Abzählungen verschiedener invertierbarer Matrizen über endlichen Körpern

Masterarbeit

zur Erlangung des akademischen Grades
Master of Science
im Studiengang Mathematik
der Naturwissenschaftlich-Technischen Fakultät VI
-Mathematik und Informatik-
der Universität des Saarlandes

von

Ruwen Hollenbach

Saarbrücken, 2015

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Saarbrücken, den 27.01.2015

(*Ruwen Hollenbach*)

Einführung

Die allgemeine lineare Gruppe $GL_n(k)$ vom Grad n über k ist die Gruppe der invertierbaren nxn-Matrizen über k und spielt eine sehr prominente Rolle in der Mathematik, egal welchen Grundkörper k man wählt. Diese Gruppe taucht in natürlicher Weise in allen großen Bereichen, wie zum Beispiel der algebraischen Geometrie und der Zahlentheorie, auf.

Der Name *Allgemeine lineare Gruppe* leitet sich von der Tatsache ab, dass Elemente dieser Gruppe Punkte in allgemeiner linearer Lage wieder auf Punkte in allgemeiner linearer Lage abbilden; die Notation $GL_n(k)$ kommt dabei von der Abkürzung der englischen Bezeichnung "**g**eneral **l**inear group".

In der vorliegenden Arbeit behandeln wir $GL_n(k)$ speziell für endliche Körper. In diesem Fall ist die Gruppe endlich, was uns ermöglicht einige interessante Invarianten mit Hilfe einfacher kombinatorischer Methoden zu ermitteln. Die untersuchten Größen stehen dabei alle im Zusammenhang zu einer besonderen Operation auf $GL_n(k)$ - der Konjugation. Damit bezeichnen wir die Operation von $GL_n(k)$ auf $GL_n(k)$ gegeben durch:

$$GL_n(k) \times GL_n(k) \to GL_n(k), \quad (S, T) \mapsto STS^{-1}.$$

Die Bahnen dieser Operation nennt man Konjugationsklassen und sie werden uns in der einen oder anderen Weise in jedem Kapitel beschäftigen.

Das erste Kapitel stellt die Hilfsmittel, die wir für die meisten Abzählungen benötigen. Im Laufe der Arbeit werden wir feststellen, dass alle Probleme eng mit Partitionen -genauer Partitionsfunktionen- verwoben sind. Aus diesem Grund sammeln wir in 1.1 alle nötigen Notationen und Begrifflichkeiten aus der Theorie der Partitionen. Der Vorteil am Umweg über die Partitionsfunktionen ist, dass diese sehr einfach mit Hilfe erzeugender Funktionen abgezählt werden können. Da diese Abzählungen ein großer Bestandteil dieser Arbeit sind, wird, um die Abgeschlossenheit dieser Arbeit zu gewährleisten, in die Theorie erzeugender Funktionen eingeführt. Dabei wird eine Topologie auf der Menge der erzeugenden Funktionen gegeben, die von einer einfachen Metrik kommt, die in der vorliegenden Arbeit nicht angesprochen wird. Die zusätzliche Arbeit, die durch diese Vorgehensweise entsteht, soll dem Leser einfach nur ein besseres Verständnis der behandelten Struktur vermitteln. Der Leser mit Vorkenntnissen darf Abschnitt 1.2 gerne auslassen; nicht jedoch Abschnitt 1.1, da die Notationen und Bezeichnungen in diesem Bereich von Autor zu Autor stark variieren.

In Kapitel 2 werden wir uns davon überzeugen, dass es eine Bijektion gibt zwischen der Menge der Konjugationsklassen und der Menge der Partitionsfunktionen mit einer einfachen Nebenbedingung. Dabei ist diese Abbildung nicht willkürlich, sondern liefert eine natürliche Parametrisierung der Konjugationsklassen, die wir in späteren Kapiteln nur geeignet modifizieren müssen. In 2.2 zählen wir dann diese besonderen Partitionsfunktionen mit Hilfe erzeugender Funktionen, was uns auf eine schöne Formel für die Anzahl der Konjugationsklassen führt.

Kapitel 3 beschäftigt sich mit der Bestimmung der Größen der verschiedenen Konjugationsklassen, was äquivalent zur Bestimmung der Größen der Zentralisatoren ist. Diese sind aber mit sehr viel mehr Struktur versehen, was uns die Berechnung überhaupt erst ermöglicht. Der Weg zu einer expliziten Formel führt dann weiter über die Interpretation dieser Zentralisatoren als einfache Automorphismengruppen. Die erhaltene Formel wirkt anfänglich sehr unangenehm, nimmt aber in allen behandelten Fällen eine sehr einfache Form an.

In Kapitel 4 untersuchen wir die drei wichtigsten Familien von Matrizen, die invariant unter Konjugation sind. Dabei folgen die drei Unterabschnitte alle dem selbem Muster, das wir am Beispiel der diagonalisierbaren Matrizen veranschaulichen wollen. Zu Beginn bestimmen wir die Anzahl der Konjugationsklassen aus $GL_n(k)$ mit diagonalisierbaren Elementen, indem wir die Parametrisierung aus Kapitel 2.1 passend modifizieren und die modifizierten Partitionsfunktionen dann mit Hilfe erzeugender Funktionen abzählen. Danach zeigen wir, dass die Anzahl der diagonalisierbaren, invertierbaren nxn-Matrizen über $\mathbb{F}_q$ -kurz $D_n(q)$- bei fester Dimension n durch ein Polynom in q gegeben ist. Da wir uns speziell für das asymptotische Verhalten von $D_n(q)$ für $q \to \infty$ interessieren, reicht es deshalb einfach den Leitterm von $D_n(q)$ zu bestimmen. Dasselbe tun wir auch für die jordan-normalisierbaren und halbeinfachen Matrizen. Unsere Asymptotiken liefern dabei folgende Interpretation:
"Für beliebiges aber festes $n \in \mathbb{N}$ geht die Wahrscheinlichkeit, zufällig eine invertierbare diagonalisierbare/ jordan-normalisierbare/ halbeinfache nxn-Matrix auszuwählen, für $q \to \infty$ gegen [...]."

Die erlangten Ergebnisse sind sicherlich nicht neu. Der Anspruch war es lediglich die wichtigsten, arithmetischen Größen, bezüglich der Konjugation, in kohärenter Form in einer Arbeit zusammenzutragen. Dabei erwuchs während der Bearbeitung der zusätzliche Anspruch dies auf möglichst elementare Art und Weise zu tun. Das Resultat ist die vorliegende Arbeit, die mit Hilfe von erzeugenden Funktionen und einer einfachen Proposition (Proposition 4.4) alle angesprochenen Ergebnisse reproduziert, ohne wirklich mehr vom Leser zu verlangen, als die Kenntnis über den Struktursatz endlich erzeugter Moduln über Hauptidealringen.

Danksagung

An dieser Stelle möchte ich mich bei Herrn Gekeler für die Vergabe des interessanten Themas bedanken. Vielmehr danke ich ihm aber für die Gespräche fernab meiner Arbeit; die Gespräche darüber, welche Theorien unverzichtbar für jeden Mathematiker sind, die vielen Buchtipps und die ein oder andere Grammatiklehrstunde. Natürlich gilt mein Dank auch meiner Familie, die mir immer Rückhalt gibt; meinen Freunden weil sie während des Studiums immer für die nötige Ablenkung gesorgt haben und allen anderen die direkt oder indirekt an dieser Arbeit oder dem Erfolg meines Studiums beteiligt waren.

Inhaltsverzeichnis

Symbolverzeichnis

$\mathbb{N}$	$\{0,1,2,\dots\}$
$\mathbb{F}_q$	endlicher Körper mit q Elementen
$Mat_n(K)$	Ring der nxn-Matrizen über K
$GL_n(K)$	Einheitengruppe von $Mat_n(K)$
$End_n(K)$	Endomorphismenring linearer Abbildungen von K^n
$\mathrm{char}(K)$	Charakteristik des Körpers K
$d_n(q)$	Anzahl der Konjugationsklassen von $GL_n(q)$ mit diagonalisierbarem Repräsentanten
$j_n(q)$	Anzahl der Konjugationsklassen von $GL_n(q)$ mit jordan-normalisierbarem Repräsentanten
$s_n(q)$	Anzahl der Konjugationsklassen von $GL_n(q)$ mit halbeinfachem Repräsentanten
$D_n(q)$	Anzahl der diagonalisierbaren Matrizen aus $GL_n(K)$
$J_n(q)$	Anzahl der jordan-normalisierbaren Matrizen aus $GL_n(K)$
$S_n(q)$	Anzahl der halbeinfachen Matrizen aus $GL_n(K)$

1 Vorbereitung

1.1 Partitionen

Partitionen, genauer Partitionsfunktionen, spielen eine Schlüsselrolle in dieser Arbeit. Viele Abzählprobleme werden auf die Abzählung von bestimmten Partitionsfunktionen reduziert. Dieser Abschnitt soll die wichtigsten Begriffe und Notationen bereitstellen.

Eine *Partition* ist eine (endliche oder unendliche) Sequenz

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r, \ldots)$$

nicht-negativer ganzer Zahlen, sodass:

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq \ldots,$$

wobei nur endlich viele ungleich Null sind. Dabei unterscheiden wir nicht zwischen Sequenzen wie z.B (2,1), (2,1,0) oder (2,1,0,0,0, ...).
Die $\lambda_i \neq 0$ bezeichnen wir als die Summanden von λ. Die Anzahl der Summanden $l(\lambda)$ nennt man die *Länge* von λ und die Summe

$$|\lambda| = \lambda_1 + \lambda_2 + \ldots$$

nennt man das *Gewicht* von λ. Ist $|\lambda| = n$, so sagt man, dass λ eine Partition von n ist.

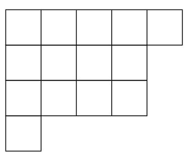
Die Anzahl aller Partitionen von n bezeichnen wir in dieser Arbeit mit $p(n)$. Man kann $p(n)$ nach Belieben modifizieren; eine solche Modifizierung stellt zum Beispiel die Anzahl aller Partitionen mit größtem Summand $\leq k$ dar, bezeichnet mit $p_{\leq k}(n)$.

