien (1-satten) Matrizen beschränken.

Wir werden in diesem Kapitel nur die Generellen Linearen Gruppen betrachten. Wie in den Kapiteln zuvor geben $n \in \mathbb{N}$ den Grad der Matrizen und $\mathbb{F}_q$ einen endichen Körper an.

Definition 8.1 *(Quokka-Mengen)*
Eine Teilmenge $Q \subseteq GL(n, q)$ heißt Quokkamenge*, falls die folgenden zwei Bedingungen gelten.*

(i) Sei $g \in GL(n, q)$ mit halbeinfachem Anteil s in der Jordanzerlegung (siehe Satz 2.32). Dann gilt

$$g \in Q \Leftrightarrow s \in Q.$$

(ii) Q ist Vereinigung von $GL(n, q)$-Konjugiertenklassen.

Quokka-Mengen können allgemeiner definiert werden, wir wollen uns aber hierauf beschränken.

Wir führen noch einige weitere Begriffe ein.

Definition 8.2

- *Sei $G := GL(\bar{\mathbb{F}}_q^{\,n})$. G ist zusammenhängende (linear) reduktive Gruppe, definiert über dem algebraisch abgeschlossenen Körper $\bar{\mathbb{F}}_q$.*
- *$F : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, \lambda \mapsto \lambda^q$ sei ein Frobeniusmorphismus. F sei durch komponentenweise Anwendung auf G fortgesetzt, sodass $G^F = GL(n, q)$ die Fixgruppe von F ist.*
- *Eine Untergruppe $U \subseteq G$ heißt $F-$*stabil*, falls $F(U) = U$.*

- *Für $U \leq G$ bezeichne $U^F := U \cap GL(n,q)$ den von F fixierten Anteil.*
- *Sei $T \leq G$ ein $F-$stabiler maximaler Torus (d.h. T ist F-stabile endliche abelsche Gruppe mit $T \cong \bar{\mathbb{F}_q}^* \times ... \times \bar{\mathbb{F}_q}^*$ und maximal mit diesen Eigenschaften). Enthält T ein Element der Quokkamenge, so nennen wir T einen* Quokkatorus *oder Q-*Torus*.*
- *Die Menge aller Quokkatori sei mit $\mathcal{T}_Q$ bezeichnet.*
- *Sei T_0 die Gruppe der Diagonalmatrizen in G. T_0 ist ein maximaler F-stabiler Torus und $W = N_G(T_0)/T_0 \cong S_n$ ist die* Weylgruppe *von G, hier identifiziert mit der Symmetrischen Gruppe S_n.*
- *Zwei Permutaionsmatrizen $w, w' \in W$ heißen $F-$*konjugiert*, falls ein $h \in W$ existiert mit $w' = h^{-1}wF(h)$. Dies liefert eine Äquivalenzrelation, die $F-$Konjugation.*

Die $F-$Konjugiertenklassen entsprechen den $GL(n,q)-$Konjugiertenklassen der Permutationsmatrizen und damit den S_n-Konjugiertenklassen der S_n. Die Zykelstruktur ist trennende Invariante der Konjugationsoperation. Die $F-$Konjugiertenklassen stehen in Bijektion zu den $GL(n,q)-$Konjugiertenklassen der $F-$stabilen maximalen Tori von G. Ein Beweis und eine Konstruktion der Bijektion ist in [8], Lemma 2.1 zu finden.

Definition 8.3 *Eine* Quokkaklasse *oder* Q-Klasse *C sei eine $F-$Konjugiertenklasse von W, die durch eine $GL(n,q)$-Konjugiertenklasse von Quokkatori über die Bijektion induziert wird. Einen induzierenden Quokkatorus bezeichnen wir mit $T_C \in \mathcal{T}_Q$.*

Die Menge der Quokkaklassen sei $\mathcal{C}_Q$.

In [8] haben Alice Niemeyer und Cheryl Praeger eine Formel für die Proportion einer Quokkamenge gezeigt.

Satz 8.4 *Es gilt*

$$\frac{|Q|}{|GL(n,q)|} = \sum_{C \in C_Q} \frac{|C|}{|S_n|} \cdot \frac{|T_C^F \cap Q|}{|T_C^F|} .$$

8.1 Eigenwert-frei Elemente

Wir diskutieren die Anwendung der Quokka-Methode für die Proportionen Eigenwert-freier Matrizen.

Definition 8.5

- *Wir definieren die Quokka-Menge*

$$Q_n := S^1(GL(n,q)) = \{g \in GL(n,q) |\ g \text{ hat keine Eigenwerte}\}.$$

- *Vertreter der $F-$Konjugiertenklassen der Weylgruppe ($W = S_n$ identifiziert), hier also S_n-Konjugiertenklassen von S_n, sind durch Partitionen*

$$\alpha = (\alpha_1, ..., \alpha_s)$$

von n gegeben ($1 \leq \alpha_1 \leq ... \leq \alpha_s$, $\sum_{i=1}^{s} \alpha_i = n$). Der Vertreter ist dann eine Permutation mit Zykelstruktur α:

$$c_\alpha := (1, ..., \alpha_1)(\alpha_1 + 1, ..., \alpha_1 + \alpha_2) \cdot ... \cdot (\alpha_1 + ... + \alpha_{s-1}, ..., n).$$

- *Sei α eine Partition von n und C die $F-$ bzw. S_n-Konjugiertenklasse, wobei c_α als Permutationsmatrix aufgefasst wird. Dann bezeichnen wir mit $T_\alpha := T_c$ den korrespondierenden Torus.*

Eine Konjugiertenklasse $C = {}^{S_n}c_\alpha$ ist genau dann eine Quokkaklasse, wenn die Partition α keinen Teile der Größe 1 hat, d.h. $\alpha_1 > 1$. Dies ist der Fall, denn die Teile einer Partition korrespondieren mit den Blockgrößen der Permutaionsmatrizen. und diese wiederum geben die Eigenwerte an. Die Bedingung $\alpha_1 > 1$ gilt also genau dann, wenn c_α 1-satt ist. Die Menge der Quokkaklassen steht in Bijektion zu

$$A_n^1 := \{\alpha = (\alpha_1, ..., \alpha_s) \mid \alpha \text{ ist Partition von } n,\ 1 < \alpha_1 \leq \alpha_2 \leq ... \leq \alpha_s,\ s \in \mathbb{N}\}.$$

Nach Satz 8.4 gilt nun Folgendes.