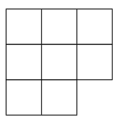
Die Zahl

$$m_i = m_i(\lambda) = |\{j \mid \lambda_j = i\}|$$

nennen wir die *Multiplizität* von i in λ.

Partitionen lassen sich am besten durch Diagramme darstellen und verstehen. Sei $\lambda = (\lambda_1, \lambda_2, \ldots)$. Unter einem Diagramm für λ verstehen wir die Menge von Punkten $(i, j) \in \mathbb{Z}^2$ sodass $-1 \geq j \geq -\lambda_i$. Setzen wir keine Punkte, sondern veranschaulichen jeden Punkt durch ein Kästchen, so erhalten wir ein sogenanntes Young-Diagramm oder Young-Tableau. Für die Partitionen (5,4,4,1) und (3,3,2) sehen die Young-Diagramme wie folgt aus:





Diese Darstellung einer Partition legt die Definition einer *konjugierten Partition* nahe. Darunter verstehen wir die Partition $\lambda' = (\lambda'_1, \lambda'_2, \dots)$, wobei λ'_i die Anzahl der Kästchen in der i-ten Spalte ist. Genauer gilt also

$$\lambda'_i := \left|\{j \in \mathbb{N} \mid \lambda_j \geq i\}\right|.$$

Offensichtlich hat man

$$m_i(\lambda) = \lambda'_i - \lambda'_{i+1}.$$

Des Weiteren definieren wir

$$n(\lambda) := \sum_{i \geq 1} (i-1)\lambda_i.$$

Schreiben wir im Young-Diagramm in alle Kästchen in der ersten Zeile eine Null, in alle Kästchen der zweiten Zeile eine Eins usw. so ist $n(\lambda)$ die Summe der Einträge. Summieren wir nun über die Spalten dann ergibt sich

$$n(\lambda) = \sum_{i \geq 1} \binom{\lambda'_i}{2}.$$

Nun kommen wir zu dem Begriff, der Hauptbestandteil unserer Beweise sein wird. Bezeichne *Par* die Menge aller unterschiedlichen Partitionen, so bezeichnen wir jede Funktion, deren Wertebereich in *Par* liegt, als *Partitionsfunktion*.

Somit haben wir alles, was wir über Partitionen etc. wissen müssen, um die gestellten Probleme erfolgreich zu bearbeiten.

1.2 Erzeugende Funktionen

Sei $f : \mathbb{N} \to \mathbb{C}$ eine arithmetische Funktion. Dann heißt die formale Potenzreihe

$$F(X) := \sum_{n \geq 0} f(n) X^n$$

die *erzeugende Funktion* von f. Weiter heißt

$$E(X) := \sum_{n \geq 0} f(n) \frac{X^n}{n!}$$

die *erzeugende Exponentialfunktion* von f.

Trotz ihres Namens handelt es sich bei *erzeugenden Funktionen* in erster Linie nur um formale Potenzreihen (über $\mathbb{C}$). Der Begriff umfasst sogar Objekte, die außerhalb von 0 nirgends im klassischen Sinn konvergieren. Die Namensgebung ist aber die traditionelle und Missverständnisse können dabei kaum entstehen, weshalb sie auch hier beibehalten wird.

Zur Erinnerung:
Als Menge definiert man den formalen Potenzreihenring $\mathbb{C}[[X]] := \{\sum_{n\geq 0} a_n X^n \mid a_n \in \mathbb{C}\}$. Darauf definiert man die beiden Verknüpfungen

$$\left(\sum_{n\geq 0} a_n X^n\right) + \left(\sum_{n\geq 0} b_n X^n\right) = \sum_{n\geq 0} (a_n + b_n) X^n$$

und

$$\left(\sum_{n\geq 0} a_n X^n\right) * \left(\sum_{n\geq 0} b_n X^n\right) = \sum_{n\geq 0} c_n X^n,$$

wobei $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

Somit wird $\mathbb{C}[[X]]$ offenbar zu einem kommutativen Integritätsring. Definieren wir zusätzlich eine Abbildung $v : \mathbb{C}[[X]] \to \mathbb{Z} \cup \{\infty\}$ durch

$$v(0) = \infty \text{ und } v\left(\sum_{n\geq 0} a_n X^n\right) = \text{ 'das kleinste } n \text{ mit } a_n \neq 0 \text{ ' },$$

so wird $\mathbb{C}[[X]]$ zu einem *diskreten Bewertungsring* mit Bewertung v. Insbesondere handelt es sich bei $\mathbb{C}[[X]]$ also um einen lokalen Hauptidealring, wobei (X) das maximale Ideal ist.

Um wirkliche Kombinatorik mit Hilfe erzeugender Funktionen zu betreiben, reicht uns die vorliegende Struktur noch nicht aus. Seien $G(X), F(X), F_1(X), \ldots$ formale Potenzreihen, so wollen wir auch Objekte der Bauart $F(G(X))$, $\sum_{n\geq 1} F_n(X)$ und $\prod_{n\geq 1} F_n(X)$ interpretieren können (falls sie Sinn machen), und um dieser Anforderung gerecht zu werden, versehen wir $\mathbb{C}[[X]]$ mit einer passenden Topologie.

Definition Sei R ein kommutativer Ring und $\mathfrak{m}$ ein Ideal von R. Dann definieren wir die $\mathfrak{m}$-*adische Topologie* als diejenige Topologie, deren Basis aus den Nebenklassen $f + \mathfrak{m}^k$ besteht, wobei $f \in R$ und $k \geq 0$.

Wir statten $\mathbb{C}[[X]]$ nun mit der (X)-adischen Topologie aus.

Eine Folge (f_n) aus $\mathbb{C}[[X]]$ heißt *Cauchy-Folge*, falls für jedes $k \geq 0$ ein N aus $\mathbb{N}$ existiert, sodass $f_n - f_m \in (X)^k$ für alle $n, m \geq N$. Analog sagen wir, eine Folge (f_n) aus $\mathbb{C}[[X]]$ *konvergiert* gegen f (geschrieben $\lim_{n\to\infty} f_n = f$), falls für jedes $k \geq 0$ ein $N \in \mathbb{N}$ existiert, sodass $f_n - f \in (X)^k$ für alle $n \geq N$. Eine Reihe $\sum_{n\geq 0} f_n$ in $\mathbb{C}[[X]]$ ist *konvergent*, falls die Folge der Teilsummen konvergiert. Analog definiert man Konvergenz für unendliche Produkte $\prod_{n\geq 0} f_n$. Hier können technische Probleme entstehen, die wir nicht besprechen wollen und deshalb verlangen wir einfach, dass alle Faktoren f_n die Bedingung $f_n(0) = 1$ erfüllen ($f_n(0)$ bezeichnet hier rein formal den konstanten Term der Potenzreihe und keine eventuelle Auswertung einer Funktion).

Um wirklich mit dem einhergehenden Konvergenzbegriff arbeiten zu können, müssen wir uns noch davon überzeugen, dass die (X)-adische Topologie hausdorffsch ist.

Proposition 1.1 *Sei R ein kommutativer Ring und $\mathfrak{m}$ ein Ideal von R. Dann ist die $\mathfrak{m}$-adische Topologie genau dann hausdorffsch, wenn $\cap_{k=0}^{\infty}\mathfrak{m}^k = (0)$.*

Beweis Sei die Topologie nicht hausdorffsch, d.h. $\exists f, g \in R$, $f \neq g$, die nicht trennbar sind. Dann haben wir insbesondere

$$\left(f + \mathfrak{m}^k\right) \cap \left(g + \mathfrak{m}^k\right) \neq \emptyset \ \forall k \geq 0.$$

Da zwei Nebenklassen aber entweder disjunkt oder gleich sind, gilt hier

$$f + \mathfrak{m}^k = g + \mathfrak{m}^k \ \forall k \geq 0.$$

Somit ist $0 \neq f - g \in \bigcap_{k\geq 0} \mathfrak{m}^k$.
Sei nun $\bigcap_{k\geq 0} \mathfrak{m}^k \neq (0)$. Wählen wir ein $0 \neq f \in \bigcap_{k\geq 0} \mathfrak{m}^k$, so sind 0 und f nicht trennbar.

□

Die Hausdorff-Eigenschaft für unseren Fall folgt nun direkt aus dem *Durchschnittssatz von Krull* oder Ad-hoc wie folgt:

Falls eine Potenzreihe $f = \sum a_n X^n$ in $\mathfrak{m}^k$ enthalten ist, so ist $a_n = 0$ für alle $n < k$. Also gilt $\bigcap_{k\geq 0} \mathfrak{m}^k = (0)$ und nach obiger Proposition somit die Aussage.

Als nächstes folgen ein paar sehr hilfreiche Konvergenzkriterien.

Proposition 1.2 *Seien $f_n \in \mathbb{C}[[X]]$. Dann konvergiert $\sum_{n\geq 0} f_n$ genau dann, wenn*

$$\lim_{n\to\infty} v(f_n) = \infty.$$

Beweis "⇒" Konvergiert die Reihe, so bilden die Teilsummen eine Cauchy-Folge, d.h. :

$$\forall k \in \mathbb{N}\ \exists N \in \mathbb{N} \ \text{ sodass } \ \left(\sum_{n=0}^{l} f_n - \sum_{n=0}^{m} f_n\right) = \sum_{n=m+1}^{l} f_n \in (X)^k \ \ \forall l, m \geq N.$$

Insbesondere gilt dies für $l = m + 1$ und wir erhalten $f_{m+1} \in (X)^k$ für alle $m \geq N$, oder anders ausgedrückt:

$$\forall k \in \mathbb{N}\ \exists N_1 \in \mathbb{N} \ \text{ sodass } \ v(f_m) \geq k \ \ \forall m \geq N_1.$$

"⇐" Da $\lim_{n\to\infty} v(f_n) = \infty$ gilt:

$$\forall\ N \in \mathbb{N}\ \ \exists \text{ nur endlich viele } f_k \text{ mit } v(f_k) \leq N. \qquad (\star)$$

Wir schreiben $f_k = \sum_{n\geq 0} a_n^{(k)} X^n$ und setzen $a_n = \sum_{k\geq 0} a_n^{(k)}$. Nach $(\star)$ ist a_n für alle n ein wohldefiniertes Element von $\mathbb{C}$. Nun setzen wir $f := \sum_{n\geq 0} a_n X^n$. Sei nun $k \in \mathbb{N}$. Dann wählen wir $N_1 \in \mathbb{N}$ so groß, dass alle f_j mit $v(f_j) \leq k$ in $\{f_1, \ldots, f_{N_1}\}$ enthalten sind. Damit hat man nach Definition der a_n:

$$\left(f - \sum_{n=0}^{N_1} f_n\right) \in (X)^k.$$

Also konvergiert die Reihe gegen f und die Behauptung ist bewiesen. □

Proposition 1.3 *Seien $f_n \in \mathbb{C}[[X]]$ mit $f_n(0) = 0$. Dann konvergiert $\prod_{n\geq 0}(1 + f_n)$ genau dann, wenn*

$$\lim_{n\to\infty} v(f_n) = \infty.$$

Beweis Ähnlich zum obigen Beweis. Für die Hinrichtung nutzen wir wieder die Cauchy-Bedingung für $l = m + 1, m \geq N$ und für die Rückrichtung konstruieren wir den Grenzwert des Produkts, indem wir die Koeffizienten so setzen wie man es für die Konvergenz bräuchte und folgern aus der Divergenz von $(v(f_n))_n$ die Wohldefiniertheit dieser Koeffizienten. □

Bemerkung: Diese beiden Propositionen zeigen gleichzeitig auch, dass Umordnungen den Grenzwert von Reihen und Produkten nicht ändern.
Seien $f_n \in \mathbb{C}[[X]]$ mit $\lim_{n\to\infty} v(f_n) = \infty$ (also konvergiert $\sum_{n\geq 0} f_n$) und $\sigma : \mathbb{N} \to \mathbb{N}$ eine Umordnung. Dann gilt auch $\lim_{n\to\infty} v(f_{\sigma(n)}) = \infty$, sodass nach Proposition 1.2 folgt, dass auch $\sum_{n\geq 0} f_{\sigma(n)}$ konvergiert. Man prüft leicht nach, dass beide Reihen den gleichen Grenzwert haben.

Seien $F(X) = \sum_{n\geq 0} a_n X^n$ und $G(X)$ formale Potenzreihen mit $G(0) = 0$. Dann definieren wir $F(G(X)) := \sum_{n\geq 0} a_n G(X)^n$. Da $v(G(X)^n) = n\, v(G(X))$, zeigt Proposition 1.2, dass $F(G(X))$ als formale Potenzreihe wohldefiniert ist.

Im Laufe der weiteren Arbeit wird im Einzelnen nicht nachgewiesen, dass alle verwendeten Objekte wohldefiniert sind, aber an allen solchen Stellen ist das mit Hilfe dieser Konvergenzkriterien direkt ersichtlich.

Definition Sei k ein Körper. Dann heißt die Abbildung

$$\mathrm{d} : k[[X]] \to k[[X]], \quad \sum_{n\geq 0} a_n X^n \mapsto \sum_{n\geq 0} (n+1) a_{n+1} X^n$$

der *formale Ableitungsoperator*.

Diese formale Ableitung erfüllt, wie zu erwarten, die typischen Ableitungsregeln

$$\begin{aligned}
&\mathrm{d}\,(F(X) + G(X)) = \mathrm{d}F(X) + \mathrm{d}G(X),\\
&\mathrm{d}\,(F(X)G(X)) = (\mathrm{d}F(X))G(X) + F(X)(\mathrm{d}G(X)),\\
&\mathrm{d}\,(F(G(X))) = (\mathrm{d}F)(G(X))\mathrm{d}G(X).
\end{aligned}$$

Zum vernünftigen Arbeiten mit den hier auftretenden erzeugenden Funktionen benötigen wir noch die

Proposition 1.4 (+Definition) *Es sei*

$$\log(1 + X) := \sum_{n\geq 1} (-1)^{n-1} \frac{X^n}{n}$$

der formale Logarithmus. Seien nun $F_j(X) = \sum_{n\geq 0} a_n^{(j)} X^n \in \mathbb{C}[[X]]$ *(*$j \in \mathbb{N}$*) mit* $F_j(0) = 1$ *und so, dass* $\prod_j F_j(X)$ *gegen ein* $F(X) = \sum_{n\geq 0} a_n X^n \in \mathbb{C}[[X]]$ *konvergiert. Dann gilt*

$$\log\left(\prod_{j\geq 0} F_j(X)\right) = \sum_{j\geq 0} \log\left(F_j(X)\right).$$

Beweis Sieht man sich die formale Potenzreihe zu $\mathrm{d}(\log(1+X))$ einmal an, so sieht man sofort, dass

$$\mathrm{d}(\log(1+X)) = \frac{1}{1+X}.$$

Sind $F_1(X), F_2(X) \in \mathbb{C}[[X]]$, so haben wir also

$$\begin{aligned}\mathrm{d}(\log(F_1(X)F_2(X)) &= \frac{1}{F_1(X)F_2(X)}((\mathrm{d}F_1(X))F_2(X) + F_1(X)(\mathrm{d}F_2(X)))\\ &= \mathrm{d}(\log(F_1(X)) + \mathrm{d}(\log(F_2(X)).\end{aligned}$$

Nach Koeffizientenvergleich folgt somit

$$\log(F_1(X)F_2(X)) = \log(F_1(X)) + \log(F_2(X)).$$

Mit Induktion ergibt sich das Ergebnis für beliebige endliche Produkte.

Sei nun $(F_j(X) = \sum_{j\geq 0} a_n^{(j)} X^n)_j$ eine Folge formaler Potenzreihen mit $a_0^{(j)} = 1$, die gegen ein $F(X) = \sum_{n\geq 0} a_n X^n$ (notwendigerweise gilt auch $a_0 = 1$) konvergiert. Wir zeigen, dass

$$\log(\lim_{j\to\infty} F_j) = \lim_{j\to\infty} \log(F_j).$$

Wir wählen ein F_m mit $F - F_m \in (X)^k$. Dann gilt auch $\log(F) - \log(F_m) \in (X)^k$, denn:

$$\begin{aligned}\log(F(X)) &= \log(1 + \sum_{n\geq 1} a_n X^n)\\ &= \sum_{m\geq 1} \frac{(-1)^{m-1}}{m} \left(\sum_{n\geq 1} a_n X^n\right)^m\\ &= \sum_{m\geq 1} \frac{(-1)^{m-1}}{m} \left(\sum_{n\geq m} \left(\sum_{\substack{j\in\mathbb{N}_{\geq 1}^m\\ |j|=n}} a_{j_1} a_{j_2} \cdots a_{j_m}\right) X^n\right)\\ &= \sum_{N\geq 1} \left(a_N + \sum_{m=2}^{N} \frac{(-1)^{m-1}}{m} \sum_{\substack{j\in\mathbb{N}_{\geq 1}^m\\ |j|=N}} a_{j_1} \cdots a_{j_m}\right) X^N.\end{aligned}$$

Dabei setzen wir $\mathbb{N}_{\geq 1}^m = \{j \in \mathbb{N}^m \mid j_i \geq 1 \text{ für alle i}\}$. Nun bedeutet $F - F_m \in (X)^k$ einfach, dass $a_i = a_i^{(m)}$ für alle $i \leq k$. Da der Koeffizient von X^k in $\log F(X)$ nur die a_i mit $i \leq k$ enthält, gilt insbesondere $\log(F) - \log(F_m) \in (X)^k$.

Setzen wir die Ergebnisse zusammen erhalten wir

$$\begin{aligned}\log\left(\prod_{j\geq 0} F_j(X)\right) &= \log\left(\lim_{n\to\infty}\prod_{j=1}^{n} F_j\right)\\ &= \lim_{n\to\infty}\log\left(\prod_{j=1}^{n} F_j\right)\\ &= \lim_{n\to\infty}\sum_{j=1}^{n}\log(F_j)\\ &= \sum_{j\geq 0}\log(F_j).\end{aligned}$$

□

Proposition 1.5 *Die Abbildung* $\log : \{F \in \mathbb{C}[[X]] \mid F(0) = 1\} \to \mathbb{C}[[X]]$ *ist injektiv.*

Beweis Wir schreiben $F(X) = \sum_{n\geq 0} a_n X^n$ und $\log F(X) = \sum_{n\geq 0} b_n X^n$. Aus dem Beweis von Proposition 1.4 wissen wir, dass:

$$b_n = a_n + \sum_{m=2}^{n}\frac{(-1)^{m-1}}{m}\sum_{\substack{j\in\mathbb{N}_{\geq 1}^m\\ |j|=n}}\underbrace{a_{j_1}\cdots a_{j_m}}_{(\star)}.$$

Seien nun $G(X) = \sum_{n\geq 0} a'_n X^n$ und $\log G(X) = \sum_{n\geq 0} b'_n X^n \in \mathbb{C}[[X]]$ mit $\log F(X) = \log G(X)$. Die Produkte $(\star)$ für b_n bzw. b'_n enthalten nur a_k bzw a'_k für $k < n$. Die Gleichheit von b_1 und b'_1 liefert die Gleichheit von a_1 und a_1. Damit liefert die Gleichheit von b_2 und b'_2 die Gleichheit von a_2 und a'_2 usw. □

Bemerkung In allen Fällen wo die Ausdrücke Sinn machen, gelten die üblichen Logarithmengesetze.

Jetzt haben wir soweit alle Werkzeuge, die wir benötigen und der nächste Schritt ist nun, mit Hilfe dieser Werkzeuge die Konjugationsklassen abzuzählen.

2 Anzahl der Konjugationsklassen

2.1 Die richtige Parametrisierung

Um die Anzahl der Konjugationsklassen zu bestimmen, müssen wir die Fragestellung vorher ausreichend 'algebraisieren'.