Satz 8.6 *Es gilt*

$$\frac{|Q_n|}{|GL(n,q)|} = \sum_{\alpha \in A_n^1} \frac{|{}^{S_n}c_\alpha|}{|S_n|} \frac{|T_\alpha^F \cap Q_n|}{|T_\alpha^F|}.$$

Mit diesem Satz haben wir die Proportion in zwei Bereiche aufgeteilt, die Proportionen $\frac{|{}^{S_n}c_\alpha|}{|S_n|}$ in der Symmetrische Gruppe und die Proportionen $\frac{|T_\alpha^F \cap Q_n|}{|T_\alpha^F|}$ in abelschen Gruppen.

Die vorkommenden Zykel oder Permutationsmatrizen im ersten Bereich sind genau die Fixpunkt-freien Elemente (Derangements) beziehungsweise Vertreter dieser. Deren Proportion haben wir bereits im 1. Kapitel ermittelt. Es gilt

$$\sum_{\alpha \in A_n^1} \frac{|{}^{S_n}c_\alpha|}{|S_n|} \approx e^{-1}.$$

(Siehe Satz 1.5 (i).)

Wir wollen nun versuchen, im zweiten Bereich die Proportionen in gewissen Tori passend abzuschätzen. Wir müssen allerdings eine (untere) Schranke finden, die für steigendes n gegen 1 konvergiert. Wie wir sehen werden, müssen wir dafür aber die Vertreter, über die wir summieren, beschränken. Schwierig wird es dann, noch zu gewährleisten, dass die Proportion der ausgewählten Vertreter im ersten Bereich gegen e^{-1} konvergiert. Dies können wir tatsächlich nicht erreichen.

Betrachten wir zunächst den zweiten Bereich, Proportionen in gewissen *Tori*.

Definition 8.7 *Wir definieren die Abbildung*

$$g : A_n^1 \to [0,1],\ \alpha \mapsto \frac{|T_\alpha^F \cap Q_n|}{|T_\alpha^F|}.$$

Lemma 8.8 *Sei α eine Partition von n.*
Dann gilt:

(i) Der $F-$fixierte Anteil eines Torus hat die Form

$$T_\alpha^F \cong \mathbb{F}_{q^{\alpha_1}}^* \times ... \times \mathbb{F}_{q^{\alpha_s}}^*,$$

(ii) Der Schnitt mit der Quokkamenge $T_\alpha^F \cap Q_n$ steht in Bijektion zu

$$(\mathbb{F}_{q^{\alpha_1}} \setminus \mathbb{F}_q) \times ... \times (\mathbb{F}_{q^{\alpha_s}} \setminus \mathbb{F}_q).$$

(iii) Damit ist

$$g(\alpha) = \frac{|Q_n \cap T_\alpha|}{|T_\alpha|} = \prod_{i=1}^{s} \frac{q^{\alpha_i} - q}{q^{\alpha_i} - 1},$$

(iv) und $\alpha \in A_n^1 \Leftrightarrow g(\alpha) = 0 \Leftrightarrow \alpha_1 = 1$.

(v) Außerdem ist $g(\alpha) = \prod_{i=1}^{s} \frac{q^{\alpha_i}-q}{q^{\alpha_i}-1} = \prod_{i=1}^{s}(1-(q^{\alpha_i-1}+q^{\alpha_i-2}+...+1)^{-1})$,

(vi) und $g(\alpha) \leq \frac{q^{\alpha_i}-q}{q^{\alpha_i}-1} < 1$ *für alle* $i \in \{1,...,s\}$.

Beweis: Zu (i): Man siehe [8], Abschnitt 3.1. Der Torus T_α enthält die Blockdiagonalmatrizen in G mit Blockgrößen α_1 bis α_s. Die jeweiligen Blöcke sind, als Matrizen kleineren Grades aufgefasst, halbeinfach mit irreduziblem Minimalpolynom (über $\mathbb{F}_q$). Somit korrespondieren die Blöcke mit jeweils einem Eigenwert. Für Elemente aus $T_\alpha^F = T_\alpha \cap GL(n,q)$ bedeutet dies, dass die Eigenwerte des $i-$ten Blockes Elemente von $\mathbb{F}_{q^{\alpha_i}}$ seien müssen. Damit folgt die angegebene Isomorphie.

(ii) folgt sofort aus (i), denn charakteristisches und Minimalpolynom eines 1-satten Elementes müssen selbst 1-satt sein.

(iii) und (iv) lassen sich dann leicht berechnen.

Zu (v): Man wende die abbrechende geometrische Reihe an:

$$\begin{aligned} g(\alpha) &= \prod_{i=1}^{s} \frac{q^{\alpha_i}-q}{q^{\alpha_i}-1} \\ &= \prod_{i=1}^{s}(1-\frac{q-1}{q^{\alpha_i}-1}) \\ &= \prod_{i=1}^{s}(1-(q^{\alpha_i-1}+q^{\alpha_i-2}+...+1)^{-1}). \end{aligned}$$

(vi) ist klar wegen $\frac{q^{\alpha_i}-q}{q^{\alpha_i}-1} < 1$ für alle i. □

Insgesamt muss also

$$\frac{|Q_n|}{|GL(n,q)|} = \sum_{\alpha \in A_n^1} \frac{|^{S_n}c_\alpha|}{|S_n|} \prod_{i=1}^{s} \frac{q^{\alpha_i}-q}{q^{\alpha_i}-1}$$

berechnet oder abgeschätzt werden. Die Komplexität des Ausdrucks ist erkennbar. Wir sehen keinen Weg, den Ausdruck direkt zu berechnen. Also müssen wir versuchen, $\frac{|Q_n|}{|GL(n,q)|}$ abzuschätzen.