Wenn nichts anderes gesagt wird, bezeichnet k ab jetzt einen endlichen Körper $\mathbb{F}_q$, wobei q eine Primzahlpotenz ist.

Es bezeichnen $End_n(k) := \{g : k^n \to k^n \mid g \text{ ist k-linear}\}$ den Endomorphismenring von k^n und $Mat_n(k)$ den Ring aller $n \times n$-Matrizen mit Einträgen aus k. Legen wir eine Basis für k^n fest, so gilt $End_n(k) \cong Mat_n(k)$. Im Fokus dieser Arbeit liegt nun aber die Einheitengruppe $GL_n(k)$ von $Mat_n(k)$. Man sieht leicht, dass für die Mächtigkeit dieser Gruppe

$$\gamma(n) := |GL_n(k)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

gilt. Bevor wir uns nun aber speziell der $GL_n(k)$ zuwenden, formulieren wir alle nötigen (und immer wiederkehrenden) Sätze für $Mat_n(k)$.

Sei $A \in Mat_n(k)$. Setzen wir $X.v := Av$, so erhalten wir eine $k[X]$-Modulstuktur auf k^n. Diesen Modul bezeichnen wir fortan mit V_A. Als endlich-dimensionaler k-Vektorraum ist k^n, ausgestattet mit der angesprochenen Modulstruktur, offensichtlich ein endlich erzeugter $k[X]$-Modul. Da $k[X]$ zudem ein Hauptidealring ist, handelt es sich bei den zu untersuchenden Objekten um endlich erzeugte Moduln über Hauptidealringen; einer Klasse von Objekten die sehr gut verstanden ist.

Sei R nun ein allgemeiner Hauptidealring, E ein R-Modul und $p \in R$ ein Primelement. Dann definieren wir $E(p) := \{x \in E \mid p^r x = 0 \text{ für ein } r \geq 1\}$. Man sieht direkt, dass es sich bei $E(p)$ um einen Untermodul handelt. Man beachte, dass für zwei assoziierte Primelemente $p, q \in R$ (d.h. $p = uq$, wobei $u \in R^*$) $E(p) = E(q)$ gilt. Sei p ein Primelement, so bezeichnen wir mit $\bar{p}$ einen Repräsentanten aus $\{q \in R \mid q = up,\ u \in R^*\}$.

Nun sind wir in der Lage den Struktursatz zu formulieren, der die Grundlage unserer Abzählung bildet.

Satz 2.1 *Sei E ein nichttrivialer, endlich erzeugter Torsionsmodul über einem Hauptidealring R. Dann ist E die direkte Summe*

$$E = \bigoplus_{\bar{p}} E(\bar{p}),$$

über ein Repräsentantensystem $\bar{p} \in R$ von Primelementen, sodass $E(\bar{p}) \neq 0$. Zudem kann jedes $E(p)$ selbst geschrieben werden als direkte Summe

$$E(p) \cong R/(p^{\nu_1}) \oplus R/(p^{\nu_2}) \oplus \cdots \oplus R/(p^{\nu_s}),$$

mit $1 \leq \nu_1 \leq \nu_2 \leq \cdots \leq \nu_s$. Die Sequenz $(\nu_1, \nu_2, \ldots, \nu_s)$ ist dabei eindeutig bestimmt.

Bezeichnet $m_A(X)$ das zu $A \in Mat_n(k)$ gehörige Minimalpolynom, so gilt für alle $v \in V_A$, dass $m_A(X).v = 0$, also handelt es sich hier, wie im Satz verlangt, um einen Torsionsmodul. (Nach dem Satz von Caley-Hamilton könnte man dieselbe Erklärung auch mit dem charakteristischen Polynom zu A bringen.)

Somit erhalten wir

Korollar 2.2 *Sei $A \in Mat_n(k)$ und $\mathcal{I}$ die Menge aller normierten, irreduziblen Polynome über k. Dann ist V_A darstellbar als die direkte Summe*

$$V_A \cong \bigoplus_{i, f \in \mathcal{I}} k[X]/(f)^{\lambda(f)_i},$$

mit einer Partitionsfunktion $\lambda : \mathcal{I} \to Par$, sodass:

$$\sum_{f \in \mathcal{I}} |\lambda(f)| deg(f) = n.$$

Nun sei $\mathcal{I}^\star := \mathcal{I} \setminus \{x\}$. Die Anzahl der Konjugationsklassen von $GL_n(k)$ entspricht der Anzahl der partitionswertigen Funktionen $\lambda : \mathcal{I}^\star \to Par$ mit

$$\sum_{f \in \mathcal{I}^\star} |\lambda(f)| deg(f) = n.$$

Beweis. Mit der Einschränkung auf die normierten, irreduziblen Polynome haben wir automatisch ein Repräsentantensystem der Primelemente von $k[X]$, sodass der erste Teil der Aussage einfach nur eine Umformulierung des Satzes ist.

Zum zweiten Teil: Es ist klar, dass

$$V_A \cong V_C \Leftrightarrow A = SCS^{-1} \text{ für ein } S \in GL_n(k) \quad (\star)$$

(man erinnere sich daran, dass die Zerlegung von V_A mit einer Normalform für A einhergeht). Sei c eine Konjugationsklasse von $GL_n(k)$ und $A \in c$, so schreiben wir $V_c := V_A$. Diese Definition ist wegen $(\star)$ gerechtfertigt; jedes andere $A' \in c$ erzeugt einen isomorphen Modul mit der gleichen Zerlegung.

Sei $V_A(X) := \{v \in V_A \mid X^r.v = 0 \text{ für ein } r \geq 1\} \neq 0$, also insbesondere $\lambda(X) \neq (0, 0, \ldots)$, und bezeichne χ_A das charakteristische Polynom von $A \in Mat_n(k)$. Aus der Zerlegung von V_A folgt:

$$\chi_A = \prod_{i, f \in \mathcal{I}} f^{\lambda(f)_i}.$$

Für $V_A(X) \neq 0$ kommt im obigen Produkt eine Potenz von X vor. Somit gilt $\det(A) = \chi_A(0) = 0$, d.h. A ist nicht invertierbar. Somit gewährleistet uns die Reduktion von $\mathcal{I}$ auf $\mathcal{I}^\star$ die Invertierbarkeit aller Matrizen A, deren Zerlegung von V_A durch eine partitionswertige Funktion $\lambda : \mathcal{I}^\star \to Par$ parametrisiert wird. Nun erhalten wir wohldefinierte, zueinander inverse Abbildungen

$$\begin{array}{rcl} \{\text{ Konjugationsklassen in } GL_n(k)\} & \to & \{\Phi : \mathcal{I}^\star \to \text{ Par} \mid \sum_{f \in \mathcal{I}^\star} |\Phi(f)| \deg(f) = n\} \\ c & \mapsto & \text{Partitionsfunktion zu } V_c \\ \text{Klasse von } A = \oplus_{i,f} B_{f^{\Phi(f)_i}} & \leftarrow & \Phi. \end{array}$$

Dabei bezeichnet B_g für ein Polynom $g = X^n + a_{n-1}X^{n-1} + \dots a_0$ die Begleitmatrix

$$\begin{pmatrix} 0 & 0 & \dots & & -a_0 \\ 1 & 0 & & & \\ 0 & 1 & & & \vdots \\ \vdots & & \ddots & & \\ 0 & & & 1 & -a_{n-1} \end{pmatrix}$$

und wir schreiben $E \oplus F := \begin{pmatrix} E & 0 \\ 0 & F \end{pmatrix}$ mit geeigneten Nullblöcken. □

Mit wenigen Aussagen über die Theorie endlich erzeugter Moduln konnten wir das ursprüngliche Problem nun erheblich reduzieren. Als nächstes werden wir die angegebenen Partitionsfunktionen mit Hilfe erzeugender Funktionen abzählen.

2.2 Abzählung der Klassen

Wir ändern die Notation aus 2.1 ein wenig, indem wir nun mit $\mathcal{I}(q)$ die Menge aller normierten, irreduziblen Polynome über $\mathbb{F}_q$ außer X bezeichnen. Dabei lassen wir den Parameter q weg, falls klar ist über welchem endlichen Körper wir gerade arbeiten.

Ein erster wichtiger Zwischenschritt bei unserer Abzählung bildet:

Satz 2.3 *Sei $c_n(q)$ die Anzahl der Konjugationsklassen der $GL_n(q)$ oder äquivalent dazu, die Anzahl der, in Korollar 2.2 beschriebenen, Partitionsfunktionen. Dann gilt:*

$$\sum_{n \geq 0} c_n(q) X^n = \prod_{j \geq 0} \frac{1 - X^j}{1 - qX^j}.$$

Diese Identität ist z.B in [Sta02] oder [Mac81] zu finden. Dabei modifizieren wir den Beweis aus [Sta02] dahingehend, dass wir die Formel tatsächlich herleiten und nicht nur überprüfen.

Zuvor benötigen wir aber noch die folgenden Aussagen:

Proposition 2.4 *Sei $p(n)$ die Zahl der Partitionen der natürlichen Zahl n. Dann gilt*

$$\sum_{n\geq 0} p(n)X^n = \prod_{i\geq 1} \frac{1}{1-X^i}.$$

Proposition 2.5 *Sei $\beta(n,q)$ die Anzahl der normierten, irreduziblen Polynome vom Grad n über $\mathbb{F}_q$ mit $f(0)\neq 0$. So erhalten wir*

$$\beta(n,q) = \begin{cases} q-1, & n=1 \\ \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}, & n\geq 2. \end{cases}$$

Da beide Aussagen zum Standardrepertoire gehören, wird hier auf einen Beweis verzichtet. Für das erste Ergebnis siehe man z.B. [Sta02, S.68].

Beweis zu Satz 2.3 Es gilt

$$\begin{aligned}
\sum_{n\geq 0} c_n(q)X^n &= \sum_{\Phi:\mathcal{I}\to Par} X^{\sum_{f\in\mathcal{I}}|\Phi(f)|deg(f)} \\
&= \prod_{f\in\mathcal{I}}\left(\sum_{\lambda\in Par} X^{|\lambda|deg(f)}\right) \\
&\overset{2.4}{=} \prod_{f\in\mathcal{I}}\prod_{j\geq 1}\left(1-X^{j\,deg(f)}\right)^{-1} \\
&= \prod_{n\geq 1}\prod_{j\geq 1}\left(1-X^{jn}\right)^{-\beta(n,q)}.
\end{aligned}$$

Mit Proposition 1.4 und der Formel für $\beta(n,q)$ erhalten wir

$$\begin{aligned}
\log\sum_{n\geq 0} c_n(q)X^n &= \sum_{n\geq 1}\sum_{j\geq 1} -\beta(n,q)\log(1-X^{jn}) \\
&= \sum_{n\geq 1}\sum_{j\geq 1}\beta(n,q)\sum_{i\geq 1}\frac{X^{ijn}}{i} \\
&= \sum_{j\geq 1}(q-1)\sum_{i\geq 1}\frac{X^{ij}}{i} + \sum_{n\geq 2}\sum_{j\geq 1}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d\sum_{i\geq 1}\frac{X^{ijn}}{i} \\
&= \sum_{j\geq 1}(-1)\sum_{i\geq 1}\frac{X^{ij}}{i} + \sum_{j\geq 1}q\sum_{i\geq 1}\frac{X^{ij}}{i} + \sum_{n\geq 2}\sum_{j\geq 1}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d\sum_{i\geq 1}\frac{X^{ijn}}{i} \\
&= \sum_{j\geq 1}(-1)\sum_{i\geq 1}\frac{X^{ij}}{i} + \sum_{n\geq 1}\sum_{j\geq 1}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d\sum_{i\geq 1}\frac{X^{ijn}}{i}.
\end{aligned}$$

Wir bezeichnen den Koeffizienten von q^dX^N mit $a(d,N)$. Dann gilt:

$$a(0,N) = \sum_{d|N}\frac{-1}{d}.$$

Für $d \nmid N$ gilt $a(d,N) = 0$ und für $d \mid N$ gilt

$$\begin{aligned} a(d,N) &= \sum_{i \mid N} \frac{1}{i} \sum_{n: d \mid n \mid \frac{N}{i}} \frac{1}{n} \mu(n/d) \\ &= \sum_{d \mid \frac{N}{d}} \frac{1}{i} \sum_{m \mid \frac{N}{id}} \frac{1}{dm} \mu(m). \end{aligned}$$

Ist ϕ die Eulersche Phi-Funktion, so ergibt sich mit Hilfe von

$$\sum_{k \mid r} \frac{\mu(k)}{k} = \frac{\phi(r)}{r}, \tag{2.1}$$

$$\sum_{k \mid r} \phi(r/k) = \sum_{k \mid r} \phi(k) = r, \tag{2.2}$$

$$\begin{aligned} a(d,N) &= \frac{1}{d} \sum_{d \mid \frac{N}{d}} \frac{\phi(N/id)}{N/d} \\ &= \frac{1}{d} \frac{N/d}{N/d} \\ &= \frac{1}{d}. \end{aligned}$$

Somit haben wir nun

$$\begin{aligned} \log \sum_{n \geq 0} c_n(q) X^n &= \sum_{n \geq 1} \left(-\left(\sum_{d \mid n} \frac{1}{d} \right) + \sum_{d \mid n} \frac{1}{d} q^d \right) X^n \\ &= \underbrace{\sum_{n \geq 1} \left(-\sum_{d \mid n} \frac{1}{d} \right) X^n}_{(1)} + \underbrace{\sum_{n \geq 1} \left(\sum_{d \mid n} \frac{1}{d} q^d \right) X^n}_{(2)}. \end{aligned}$$

Man erinnere sich, dass $\log(1 + X) := \sum_{n \geq 1} (-1)^{n-1} \frac{X^n}{n}$. Durch Umformung erhalten wir für (1) und (2):

$$\begin{aligned} (1) &= \sum_{n \geq 1} \sum_{k \geq 1} -\frac{1}{k} X^{kn} \\ &= \sum_{n \geq 1} \log(1 - X^n). \end{aligned}$$

$$\begin{aligned} (2) &= \sum_{n \geq 1} \sum_{k \geq 1} \frac{1}{k} q^k X^{kn} \\ &= \sum_{n \geq 1} - \log(1 - qX^n). \end{aligned}$$

Es ergibt sich insgesamt:

$$\begin{aligned}\log \sum_{n\geq 1} c_n(q)X^n &= \sum_{n\geq 1} \log(1-X^n) + \sum_{n\geq 1} -\log(1-qX^n)\\ &= \sum_{n\geq 1} \log\left(\frac{1-X^n}{1-qX^n}\right)\\ &= \log\left(\prod_{n\geq 1} \frac{1-X^n}{1-qX^n}\right).\end{aligned}$$

Da log injektiv ist, folgt damit die Behauptung. □

Um die gewünschte Formel für $c_n(q)$ zu erhalten, untersuchen wir nun den Koeffizienten von X^n des Produkts

$$\prod_{j\geq 1} \frac{1-X^j}{1-qX^j} = \left(\prod_{j\geq 1}(1-X^j)\right)\left(\prod_{j\geq 1}(1-qX^j)^{-1}\right). \qquad (\star)$$

Diese Identität folgt, weil alle auftretenden unendlichen Produkte konvergieren (wovon man sich gerne mit den bereitgestellten Kriterien überzeugt) und im bewerteten Ring $(\mathbb{C}[[X]], v)$ die übliche Relation $\lim_{n\to\infty} a_n b_n = (\lim_{n\to\infty} a_n)(\lim_{n\to\infty} b_n)$ gilt.

Da die beiden unendlichen Produkte auf der rechten Seite von $(\star)$ konvergieren, erhalten wir für beide eine Darstellung als formale Potenzreihe. Obwohl der erste Faktor eine sehr bekannte Potenzreihendarstellung besitzt (siehe Pentagonalzahlensatz), benötigen wir nur die konkrete Darstellung des zweiten Faktors und für diesen gilt [Sta02, S.72]:

$$\begin{aligned}\prod_{j\geq 1}(1-qX^j)^{-1} &= \sum_{k\geq 0} \frac{X^k q^k}{(1-X)(1-X^2)\cdots(1-X^k)}\\ &= \sum_{k\geq 0} X^k q^k \prod_{j=1}^{k} \underbrace{\left(\sum_{l\geq 0} X^{lj}\right)}_{=:F_j(X)}.\end{aligned}$$

Schreiben wir nun $F_j(X) = \sum_{n\geq 0} a_n^{(j)} X^n$, so ergibt sich $a_0^{(j)} = 1$ und für $n \geq 1$

$$a_n^{(j)} = \begin{cases} 0, & \text{falls } j \nmid n\\ 1, & \text{falls } j \mid n.\end{cases}$$

Nach der Definition des Produktes in $\mathbb{C}[[X]]$ gilt

$$\prod_{j=1}^{k}\left(\sum_{n\geq 0} a_n^{(j)} X^n\right) = \sum_{N=0}^{\infty} \underbrace{\left(\sum_{l_1+\cdots+l_k=N} a_{l_1}^{(1)}\cdots a_{l_k}^{(k)}\right)}_{=:c_N} X^N.$$

Man sieht außerdem, dass

$$a_{l_1}^{(1)} \cdots a_{l_k}^{(k)} = \begin{cases} 1, & \text{falls } 1 \mid l_1, 2 \mid l_2, \ldots, k \mid l_k \\ 0, & \text{sonst.} \end{cases}$$

Damit ist der Koeffizient c_N die Anzahl der nichtnegativen, ganzzahligen Lösungen von $N = m_1 + 2m_2 + \cdots + km_k$. Schreiben wir $p_{\leq k}(N)$ für die Anzahl der Partitionen von N mit größtem Summanden $\leq k$, so bedeutet das einfach $c_N = p_{\leq k}(N)$. Genau wie für die Anzahl aller Partitionen, setzen wir auch hier $p_{\leq k}(0) := 1$ und $p_{\leq 0}(N) := 1$ für alle N. Insgesamt haben wir nun

$$\begin{aligned} \prod_{j\geq 1}(1-qX^j)^{-1} &= \sum_{k\geq 0} X^k q^k \sum_{N\geq 0} p_{\leq k}(N) X^N \\ &= \sum_{m\geq 0}\left(\sum_{l=0}^{m} q^l p_{\leq l}(m-l)\right) X^m. \end{aligned}$$

Wie oben schon erwähnt, konvergiert auch $F(X) := \prod_{j\geq 1}(1-X^j)$ in $\mathbb{C}[[X]]$ und wir schreiben $F(X) = \sum_{n=0}^{\infty} a_n X^n$. Wir erhalten

$$\begin{aligned} \prod_{j\geq 1}\frac{1-X^j}{1-qX^j} &= \left(\sum_{m=0}^{\infty}\left(\sum_{k=0}^{m} q^k p_{\leq k}(m-k)\right)X^m\right)\left(\sum_{m=0}^{\infty} a_m X^m\right) \\ &= \sum_{N=0}^{\infty}\left(\sum_{i=0}^{N}\left(\sum_{k=0}^{i} q^k p_{\leq k}(i-k)\right)a_{N-i}\right)X^N. \end{aligned}$$

Als erstes kleines Zwischenergebnis können wir festhalten, dass

$$c_N(q) = \sum_{i=0}^{N}\left(\sum_{k=0}^{i} q^k p_{\leq k}(i-k)\right)a_{N-i}$$

also ein Polynom in q ist. Der nächste Schritt ist die Bestimmung der, noch sehr kompliziert erscheinenden, Koeffizienten diese Polynoms. Wir schreiben die obige Summe um und untersuchen

$$\sum_{i=0}^{N}\left(\sum_{k=0}^{i} q^k p_{\leq k}(i-k)\right)a_{N-i} = \sum_{m=0}^{N}\left(\sum_{l=0}^{m} p_{\leq m}(l) a_{N-m-l}\right)q^m.$$