Bemerkung 8.9 *(Obere Schranke)*
Es gilt $g(\alpha) < 1$ *für alle Partitionen* α*, also ist eine obere Schranke gegeben durch*

$$\frac{|Q_n|}{|GL(n,q)|} < \sum_{\alpha \in A_n^1} \frac{|^{S_n}c_\alpha|}{|S_n|} = |\{\pi \in S_n |\ \pi \textit{ ist Fixpunkt-frei}\}| =$$

$$\sum_{k=0}^{n} \frac{(-1)^k}{k!} = \frac{1}{e} + O(\frac{1}{(n+1)!}).$$

Die untere Schranke stellt uns vor größere Probleme. Die „schlimmsten“ Partitionen, die auftreten können, bestehen aus vielen kleinen Teilen wie zum Beispiel $(2,2,...)$, denn $g((2,2,..))$ ist Produkt vieler kleiner Faktoren. Sei n gerade, dann könnten wir die Proportionen der Tori folgendermaßen abschätzen:

$$g(\alpha) \geq g((2,2,...)) = (\frac{q^2-q}{q^2-1})^{\frac{n}{2}} = (1-\frac{1}{q+1})^{\frac{n}{2}} \text{ für alle } \alpha \in A_n^1.$$

Für ungerade n ist die Schranke praktisch gleich - der letzte auftretende Teil in der schlimmsten Partition ist 3 anstatt 2. In jedem Fall sind die Schranken eine Nullfolge in n. Diese Abschätzung

können wir also nicht verwenden. Die schlimmen Partitionen ((2, 2, ...) und ähnliche) müssen also gesondert betrachtet werden oder gar nicht beachtet werden. Eine gesonderte Betrachtung ist wiederum aufwendig bis unmöglich, da man ähnlich wie oben eine unübersehbare Anzahl an „schlimmen“ Partitionen finden kann. Die einzige Möglichkeit, die wir sehen, ist es, eine Teilmenge $\tilde{A}_n^1 \subsetneq A_n^1$ auszuwählen. Es gilt sicher

$$\frac{|Q_n|}{|GL(n,q)|} \geq \sum_{\alpha \in \tilde{A}_n^1} \frac{|c_\alpha^{GL(n,q)}|}{|S_n|} \cdot g(\alpha).$$

Wir müssten aber weiterhin erreichen, dass gilt

$$\sum_{\alpha \in \tilde{A}_n^1} \frac{|c_\alpha^{GL(n,q)}|}{|S_n|} \to e^{-1},\ n \to \infty,$$

und wir andererseits eine gegen 1 konvergierende Folge $(a_n)_{n\in\mathbb{N}}$ finden, sodass $g(\alpha) \geq a_n$ für alle $\alpha \in \tilde{A}_n^1$ gilt.

Wir diskutieren einen Ansatz.

Lemma 8.10 *Sei $\alpha \in A_n^1$.*

(i) Sei zusätzlich α strikt (d.h. $1 < \alpha_1 < ... < \alpha_s$). Dann gilt

$$g(\alpha) \geq (1 - \frac{1}{q}).$$

(ii) α enthalte nicht mehr als k gleiche Teile. Es folgt

$$g(\alpha) \geq (1 - \frac{1}{q})^k.$$

Beweis: Zu (i): Die Funktion

$$x \mapsto \frac{q^x - q}{q^x - 1}$$

ist monoton steigend in $x \geq 1$. Die Partition $\alpha \in A_n^1$ ist strikt und damit gilt $\alpha_i \geq i + 1$ für alle $i = 1, ..., s$. Wir erhalten

$$g(\alpha) \geq \prod_{i=1}^{s} \frac{q^{s+1} - q}{q^{s+1} - 1} = \frac{q^s(q-1)}{q^{s+1} - 1} = 1 - \frac{q-1}{q^{s+1} - 1}.$$

Wegen $\frac{q-1}{q^{s+1}-1} \leq \frac{q}{q^{s+1}} \leq \frac{1}{q}$ können wir insgesamt abschätzen:

$$g(\alpha) \geq (1 - \frac{1}{q})$$

(ii) ergibt sich durch eine leichte Variation der gleichen Argumente. □

Zur letzten Aussage bietet sich die Betrachtung des Spezialfalls $k = q$ an, denn es ist

$$(1 - \frac{1}{q})^q \approx e^{-1}.$$

Die Permutationen, die $g(\alpha) \geq (1 - \frac{1}{q})^q$ nicht erfüllen (bzw. unter Umständen nicht erfüllen) sind gegeben durch das nächste Lemma.

Lemma 8.11 *Sei $n \geq q+1$.*

(i) Sei $1 \leq k \leq \lfloor \frac{n}{q+1} \rfloor$. Die Proportion der Permutationen mit $q+1$ oder mehr k-Zykeln (als Produkt von disjunkten Zykeln) ist $\frac{1}{(q+1)!}k^{-(q+1)}$.

(ii) Die Proportion aller Permutationen mit q+1 oder mehr k- Zykeln für ein $k \in \{2, ..., \lfloor \frac{n}{q+1} \rfloor\}$ sei bezeichnet mit p. Es gilt

$$p \leq \frac{1}{(q+1)!} \sum_{i=2}^{\lfloor \frac{n}{q+1} \rfloor} k^{-(q+1)} \leq \frac{1}{(q+1)! \cdot q}.$$

Beweis: Zu (i): Die Anzahl der Permutationen ist gegeben durch

$$\binom{n}{k} \cdot (k-1)! \cdot \binom{n-k}{k} \cdot (k-1)! \cdot ... \cdot \binom{n-(q-1)k}{k} \cdot (k-1)! \cdot \frac{1}{(q+1)!} \cdot (n-(q+1)k)! = n! \cdot \frac{1}{(q+1)!} \cdot k^{-(q+1)}$$

Zu (ii):Es gilt

$$p \cdot (q+1)! \leq \sum_{i=2}^{\lfloor \frac{n}{q+1} \rfloor} k^{-(q+1)} \leq \int_1^{\lfloor \frac{n}{q+1} \rfloor} k^{-(q+1)} dk = -\frac{1}{q} k^{-q} \Big|_{k=1}^{k=\lfloor \frac{n}{q+1} \rfloor} \leq \frac{1}{q} 1^{-q} \; = \; \frac{1}{q}$$

□

Satz 8.12 *(Untere Schranke)*
Für $n \geq q = 1$ ist eine untere Schranke gegeben durch

$$\frac{|Q_n|}{|GL(n,q)|} \; \gtrapprox \; \frac{1}{e}(1 - \frac{1}{(q+1)!q})(1 - \frac{1}{q})^q \; = \; e^{-\frac{1}{2}} \cdot (1 - \frac{1}{(q+1)!q})(1 - \frac{1}{2}q^{-1} + O(q^{-2})) \approx \frac{1}{e^2}$$

Beweis: Für eine Partition $\alpha \in A_n^1$, für die c_α höchstens q Zykel von gleicher Länge hat, gilt $g(\alpha) \geq (1 - \frac{1}{q})^q$ nach Lemma 8.10 (ii). Dieser Wert konvergiert für q gegen unendlich gegen e^{-1}, genauer können wir entwickeln:

$$g(\alpha) \geq (1 - \frac{1}{q})^q = e^{-1} \cdot (1 - \frac{1}{2}q^{-1} + O(q^{-2})).$$

Die Proportion aller Permutationen in S_n, die höchstens q Zykel gleicher Länge haben, ist $1 - p \leq 1 - \frac{1}{(q+1)!q}$ nach Lemma 8.11 (ii). Davon können nur die Permutationen ohne Fixpunkte betrachtet werden. Deren Proportion in der S_n ist circa e^{-1}, mit einer Abweichung $O(\frac{1}{(n+1)!}$. Wir betrachten die Menge

$$\tilde{A_n^1} := \{\alpha \in A_n^1 \mid g(\alpha) \geq (1 - \frac{1}{q})^q\}.$$

Die Proportion der Permutationen, deren Zykeltypen beziehungsweise Partitionen in $\tilde{A_n^1}$ liegen, können wir mit

$$\frac{1}{e}(1 - \frac{1}{(q+1)! \cdot q})$$

eine gute untere Näherung angeben.

Eine untere Näherung für die Proportion der Quokkamenge ist dann, mit eier Abweichung $O(\frac{1}{(n+1)!}$,

$$\frac{|Q_n|}{|GL(n,q)|} \gtrapprox \frac{1}{e}(1 - \frac{1}{(q+1)! \cdot q}) \cdot (1 - \frac{1}{q})^q = e^{-\frac{1}{2}} \cdot (1 - \frac{1}{(q+1)!q})(1 - \frac{1}{2}q^{-1} + O(q^{-2})).$$

□

Diese Schranke ist schlechter als die in [7] und Kapitel 3 angegebene. Das Problem ist, dass der erste Teil der Summe (Proportion aller Permutationen ohne Fixpunkte) circa e^{-1} ist. Der zweite Teil müsste also etwa gegen 1 abgeschätzt werden. Dafür muss man sich aber auf einige gute Partitionen beschränken, was wiederum im ersten Teil eine (konstante) Abweichung von e^{-1} bedingt. Es existieren viele, von n unabhängige Partitionen α, für die $g(\alpha)$ klein ist („schlimme“ Partitionen). Diese tragen also wenig zur Summe bei, müssen aber betrachtet werden. Dies macht die Abschätzung des zweiten Teils schwierig bis unmöglich. Wir sehen keine Möglichkeit mit Hife von Quokkamengen die Proportion 1-satter Matrizen zu zählen.

8.2 Eine obere Schanke für die Proportion b-satter Elemente

Die Bemerkung 8.9 lässt sich leicht auch auf b-satte Elemente anwenden.

Definition 8.13

- *Wir definieren die Quokka-Menge*

$$Q_n^b := S^b(GL(n,q)) = \{g \in GL(n,q) |\ g\ b-satt\}.$$

- *Vertreter der Quokkaklassen der Weylgruppe $W = S_n$ (hier: S_n-Konjugiertenklassen von b-satten Permutationen) sind durch Partitionen*

$$\alpha = (\alpha_1, ..., \alpha_s)$$

von n gegeben ($b < \alpha_1 \leq ... \leq \alpha_s$, $\sum_{i=1}^{s} \alpha_i = n$). Der Vertreter ist dann eine Permutation mit Zykelstruktur α:

$$c_\alpha := (1, ..., \alpha_1)(\alpha_1 + 1, ..., \alpha_1 + \alpha_2) \cdot ... \cdot (\alpha_1 + ... + \alpha_{s-1}, ..., n).$$

- *Die Menge der Quokkaklassen steht in Bijektion zu*

$$A_n^b := \{\alpha = (\alpha_1, ..., \alpha_s) \mid \alpha \text{ ist Partition von } n,\ b < \alpha_1 \leq \alpha_2 \leq ... \leq \alpha_s,\ s \in \mathbb{N}\}.$$

Satz 8.14 *Nach Satz 8.4 gilt*

$$\frac{|Q_n^b|}{|GL(n,q)|} = \sum_{\alpha \in A_n^b} \frac{|^{S_n}c_\alpha|}{|S_n|} \frac{|T_\alpha^F \cap Q_n|}{|T_\alpha^F|},$$

wobei T_α den Quokkatori zur Quokkaklasse mit Vertreter c_α bezeichne.

Die Proportionen in den Tori lassen sich ohne Schrierigkeiten jeweils gegen 1 abschätzen. Wir erhalten damit sofort eine obere Schranke, die wir mit den Methoden in den vorherigen Kapiteln (über Potenzreihen) nicht so leicht erhalten könnten.

Satz 8.15 *(Obere Schranke)*
Es gilt

$$v^b(GL(n,q)) = \frac{|Q_n|}{|GL(n,q)|} \ < \ \sum_{\alpha \in A_n^b} \frac{|^{S_n}c_\alpha|}{|S_n|} \ = \ |\frac{\{\pi \in S_n |\ \pi \text{ ist b-satt}\}|}{|S_n|}.$$

Damit gilt

$$v^b(GL, \infty, q) \leq e^{-\sum_{k=1}^{b} \frac{1}{k}}.$$

Beweis: Die Proportion b-satter Permutationen konvergiert nach Satz 1.5 (iii) gegen

$$e^{-\sum_{k=1}^{b} \frac{1}{k}}.$$

□

Für die anderen klassischen Gruppen sollten sich ähnliche Schranken, abhängig von den jeweiligen Weylgruppen, ermitteln lassen. Eine gute untere Schranke, die möglicherweise interessanter wäre, lässt sich so aber leider nicht finden.