Der Koeffizient von q^m entspricht genau dem Koeffizienten von X^{N-m} in

$$\left(\prod_{j=1}^{m}\frac{1}{1-X^j}\right)\left(\prod_{j=1}^{\infty}(1-X^j)\right) = \left(\sum_{n=0}^{\infty} p_{\leq m}(n)X^n\right)\left(\sum_{n=0}^{\infty} a_n X^n\right).$$

Mit der Identität aus Proposition 2.4 erhalten wir

$$\begin{aligned} &\left(\prod_{j\geq 1}(1-X^j)\right)\left(\sum_{n=0}^{\infty} p(n)X^n\right) = 1 \qquad\qquad \Big| * \prod_{j=1}^{m}\frac{1}{1-X^j}, \\ \Rightarrow &\left(\prod_{j=m+1}^{\infty}(1-X^j)\right)\left(\sum_{n\geq 0} p(n)X^n\right) = \sum_{n\geq 0} p_{\leq m}(n)X^n. \qquad (\star) \end{aligned}$$

Der erste Faktor der linken Seite konvergiert und wir setzen $G^{(m)}(X) := \sum_{n\geq 0} b_n^{(m)} X^n := \prod_{j=m+1}^{\infty}(1 - X^j)$. Wir sind nun an den Koeffizienten von $G^{(m)}(X)$ interessiert und mit ($\star$) ergibt sich

$$\sum_{i=0}^{n} b_i^{(m)} p(n-i) = p_{\leq m}(n).$$

Aus dieser Gleichung werden wir die $b_i^{(m)}$ bestimmen können. Da $p(N) = p_{\leq m}(N)$ für alle $N \leq m$, haben wir

$$\begin{aligned}
&n = 0 : b_0^{(m)} p(0) = p(0) && \Rightarrow b_0^{(m)} = 1 \\
&n = 1 : b_0^{(m)} p(1) + b_1 p(0) = p(1) && \Rightarrow b_1^{(m)} = 0 \\
&n = 2 : b_0^{(m)} p(2) + b_2 p(0) = p(2) && \Rightarrow b_2^{(m)} = 0 \\
&\ \vdots && \\
&n = m : b_0^{(m)} p(m) + b_m p(0) = p(m) && \Rightarrow b_m^{(m)} = 0;
\end{aligned}$$

und da außerdem $p(N) = p_{\leq m}(N) + \sum_{i=1}^{N-m} p(N-m-i)$, für $m+1 \leq N \leq 2m$, haben wir

$$\begin{aligned}
&n = m+1 : b_0^{(m)} p(m+1) + b_{m+1}^{(m)} p(0) = p_{\leq m}(m+1) && \Rightarrow b_{m+1}^{(m)} = -1 \\
&n = m+2 : b_0^{(m)} p(m+2) - p(1) + b_{m+2}^{(m)} p(0) = p_{\leq m}(m+2) && \Rightarrow b_{m+2}^{(m)} = -1 \\
&\ \vdots && \\
&n = 2m : b_0^{(m)} p(2m) - p(m+1) - p(m) - \cdots + b_{2m}^{(m)} p(0) = p_{\leq m}(2m) && \Rightarrow b_{2m}^{(m)} = -1.
\end{aligned}$$

Wir erinnern uns daran, dass der Koeffizient von q^{N-i} im Polynom $c_N(q)$ dem Koeffizienten $b_i^{(N-i)}$ entspricht. Nach obiger Berechnung der $b_i^{(m)}$ erkennt man, dass $b_i^{(N-i)} = 0$, falls $i \leq N-i$. Wir haben zudem $b_i^{(N-i)} = -1$, falls

$$\begin{aligned}
& N - i + 1 \leq i \leq 2(N-i) \\
\Leftrightarrow \quad & \lfloor \frac{1}{2}(N+1) \rfloor \leq i \leq \lfloor \frac{2}{3} N \rfloor.
\end{aligned}$$

Somit haben wir nun endlich eine vernünftige Form für $c_n(q)$.

Satz 2.6 *Sei $c_n(q)$ die Anzahl der Konjugationsklassen von $GL_n(\mathbb{F}_q)$. Dann gilt:*

$$c_n(q) = q^n - q^{\lfloor \frac{1}{2}(n-1) \rfloor} - q^{\lfloor \frac{1}{2}(n-1) \rfloor - 1} - \cdots - q^{\lfloor \frac{1}{3} n \rfloor} + O(q^{\lfloor \frac{1}{3} n \rfloor - 1}).$$

Für kleine n lässt sich $c_n(q)$ mit obiger Vorgehensweise auch explizit bestimmen. So ergibt sich nach kurzer Rechnung:

$$\begin{aligned}
c_1(q) &= q - 1,\\
c_2(q) &= q^2 - 1,\\
c_3(q) &= q^3 - q,\\
c_4(q) &= q^4 - q,\\
c_5(q) &= q^5 - q^2 - q + 1,\\
c_6(q) &= q^6 - q^2.
\end{aligned}$$

Am Ende der Arbeit befindet sich eine kleine Tabelle mit exakten Werten zu diesen $c_n(q)$ $(2 \leq n \leq 6)$ für kleine q.

Bemerkung Gleichzeitig haben wir somit auch die Anzahl der irreduziblen Darstellungen von $GL_n(K)$ bestimmt. Bemerkenswerter hierbei ist, dass diese Darstellungen -genau wie die Konjugationsklassen- auf natürliche Weise durch Partitionsfunktionen parametrisiert werden, die den hier vorgestellten Partitionsfunktionen ähneln (siehe dazu z.B [Mac98, Kap. IV.5]).

3 Größe der Konjugationsklassen

Die Frage, die sich ganz natürlich an das vorangehende Kapitel angliedert, ist die Frage nach der Größe der einzelnen Konjugationsklassen. Ist c_A die Konjugationsklasse von $A \in GL_n(k)$ so gilt

$$|c_A| = \frac{\gamma(n)}{|Z(A)|}.$$

Dies erlaubt uns das Problem auf die Bestimmung der Zentralisatoren zu verlagern; Objekten, die viel leichter zu handhaben sind. Obwohl die Frage nach einer expliziten Formel dieser Größen für sich schon interessant ist, so brauchen wir sie hier zur Bestimmung der angestrebten Asymptotiken.

Sei $A \in Mat_n(k)$. Aus der Definition der $k[X]$-Modulstruktur auf V_A folgt sofort

$$End_{k[X]} V_A = Z(A).$$

Dabei bezeichnet $Z(A) := \{B \in Mat_n(k) \mid BA = AB\}$ den Zentralisator von A (in $Mat_n(k)$). Wir definieren $V_{A,f} := \{v \in V_A | f^k v = 0 \text{ für ein k } \in \mathbb{N}\}$. Das A im Index wird im folgenden weggelassen, weil aus der Situation immer klar sein wird mit welcher Modulstruktur wir arbeiten. Mit $\mathcal{I}$ bezeichnen wir, wie im Kapitel zuvor, die Menge der normierten, irreduziblen Polynome mit $f(0) \neq 0$. In dieser Notation lässt sich die Zerlegung aus Korollar 2.2 nun wie folgt umschreiben:

$$V_A = \bigoplus_{f \in \mathcal{I} \cup \{X\}} V_f, \quad \text{mit} \quad V_f = \bigoplus_{i \in \mathbb{N}} k[X]/(f)^{(\mu(f))_i},$$

wobei μ die, zu A gehörige, Partitionsfunktion ist. Diese Zerlegung hilft uns dabei das bestehende Problem stark zu reduzieren.

Proposition 3.1 *Sei $A \in GL_n(k)$. Dann gilt*

$$End_{k[X]} V_A = \bigoplus_{f \in \mathcal{I}} End_{k[X]} V_f.$$

Insbesondere gilt also

$$Z(A)^\star = \bigoplus_{f \in \mathcal{I}} Aut_{k[X]} V_f,$$

wobei $Z(A)^\star$ die Einheitengruppe des Ringes $Z(A)$ bezeichnet.

Beweis *Sei $\phi \in End_{k[X]}V_A$. Dann gilt $\phi(f^k v) = f^k\phi(v)$, sodass $\phi(V_f) \subset V_f$. Betrachtet man nun die Abbildung*

$$End_{k[X]}V_A \to \bigoplus_{f\in\mathcal{I}} End_{k[X]}V_f, \qquad \phi \mapsto (\phi|_{V_f})_{f\in\mathcal{I}},$$

und mit $V_A = \oplus_{f\in\mathcal{I}}V_f$ auch

$$\bigoplus_{f\in\mathcal{I}} End_{k[X]}V_f \to End_{k[X]}\left(\bigoplus_{f\in\mathcal{I}} V_f\right), \quad (\phi_f)_{f\in\mathcal{I}} \mapsto \Big(\phi : V_A \to V_A,\ v = (v_f)_{f\in\mathcal{I}} \mapsto (\phi_f(v_f))_{f\in\mathcal{I}}\Big),$$

so sieht man, dass es sich um zwei zueinander inverse Isomorphismen handelt. Der Zusatz ergibt sich nun, wenn wir auf beiden Seiten die Einheiten betrachten. □

Proposition 3.1 zeigt, dass wir uns auf die Untersuchung der Automorphismengruppen $Aut_{k[X]}V_f$ für $f \in \mathcal{I}$ beschränken können. Da $V_f \cong k[X]/(f)^{\lambda_1} \oplus \cdots \oplus k[X]/(f)^{\lambda_r}$ für eine Partition $\lambda = (\lambda_1, \ldots, \lambda_r)$, gilt es also

$$Aut_{k[X]}\Big(k[X]/(f)^{\lambda_1} \oplus \cdots \oplus k[X]/(f)^{\lambda_r}\Big)$$

abzuzählen.