Anhang A

Generelle Lineare Gruppen

Die Proportionen b-satter Elemente konvergieren gegen $v^b(GL, \infty, q) = e^{-\sum_{k=1}^{\infty} 1/k} (1 + O(q^{-1}))$.
Die auftretenden Fehlerterme sind für $b \in \{1, ..., 24\}$ folgende:
(Maple-Ausdruck)

$b = 1$: $1 - 1/2\,q^{-1} + \frac{7}{24}\,q^{-2} - \frac{25}{48}\,q^{-3} + \frac{4583}{5760}\,q^{-4} - \frac{13907}{11520}\,q^{-5} + \frac{900367}{580608}\,q^{-6} - \frac{10103633}{5806080}\,q^{-7} + O\left(q^{-8}\right)$

$b = 2$: $1 - \frac{7}{12}\,q^{-2} + 1/3\,q^{-3} + \frac{77}{1440}\,q^{-4} - \frac{59}{180}\,q^{-5} + \frac{26371}{362880}\,q^{-6} + \frac{7211}{30240}\,q^{-7} - \frac{3036983}{12441600}\,q^{-8} + O\left(q^{-9}\right)$

$b = 3$: $1 - 1/4\,q^{-2} - 1/6\,q^{-3} - \frac{41}{480}\,q^{-4} + \frac{49}{120}\,q^{-5} - \frac{17009}{40320}\,q^{-6} + \frac{1319}{20160}\,q^{-7} + \frac{354079}{1075200}\,q^{-8} + O\left(q^{-9}\right)$

$b = 4$: $1 - 1/6\,q^{-3} - \frac{59}{120}\,q^{-4} + \frac{11}{30}\,q^{-5} - \frac{37}{504}\,q^{-6} + \frac{1133}{5040}\,q^{-7} + \frac{41}{28800}\,q^{-8} - \frac{57311}{113400}\,q^{-9} + O\left(q^{-10}\right)$

$b = 5$: $1 - 1/6\,q^{-3} - \frac{7}{24}\,q^{-4} + 1/15\,q^{-5} - \frac{37}{504}\,q^{-6} + \frac{193}{1008}\,q^{-7} - \frac{31}{1152}\,q^{-8} - \frac{2021}{45360}\,q^{-9} + O\left(q^{-10}\right)$

$b = 6$: $1 - 1/8\,q^{-4} - 1/10\,q^{-5} - \frac{85}{252}\,q^{-6} + 1/7\,q^{-7} - \frac{97}{1920}\,q^{-8} + \frac{161}{720}\,q^{-9} + \frac{40427}{554400}\,q^{-10} + O\left(q^{-11}\right)$

$b = 7$: $1 - 1/8\,q^{-4} - 1/10\,q^{-5} - \frac{7}{36}\,q^{-6} - 1/14\,q^{-7} - \frac{97}{1920}\,q^{-8} + \frac{161}{720}\,q^{-9} + \frac{4361}{79200}\,q^{-10} + O\left(q^{-11}\right)$

$b = 8$: $1 - 1/10\,q^{-5} - \frac{7}{36}\,q^{-6} - 1/14\,q^{-7} - \frac{59}{240}\,q^{-8} + \frac{19}{90}\,q^{-9} + \frac{203}{6600}\,q^{-10} + \frac{437}{3960}\,q^{-11} + O\left(q^{-12}\right)$

$b = 9$: $1 - 1/10\,q^{-5} - 1/12\,q^{-6} - 1/14\,q^{-7} - \frac{59}{240}\,q^{-8} + \frac{2}{45}\,q^{-9} + \frac{203}{6600}\,q^{-10} + \frac{131}{1320}\,q^{-11} + O\left(q^{-12}\right)$

$b = 10$: $1 - 1/12\,q^{-6} - 1/14\,q^{-7} - \frac{7}{48}\,q^{-8} - 1/18\,q^{-9} - \frac{41}{330}\,q^{-10} + 1/11\,q^{-11} - \frac{8027}{43680}\,q^{-12} + O\left(q^{-13}\right)$

$b = 11$: $1 - 1/12\,q^{-6} - 1/14\,q^{-7} - \frac{7}{48}\,q^{-8} - 1/18\,q^{-9} - 1/30\,q^{-10} - 1/22\,q^{-11} - \frac{8027}{43680}\,q^{-12} + O\left(q^{-13}\right)$

$b = 12$: $1 - 1/14\,q^{-7} - 1/16\,q^{-8} - 1/18\,q^{-9} - \frac{7}{60}\,q^{-10} - 1/22\,q^{-11} - \frac{10229}{32760}\,q^{-12} + \frac{27}{182}\,q^{-13} + O\left(q^{-14}\right)$

$b = 13$: $1 - 1/14\,q^{-7} - 1/16\,q^{-8} - 1/18\,q^{-9} - \frac{7}{60}\,q^{-10} - 1/22\,q^{-11} - \frac{593}{2520}\,q^{-12} + \frac{3}{91}\,q^{-13} + O\left(q^{-14}\right)$

$b = 14$: $1 - 1/16\,q^{-8} - 1/18\,q^{-9} - \frac{7}{60}\,q^{-10} - 1/22\,q^{-11} - \frac{59}{360}\,q^{-12} - 1/26\,q^{-13} - \frac{1}{60}\,q^{-14} + O\left(q^{-15}\right)$

$b = 15$: $1 - 1/16\,q^{-8} - 1/18\,q^{-9} - 1/20\,q^{-10} - 1/22\,q^{-11} - \frac{7}{72}\,q^{-12} - 1/26\,q^{-13} - 1/12\,q^{-14} + O\left(q^{-15}\right)$

$b = 16$: $1 - 1/18\,q^{-9} - 1/20\,q^{-10} - 1/22\,q^{-11} - \frac{7}{72}\,q^{-12} - 1/26\,q^{-13} - 1/12\,q^{-14} + 1/45\,q^{-15} + O\left(q^{-16}\right)$

$b = 17$: $1 - 1/18\,q^{-9} - 1/20\,q^{-10} - 1/22\,q^{-11} - \frac{7}{72}\,q^{-12} - 1/26\,q^{-13} - 1/12\,q^{-14} + 1/45\,q^{-15} + O\left(q^{-16}\right)$