Sei $f \in \mathcal{I}$ fest aber beliebig. Wir schreiben $V := V_f$. Da $Aut_{k[X]}V \subset Aut_k V$, werden wir die $k[X]$-Automorphismen einfach als besondere k-Automorphismen betrachten und eben diese abzählen. Wir wählen eine Basis $\mathcal{B}$ von V und zählen alle Basen auf die wir $\mathcal{B}$ durch einen $k[X]$-Automorphismus abbilden können. Wir notieren die Partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ mit $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$ nun als $\lambda = (\mu_1, \ldots, \mu_1, \mu_2, \ldots \mu_s)$ mit $\mu_1 > \mu_2 > \cdots > \mu_s$, aber behalten die Schreibweise für die konjugierte Partition bei; also $\lambda' = (\lambda'_1, \ldots, \lambda'_k)$ mit $\lambda'_1 \geq \lambda'_2 \geq \cdots \geq \lambda'_k$. Im Folgenden bezeichne $m_i := m_i(\lambda)$, wie in 1.1, die Anzahl mit der i in der Partition λ vorkommt.

Unsere Basis $\mathcal{B}$ sei nun die folgende:

$$\begin{array}{rl}
1 & (\bar{1}, 0, \ldots, 0), (\bar{X}, 0, \ldots, 0), \ldots, (\bar{X}^{d-1}, 0, \ldots, 0), (\bar{f}\bar{1}, 0, \ldots, 0), \ldots, \\
 & (\bar{f}\bar{X}^{d-1}, 0, \ldots, 0), (\bar{f}^2\bar{1}, 0, \ldots, 0), \ldots, (\bar{f}^{\mu_1-1}\bar{X}^{d-1}, 0, \ldots, 0) \\
2 & (0, \bar{1}, 0, \ldots, 0), \ldots, (0, \bar{f}^{\mu_1-1}\bar{X}^{d-1}, 0, \ldots, 0) \\
\vdots & \vdots \\
m_{\mu_1} & (0, \ldots, 0, \bar{1}, 0, \ldots, 0), \ldots, (0, \ldots, 0, \bar{f}^{\mu_1-1}\bar{X}^{d-1}, 0, \ldots, 0) \\
m_{\mu_1}+1 & (0, \ldots, 0, 0, \bar{1}, 0, \ldots, 0), \ldots, (0, \ldots, 0, 0, \bar{f}^{\mu_2-1}\bar{X}^{d-1}, 0, \ldots, 0) \\
\vdots & \vdots \\
m_{\mu_1} + \cdots + m_{\mu_s} & (0, \ldots, 0, \bar{1}), \ldots, (0, \ldots, 0, \bar{f}^{\mu_s-1}\bar{X}^{d-1}).
\end{array}$$

Wir nummerieren die obige Basis in natürlicher Weise wie folgt durch:

$$\begin{array}{ccccc}
1 & v_{11} & v_{12} & \dots & v_{1\,\mu_1 d} \\
2 & v_{21} & v_{22} & \dots & v_{2\,\mu_1 d} \\
\vdots & & \vdots & & \\
m_{\mu_1} & v_{\mu_1 1} & v_{\mu_1 2} & \dots & v_{\mu_1\,\mu_1 d} \\
m_{\mu_1}+1 & v_{\mu_1+1\,1} & v_{\mu_1+1\,2} & \dots & v_{\mu_1+1\,\mu_2 d} \\
\vdots & & \vdots & & \\
m_{\mu_1}+\dots m_{\mu_s} & v_{m_{\mu_1}+\dots m_{\mu_s}\,1} & v_{m_{\mu_1}+\dots m_{\mu_s}\,2} & \dots & v_{m_{\mu_1}+\dots m_{\mu_s}\,\mu_s d}.
\end{array}$$

Für die weiteren Schritte definieren wir die Untermoduln

$$V^k := \{g \in V \mid f^k g = 0\}.$$

Diese Untermoduln liefern eine Filtrierung

$$V = V^{\lambda_1} \supset V^{\lambda_1 - 1} \supset \dots \supset V_1 \supset V_0 = \{0\}$$

von V, die ausschlaggebend für unsere Abzählung sein wird.
Aus der Wahl unserer Basis folgt sofort, dass

$$dim(V^i) = h_i d,$$

wobei $h_i := \lambda'_1 + \dots + \lambda'_i$. In der Tat, denn: $(k = \lambda_1 = \mu_1)$

$$\begin{array}{rcll}
V^k & = & <\mathcal{B}> & \\
V^{k-1} & = & <\mathcal{B} & - \{v_{ij} \mid 1 \le i \le m_{\mu_1};\ \ 1 \le j \le d\} > \\
V^{k-2} & = & <\mathcal{B} & - \{v_{ij} \mid 1 \le i \le m_{\mu_1};\ \ 1 \le j \le 2d\} \\
 & & & - \{v_{ij} \mid m_{\mu_1} + 1 \le i \le m_{\mu_1} + m_{\mu_2};\ \ 1 \le j \le d\} > \\
\vdots & & \vdots & \\
V^{k-l} & = & <\mathcal{B} & - \{v_{ij} \mid 1 \le i \le m_{\mu_1};\ \ 1 \le j \le ld\} \\
 & & & - \{v_{ij} \mid m_{\mu_1} + 1 \le i \le m_{\mu_1} + m_{\mu_2};\ \ 1 \le j \le (l-1)d\} \\
 & & & \vdots \\
 & & & - \{v_{ij} \mid m_{\mu_1} + \dots + m_{\mu_{l-1}} + 1 \le i \le m_{\mu_1} + \dots + m_{\mu_l};\ \ 1 \le j \le d\} > .
\end{array}$$

Also haben wir:

$$\begin{array}{rcl}
\dim V^k & = & h_k d \\
\dim V^{k-1} & = & h_k d - m_k d = h_{k-1} d \\
\dim V^{k-2} & = & h_k d - 2m_k d - m_{k-1} d = h_{k-2} d \\
etc. & &
\end{array}$$

Sei nun $\phi \in Aut_{k[X]}(V)$. So gilt wegen $\phi(fv) = f\phi(v)\ \forall f \in k[X], v \in V$ insbesondere:

(i) $\phi(V^i) = V^i$, also $\phi(V^i \setminus V^{i-1}) = V^i \setminus V^{i-1}$.
(ii) $\phi\Big((0, \dots, 0, \bar{f}^i \bar{X}^j, 0, \dots 0)\Big) = f^i X^j \phi\Big((0, \dots, 0, \bar{1}, 0 \dots, 0)\Big)$.

Die Bedingung (ii) bedeutet, dass die Bilder der Vektoren aus Zeile k, der obigen nummerierten Basis, nach Wahl des Bildes von v_{k1} schon bestimmt sind. Wir müssen uns also nur überlegen, welche/wieviele Vektoren als Bild für die v_{k1} in Frage kommen. Im Folgenden bezeichnen wir die Bilder der v_{ij} mit w_{ij}.

Wegen (i) haben wir für w_{11} genau $q^{\dim V^{\mu_1}} - q^{\dim V^{\mu_1-1}}$ viele Möglichkeiten. Für w_{21} haben wir dann noch $q^{\dim V^{\mu_1}} - q^{\dim V^{\mu_1-1}+d}$ viele Möglichkeiten, weil w_{21} nur noch aus $V^{\mu_1} \setminus \left(V^{\mu_1-1} + < w_{11}, \ldots, w_{1d} >\right)$ gewählt werden kann. Das geht nun so weiter bis zum Vektor $w_{m_{\mu_1}1}$, für den wir aus demselben Grund nur noch $q^{\dim V^{\mu_1}} - q^{\dim V^{\mu_1-1}+(m_{\mu_1}-1)d}$ viele Möglichkeiten haben. Für $w_{m_{\mu_1}+1\,1}$ haben wir nun

$$q^{\dim V^{\mu_2}} - q^{\dim V^{\mu_2-1}+m_{\mu_1}d} = q^{\dim V^{\mu_2}} - q^{\dim V^{\mu_2}-m_{\mu_2}}$$

Möglichkeiten (wegen $h_{\mu_2-1} + m_{\mu_1} = h_{\mu_2} - m_{\mu_2}$, was wiederum aus $\lambda'_{\mu_2} = \lambda'_{\mu_1} + m_{\mu_2}$ folgt), denn wir können $w_{m_{\mu_1}+1\,1}$ beliebig aus $V^{\mu_2} \setminus \left(V^{\mu_2-1} + < \{w_{ij} \mid 1 \leq i \leq m_{\mu_1}; (\mu_1 - \mu_2)d + 1 \leq j \leq (\mu_1 - \mu_2)d + d\} >\right)$ wählen. So geht das bis zur letzten Zeile weiter.

Leichter verständlich aber etwas unsauber formuliert, lautet die Idee wie folgt:
Betrachten wir z.B die Zeile i mit $m_{\mu_1} + \cdots + m_{\mu_{t-1}} + 1 \leq i < m_{\mu_1} + \cdots + m_{\mu_t}$ und gehen davon aus, dass wir für alle vorherigen Zeilen schon die Bildvektoren ausgewählt haben. So haben wir aus den ersten m_{μ_1} Zeilen schon jeweils d Vektoren aus $V^{\mu_t} \setminus V^{\mu_t-1}$ ausgewählt und zwar die Bilder der Elemente dieser Zeilen mit $f^{\mu_1-\mu_t}x^i$ $(0 \leq i \leq d-1)$ als Eintrag. Aus den nächsten m_{μ_2} Zeilen hat man auch wieder jeweils d Vektoren ausgewählt und zwar die Bilder der Elemente dieser Zeilen mit $f^{\mu_2-\mu_t}x^i$ $(0 \leq i \leq d-1)$ als Eintrag usw. Aus den letzten $i-(\mu_1+\cdots+\mu_{t-1}+1)$ Zeilen hat man schon die Bilder der ersten d Vektoren jeder Zeile aus $V^{\mu_t} \setminus V^{\mu_t-1}$ ausgewählt, denn so wurde die Basis konzipiert. Mit

$$i = m_{\mu_1} + \cdots + m_{\mu_t} - j = \lambda'_{\mu_t} - j$$

kommt man für w_{i1} nun also auf

$$\begin{aligned} q^{\dim V^{\mu_t}} - q^{\dim V^{\mu_t-1}+(m_{\mu_1}+\ldots m_{\mu_{t-1}})d+(i-(m_{\mu_1}+\ldots m_{\mu_{t-1}}+1))d} &= q^{\dim V^{\mu_t}} - q^{\dim V^{\mu_t-1}+(i-1)d} \\ &= q^{\dim V^{\mu_t}} - q^{\dim V^{\mu_t}-jd} \end{aligned}$$

viele Wahlmöglichkeiten.