$b = 18$: $1 - 1/20\,q^{-10} - 1/22\,q^{-11} - 1/24\,q^{-12} - 1/26\,q^{-13} - 1/12\,q^{-14} - 1/30\,q^{-15} - \frac{59}{480}\,q^{-16} + O\left(q^{-17}\right)$

$b = 19$: $1 - 1/20\,q^{-10} - 1/22\,q^{-11} - 1/24\,q^{-12} - 1/26\,q^{-13} - 1/12\,q^{-14} - 1/30\,q^{-15} - \frac{59}{480}\,q^{-16} + O\left(q^{-17}\right)$

$b = 20$: $1 - 1/22\,q^{-11} - 1/24\,q^{-12} - 1/26\,q^{-13} - 1/12\,q^{-14} - 1/30\,q^{-15} - \frac{7}{96}\,q^{-16} - 1/34\,q^{-17} + O\left(q^{-18}\right)$

$b = 21$: $1 - 1/22\,q^{-11} - 1/24\,q^{-12} - 1/26\,q^{-13} - 1/28\,q^{-14} - 1/30\,q^{-15} - \frac{7}{96}\,q^{-16} - 1/34\,q^{-17} + O\left(q^{-18}\right)$

$b = 22$: $1 - 1/24\,q^{-12} - 1/26\,q^{-13} - 1/28\,q^{-14} - 1/30\,q^{-15} - \frac{7}{96}\,q^{-16} - 1/34\,q^{-17} - \frac{7}{108}\,q^{-18} + O\left(q^{-19}\right)$

$b = 23$: $1 - 1/24\,q^{-12} - 1/26\,q^{-13} - 1/28\,q^{-14} - 1/30\,q^{-15} - \frac{7}{96}\,q^{-16} - 1/34\,q^{-17} - \frac{7}{108}\,q^{-18} + O\left(q^{-19}\right)$

$b = 24$: $1 - 1/26\,q^{-13} - 1/28\,q^{-14} - 1/30\,q^{-15} - 1/32\,q^{-16} - 1/34\,q^{-17} - \frac{7}{108}\,q^{-18} - 1/38\,q^{-19} + O\left(q^{-20}\right)$

Anhang B

Matrixring

Die Proportionen b-satter Elemente konvergieren gegen $v^b(M,\infty,q) = e^{-\sum_{k=1}^{\infty} 1/k}\,(1+O(q^{-1}))$.
Die auftretenden Fehlerterme sind für $b \in \{1,...,24\}$ folgende:
(Maple-Ausdruck)

$b=1:$ $1-3/2\,q^{-1}-\frac{5}{24}\,q^{-2}-\frac{5}{16}\,q^{-3}+\frac{5903}{5760}\,q^{-4}-\frac{617}{1280}\,q^{-5}+\frac{4245047}{2903040}\,q^{-6}-\frac{306577}{387072}\,q^{-7}+O\left(q^{-8}\right)$

$b=2:$ $1-q^{-1}-\frac{19}{12}\,q^{-2}+\frac{11}{12}\,q^{-3}+\frac{437}{1440}\,q^{-4}+\frac{137}{480}\,q^{-5}+\frac{125911}{362880}\,q^{-6}+\frac{66061}{72576}\,q^{-7}+O\left(q^{-8}\right)$

$b=3:$ $1-q^{-1}-5/4\,q^{-2}+1/12\,q^{-3}+\frac{53}{160}\,q^{-4}+\frac{797}{480}\,q^{-5}-\frac{30029}{40320}\,q^{-6}+\frac{11141}{13440}\,q^{-7}+O\left(q^{-8}\right)$

$b=4:$ $1-q^{-1}-q^{-2}-1/6\,q^{-3}-\frac{13}{40}\,q^{-4}+\frac{81}{40}\,q^{-5}+\frac{13}{252}\,q^{-6}+\frac{313}{336}\,q^{-7}+O\left(q^{-8}\right)$

$b=5:$ $1-q^{-1}-q^{-2}-1/6\,q^{-3}-1/8\,q^{-4}+\frac{61}{40}\,q^{-5}+\frac{191}{1260}\,q^{-6}+\frac{671}{560}\,q^{-7}+O\left(q^{-8}\right)$

$b=6:$ $1-q^{-1}-q^{-2}-1/8\,q^{-4}+\frac{41}{40}\,q^{-5}-\frac{283}{2520}\,q^{-6}+\frac{1991}{1260}\,q^{-7}+O\left(q^{-8}\right)$

$b=7:$ $1-q^{-1}-q^{-2}-1/8\,q^{-4}+\frac{41}{40}\,q^{-5}+\frac{11}{360}\,q^{-6}+\frac{1541}{1260}\,q^{-7}+O\left(q^{-8}\right)$

$b=8:$ $1-q^{-1}-q^{-2}+\frac{9}{10}\,q^{-5}-\frac{17}{180}\,q^{-6}+\frac{1541}{1260}\,q^{-7}+O\left(q^{-8}\right)$

$b=9:$ $1-q^{-1}-q^{-2}+\frac{9}{10}\,q^{-5}+\frac{1}{60}\,q^{-6}+\frac{467}{420}\,q^{-7}+O\left(q^{-8}\right)$

$b=10:$ $1-q^{-1}-q^{-2}+q^{-5}-1/12\,q^{-6}+\frac{85}{84}\,q^{-7}+O\left(q^{-8}\right)$

$b=11:$ $1-q^{-1}-q^{-2}+q^{-5}-1/12\,q^{-6}+\frac{85}{84}\,q^{-7}+O\left(q^{-8}\right)$

$b=12:$ $1-q^{-1}-q^{-2}+q^{-5}+\frac{13}{14}\,q^{-7}+O\left(q^{-8}\right)$

$b=13:$ $1-q^{-1}-q^{-2}+q^{-5}+\frac{13}{14}\,q^{-7}+O\left(q^{-8}\right)$

$b=14:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-8}\right)$

$b=15:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-8}\right)$

$b=16:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-9}\right)$

$b=17:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-9}\right)$

$b=18:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-10}\right)$

$b=19:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-10}\right)$

$b=20:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-11}\right)$

$b=21:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-11}\right)$

$b=22:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-12}\right)$

$b=23:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-12}\right)$

$b=24:$ $1-q^{-1}-q^{-2}+q^{-5}+q^{-7}+O\left(q^{-12}\right)$

Anhang C

Symplektische und Orthogonale Gruppen

Die Proportionen b-satter Elemente konvergieren gegen $v^b(Sp,\infty,q) = e^{-\frac{1}{2}\sum_{k=1}^{\infty} 1/k}\left(1+O(q^{-1})\right)$ beziehungsweise $v^b(O^\epsilon,\infty,q) = \frac{1}{2}e^{-\frac{1}{2}\sum_{k=1}^{\infty} 1/k}\left(1+O(q^{-1})\right)$. Die auftretenden Fehlerterme sind für $b \in \{1,...,24\}$ folgende:
(Maple-Ausdruck, q gerade)

$b=1:$ $1-3/4\,q^{-1}+\frac{59}{96}\,q^{-2}-\frac{153}{128}\,q^{-3}+\frac{158399}{92160}\,q^{-4}-\frac{280147}{122880}\,q^{-5}+\frac{511781383}{185794560}\,q^{-6}+O\left(q^{-7}\right)$

$b=2:$ $1-3/4\,q^{-1}+\frac{23}{96}\,q^{-2}-\frac{53}{128}\,q^{-3}+\frac{78359}{92160}\,q^{-4}-\frac{186107}{122880}\,q^{-5}+\frac{240615019}{185794560}\,q^{-6}+O\left(q^{-7}\right)$

$b=3:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{33533}{30720}\,q^{-4}-\frac{59209}{40960}\,q^{-5}+\frac{24713987}{20643840}\,q^{-6}+O\left(q^{-7}\right)$

$b=4:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{27773}{30720}\,q^{-4}-\frac{53449}{40960}\,q^{-5}+\frac{28302467}{20643840}\,q^{-6}+O\left(q^{-7}\right)$

$b=5:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{6169}{6144}\,q^{-4}-\frac{12533}{8192}\,q^{-5}+\frac{6292711}{4128768}\,q^{-6}+O\left(q^{-7}\right)$

$b=6:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{5916391}{4128768}\,q^{-6}+O\left(q^{-7}\right)$

$b=7:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{887329}{589824}\,q^{-6}+O\left(q^{-7}\right)$

$b=8:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{887329}{589824}\,q^{-6}+O\left(q^{-7}\right)$

$b=9:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=10:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=11:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=12:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=13:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=14:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=15:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=16:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=17:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=18:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=19:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=20:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=21:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=22:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=23:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

$b=24:$ $1-3/4\,q^{-1}+\frac{13}{32}\,q^{-2}-\frac{101}{128}\,q^{-3}+\frac{2227}{2048}\,q^{-4}-\frac{13045}{8192}\,q^{-5}+\frac{102233}{65536}\,q^{-6}+O\left(q^{-7}\right)$

(Maple-Ausdruck, q ungerade)

$b = 1$: $1 - 5/4\,q^{-1} + \frac{131}{96}\,q^{-2} - \frac{997}{384}\,q^{-3} + \frac{385199}{92160}\,q^{-4} - \frac{2225839}{368640}\,q^{-5} + \frac{1527456799}{185794560}\,q^{-6} + O\left(q^{-7}\right)$

$b = 2$: $1 - 5/4\,q^{-1} + \frac{119}{96}\,q^{-2} - \frac{745}{384}\,q^{-3} + \frac{270359}{92160}\,q^{-4} - \frac{1670119}{368640}\,q^{-5} + \frac{1103940811}{185794560}\,q^{-6} + O\left(q^{-7}\right)$

$b = 3$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{106493}{30720}\,q^{-4} - \frac{611053}{122880}\,q^{-5} + \frac{26763847}{4128768}\,q^{-6} + O\left(q^{-7}\right)$

$b = 4$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{104573}{30720}\,q^{-4} - \frac{601453}{122880}\,q^{-5} + \frac{27433159}{4128768}\,q^{-6} + O\left(q^{-7}\right)$

$b = 5$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{21529}{6144}\,q^{-4} - \frac{127049}{24576}\,q^{-5} + \frac{28787911}{4128768}\,q^{-6} + O\left(q^{-7}\right)$

$b = 6$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{28755655}{4128768}\,q^{-6} + O\left(q^{-7}\right)$

$b = 7$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{4150081}{589824}\,q^{-6} + O\left(q^{-7}\right)$

$b = 8$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{4150081}{589824}\,q^{-6} + O\left(q^{-7}\right)$

$b = 9$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 10$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 11$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 12$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 13$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 14$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 15$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 16$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 17$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 18$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 19$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 20$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 21$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 22$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 23$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

$b = 24$: $1 - 5/4\,q^{-1} + \frac{45}{32}\,q^{-2} - \frac{307}{128}\,q^{-3} + \frac{7347}{2048}\,q^{-4} - \frac{43203}{8192}\,q^{-5} + \frac{464761}{65536}\,q^{-6} + O\left(q^{-7}\right)$

Anhang D

Unitäre Gruppen

Die Proportionen b-satter Elemente konvergieren gegen

$$v^b(U,\infty,q) = e^{-\frac{3}{2}\left(\sum_{1\le k\le b,\ k\ ung.} 1/k\right)-\frac{1}{2}\left(\sum_{1\le k\le b,\ k\ ger.} 1/k\right)}\left(1+O(q^{-1})\right).$$

Die auftretenden Fehlerterme sind für $b \in \{1,...,24\}$ folgende:
(Maple-Ausdruck)

$b=1:$ $1-\frac{7}{12}\,q^{-2}-1/3\,q^{-3}+\frac{77}{1440}\,q^{-4}+\frac{59}{180}\,q^{-5}+\frac{26371}{362880}\,q^{-6}-\frac{7211}{30240}\,q^{-7}+O\left(q^{-8}\right)$

$b=2:$ $1-1/3\,q^{-2}-1/3\,q^{-3}-\frac{157}{360}\,q^{-4}+\frac{11}{45}\,q^{-5}+\frac{12937}{22680}\,q^{-6}-\frac{317}{7560}\,q^{-7}-\frac{3215411}{5443200}\,q^{-8}+O\left(q^{-9}\right)$

$b=3:$ $1-\frac{13}{40}\,q^{-4}-1/5\,q^{-5}-\frac{85}{252}\,q^{-6}-1/7\,q^{-7}-\frac{53}{9600}\,q^{-8}+\frac{277}{1800}\,q^{-9}+O\left(q^{-10}\right)$

$b=4:$ $1-1/5\,q^{-4}-1/5\,q^{-5}-\frac{85}{252}\,q^{-6}-1/7\,q^{-7}-\frac{271}{1200}\,q^{-8}+\frac{29}{225}\,q^{-9}+O\left(q^{-10}\right)$

$b=5:$ $1-\frac{85}{252}\,q^{-6}-1/7\,q^{-7}-\frac{7}{48}\,q^{-8}-1/9\,q^{-9}-\frac{41}{330}\,q^{-10}+O\left(q^{-11}\right)$

$b=6:$ $1-\frac{16}{63}\,q^{-6}-1/7\,q^{-7}-1/16\,q^{-8}-1/9\,q^{-9}-\frac{137}{660}\,q^{-10}-1/11\,q^{-11}+O\left(q^{-12}\right)$

$b=7:$ $1-1/9\,q^{-6}-1/16\,q^{-8}-1/9\,q^{-9}-\frac{137}{660}\,q^{-10}-1/11\,q^{-11}+O\left(q^{-12}\right)$

$b=8:$ $1-1/9\,q^{-6}-1/9\,q^{-9}-\frac{137}{660}\,q^{-10}-1/11\,q^{-11}-\frac{9883}{42120}\,q^{-12}+O\left(q^{-13}\right)$

$b=9:$ $1-\frac{137}{660}\,q^{-10}-1/11\,q^{-11}-\frac{289}{1560}\,q^{-12}-1/13\,q^{-13}+O\left(q^{-14}\right)$

$b=10:$ $1-\frac{26}{165}\,q^{-10}-1/11\,q^{-11}-\frac{289}{1560}\,q^{-12}-1/13\,q^{-13}+O\left(q^{-14}\right)$

$b=11:$ $1-1/15\,q^{-10}-\frac{289}{1560}\,q^{-12}-1/13\,q^{-13}-\frac{1}{60}\,q^{-14}+O\left(q^{-15}\right)$

$b=12:$ $1-1/15\,q^{-10}-\frac{28}{195}\,q^{-12}-1/13\,q^{-13}-\frac{1}{60}\,q^{-14}-1/15\,q^{-15}+O\left(q^{-16}\right)$

$b=13:$ $1-1/15\,q^{-10}-1/15\,q^{-12}-\frac{1}{60}\,q^{-14}-1/15\,q^{-15}+O\left(q^{-16}\right)$

$b=14:$ $1-1/15\,q^{-10}-1/15\,q^{-12}+\frac{2}{105}\,q^{-14}-1/15\,q^{-15}-\frac{49}{544}\,q^{-16}+O\left(q^{-17}\right)$

$b=15:$ $1-1/21\,q^{-14}-\frac{49}{544}\,q^{-16}-1/17\,q^{-17}+O\left(q^{-18}\right)$

$b=16:$ $1-1/21\,q^{-14}-1/17\,q^{-16}-1/17\,q^{-17}+O\left(q^{-18}\right)$

$b=17:$ $1-1/21\,q^{-14}-\frac{2371}{14364}\,q^{-18}+O\left(q^{-19}\right)$

$b=18:$ $1-1/21\,q^{-14}-\frac{493}{3591}\,q^{-18}-1/19\,q^{-19}+O\left(q^{-20}\right)$

$b=19:$ $1-1/21\,q^{-14}-\frac{16}{189}\,q^{-18}+O\left(q^{-20}\right)$

$b=20:$ $1-1/21\,q^{-14}-\frac{16}{189}\,q^{-18}+\frac{4}{525}\,q^{-20}+O\left(q^{-21}\right)$

$b=21:$ $1-1/27\,q^{-18}-1/25\,q^{-20}+O\left(q^{-22}\right)$

$b=22:$ $1-1/27\,q^{-18}-1/25\,q^{-20}+O\left(q^{-22}\right)$

$b=23:$ $1-1/27\,q^{-18}-1/25\,q^{-20}-1/33\,q^{-22}+O\left(q^{-24}\right)$

$b=24:$ $1-1/27\,q^{-18}-1/25\,q^{-20}-1/33\,q^{-22}+O\left(q^{-24}\right)$

Index

Literaturverzeichnis

[1] Armand Borel. *Linear algebraic groups.* Springer-Verlag, 1991.

[2] E.T. Copson. *An introduction to the theory of functions of a complex variable.* Clarendon Press, 1935.

[3] Roger H. Dye. A geometric characterization of the special orthogonal groups and the Dickson invariant. *London Math. Soc.*, 15:472–476, 1977.

[4] Nathan J. Fine und Israel N. Herstein. The Probability that a matrix be nilpotent. *London Math. Soc.*, 15:472–476, 1977.

[5] Osias Gruder. Zur Theorie der Zerlegung von Permutationen in Zykel. *Arkiv för Mathematik*, 2:385–414, 1952.

[6] Frank Lübeck, Alice C. Niemeyer und Cheryl E. Praeger. Finding involutions in finite Lie type groups of odd characteristic. *Journal of Algebra*, 321:3397–3417, 2009.

[7] Peter M. Neumann und Cheryl E. Praeger. Derangements and eigenvalue-free elements in finite classical groups. *J. London Math. Soc.*, 58:564–586, 1998.

[8] Alice C. Niemeyer und Cheryl E. Praeger. Estimating proportions of elements in finite groups of lie type. *Journal of Algebra*, 324:122–145, 2010.

[9] Eamonn A. O'Brien. Towards effective algorithms for linear groups. *Finite Geometries, Groups and Computation*, pages 163–190, 2004.

[10] Eamonn A. O'Brien. Algorithms for matrix groups. *Groups St Andrews 2009 in Bath. LMS Lecture Notes*, 388:297–323, 2011.

[11] Robert Steinberg. *Endomorphisms of linear algebraic groups.* Mem. Amer. Math. Soc. 80, 1968.

[12] Robert Steinberg. *Conjugacy Classes in Algebraic Groups.* Springer-Verlag, 1974.

[13] Donald E. Taylor. *The Geometry of the Classical Groups.* Heldermann-Verlag, 1992.