Das Ergebnis dieser Abzählung lässt sich am einfachsten notieren, wenn man gegebenenfalls leere Produkte künstlich in die Formel einfügt. So ergibt sich nach der ganzen Vorarbeit

Satz 3.2 *Sei f ein normiertes, irreduzibles Polynom vom Grad d und $V_f \cong k[X]/(f)^{\lambda_1} \oplus \cdots \oplus k[X]/(f)^{\lambda_r}$. Wir setzen $\lambda := (\lambda_1, \ldots, \lambda_r)$ und die Notation sei wie zuvor. Dann gilt:*

$$\mid Aut_{k[X]} V_f \mid = \prod_{i \geq 1} \prod_{j=1}^{m_i(\lambda)} \left(q^{h_i d} - q^{(h_i - j)d}\right).$$

Um später erfolgreich asymptotische Aussagen treffen zu können, müssen wir dieses Doppelprodukt in eine handhabbare Form bringen.

$$\begin{aligned}
\mid Aut_{k[X]} V_f \mid &= \prod_{i\geq 1} \prod_{j=1}^{m_i} \left(q^{h_i d} - q^{(h_i - j)d} \right) \\
&= \prod_{i\geq 1} q^{m_i h_i d} \prod_{j=1}^{m_i} \left(1 - q^{-jd} \right) \\
&= q^{\sum_{i\geq 1} m_i h_i d} \prod_{i\geq 1} \prod_{j=1}^{m_i} \left(1 - q^{-jd} \right).
\end{aligned}$$

Da $m_i(\lambda) = \lambda'_i - \lambda'_{i+1}$ haben wir

$$\begin{aligned}
\sum_{i\geq 1} m_i h_i &= \sum_{i\geq 1} (\lambda'_i - \lambda'_{i+1}) \sum_{j=1}^{i} \lambda'_j \\
&= \sum_{i\geq 1} \lambda'^2_i \\
&= |\lambda| + \sum_{i\geq 1} \lambda'_i (\lambda'_i - 1) \\
&= |\lambda| + 2n(\lambda).
\end{aligned}$$

Somit haben wir nun

$$|Aut_{k[X]} V_f| = q^{(|\lambda| + 2n(\lambda))d} \prod_{i\geq 1} \prod_{j=1}^{m_i} \left(1 - q^{-jd} \right).$$

Insgesamt erhalten wir das

Korollar 3.3 *Sei $A \in GL_n(k)$ eine invertierbare Matrix und sei $\Phi : \mathcal{I} \to Par$ die dazugehörige Partitionsfunktion. Dann gilt*

$$\mid Z(A) \mid = \prod_{f\in\mathcal{I}} q^{(|\Phi(f)| + 2n(\Phi(f))) \deg(f)} \prod_{i\geq 1} \prod_{j=1}^{m_i(\Phi(f))} (1 - q^{-j \deg(f)}).$$

Daraus folgt zudem das

Korollar 3.4 *Bedingungen wie zuvor. Dann gilt für $q \to \infty$*

$$\mid Z(A) \mid = q^{\sum_{f\in\mathcal{I}} (|\Phi(f)| + 2n(\Phi(f))) \deg(f)} + O\left(q^{\sum_{f\in\mathcal{I}} (|\Phi(f)| + 2n(\Phi(f))) \deg(f) - \min\{\deg f | f\in\mathcal{I} \ mit \ \Phi(f)\neq 0\}} \right).$$

4 Spezielle Matrizen und ihre Klassen

4.1 Diagonalisierbare Matrizen

Genau wie im Fall von $K = \mathbb{C}$ oder $K = \mathbb{R}$ spielen diagonalisierbare Matrizen natürlich auch über endlichen Körpern eine wichtige Rolle. In diesem Abschnitt werden wir uns deshalb mit diversen Abzählproblemen zu diagonalisierbaren Matrizen beschäftigen.

Man nennt eine Matrix $A \in Mat_n(k)$ diagonalisierbar, falls ein $S \in GL_n(k)$ existiert, sodass

$$SAS^{-1} = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & \text{\Large 0} & \\ & & \lambda_1 & & & \\ & & & \lambda_2 & & \\ & \text{\Large 0} & & & \ddots & \\ & & & & & \lambda_r \end{pmatrix},$$

mit $\lambda_i \in k$ paarweise verschieden.

In der Konjugationsklasse einer diagonalisierbaren Matrix ist also immer eine Matrix in obiger Form enthalten und diese Diagonalform ist, bis auf Permutation der Einträge auf der Hauptdiagonalen, eindeutig bestimmt.

Sei A eine diagonalisierbare Matrix und $B = TAT^{-1}$ ein Element der zugehörigen Konjugationsklasse. Dann gilt offensichtlich

$$B = TAT^{-1} = TS \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & \text{\Large 0} & \\ & & \lambda_1 & & & \\ & & & \lambda_2 & & \\ & \text{\Large 0} & & & \ddots & \\ & & & & & \lambda_r \end{pmatrix} S^{-1}T^{-1}.$$

In der Konjugationsklasse einer diagonalisierbaren Matrix sind also alle Elemente selbst wieder diagonalisierbar. Daher macht es Sinn im Rahmen dieser Arbeit von *diagonalisierbaren Klassen* zu sprechen (diese Bezeichnung hat außerhalb dieser Arbeit keine Relevanz und wird aus reiner Faulheit eingeführt). Da jede Matrix einer diagonalisierbaren Klasse zu einer Matrix in Diagonalform konjugiert ist, eignen sich diese sehr einfachen Matrizen perfekt als Repräsentanten.

Um die Willkür in der Anordnung der Diagonalelemente zu beseitigen, führen wir eine Ordnung auf k ein. Wir indizieren die Elemente von $\mathbb{F}_q$ beliebig, sodass $\mathbb{F}_q = \{\alpha_0, \dots, \alpha_{q-1}\}$ und $\alpha_0 = 0$. Wir definieren '>' auf $\mathbb{F}_q$ durch

$$\alpha_i > \alpha_j :\Leftrightarrow i > j.$$

Als Repräsentantensystem für die diagonalisierbaren Klassen wählen wir nun die Matrizen der Form

$$\begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & \text{\Large 0} & \\ & & \lambda_1 & & & \\ & & & \lambda_2 & & \\ & \text{\Large 0} & & & \ddots & \\ & & & & & \lambda_r \end{pmatrix}, \text{ mit } \lambda_1 > \lambda_2 > \cdots > \lambda_r.$$

Wir bezeichnen die obigen Matrizen auch mit $\mathrm{Diag}(\lambda_1, \dots, \lambda_1, \lambda_2, \dots, \lambda_r)$ oder kürzer auch mit $\mathrm{Diag}(n_1\lambda_1, n_2\lambda_2, \dots, n_r\lambda_r)$. Dabei bezeichnen die n_i die Vielfachheiten der λ_i auf der Diagonalen.

Wir haben, für feste Dimension n, die offensichtliche Bijektion :

$$\begin{aligned} N := \{\begin{pmatrix} n_1 \\ \vdots \\ n_{q-1} \end{pmatrix} \in \mathbb{N}^{q-1} \mid n_1 + \cdots + n_{q-1} = n\} &\to \{\text{diagonalisierbare Klassen in } GL_n(k)\} \\ \begin{pmatrix} n_1 \\ \vdots \\ n_{q-1} \end{pmatrix} &\mapsto \text{Klasse von } \mathrm{Diag}(n_1\alpha_1, n_2\alpha_2, \dots, n_{q-1}\alpha_{q-1}) \end{aligned}$$

Die linke Seite der Bijektion eignet sich hervorragend, um die diagonalisierbaren Klassen zu indizieren. Zum tatsächlichen Abzählen dieser Klassen verwenden wir aber eine andere Herangehensweise. In Kapitel 2 haben wir das gestellte Problem auf das Abzählen von besonderen Partitionsfunktionen reduziert und genau das wollen wir auch hier tun.

Satz 4.1 *Sei $A \in Mat_n(k)$ und bezeichne $m_A(X)$ das Minimalpolynom. Die Matrix A ist genau dann diagonalisierbar, wenn $m_A(X) = (X - \lambda_1) \cdots (X - \lambda_r)$ mit paarweise verschiedenen λ_i.*

Es bezeichnen $\mathcal{I}_1 := \{f \in \mathcal{I} \mid deg(f) = 1\}$ und $Par_1 := \{\lambda \in Par \mid \lambda_1 \leq 1\}$ (d.h $\lambda_i \leq 1\ \forall i$).
Das obige Theorem aus der linearen Algebra, zusammen mit dem Struktursatz für endliche erzeugte Moduln über Hauptidealringen aus 2.1, ergibt folgende

Proposition 4.2 *Wir haben eine 1:1 Abbildung*

$$\begin{aligned} \{\textit{diagonalisierbare Klassen in } GL_n(k)\} &\leftrightarrow \{\Phi : \mathcal{I}_1 \to Par_1 \textit{ mit } \sum_{f \in \mathcal{I}_1} |\Phi(f)| = n\} \\ c &\mapsto \textit{Partitionsfuntkion zu } c \\ \textit{Klasse zu } \Phi &\leftarrow\!\shortmid \quad \Phi. \end{aligned}$$

Beweis. Sei $A \in GL_n(k)$ mit Zerlegung

$$V_A \cong \bigoplus_{i \in \mathbb{N}, f \in \mathcal{I}} k[X]/(f)^{\Phi(f)_i}$$

für eine Partitionsfunktion Φ mit $\sum_{f \in I} deg(f)|\Phi(f)| = n$. Beachtet man, dass wir Partitionen so definiert haben, dass $\Phi(f)_1 \geq \Phi(f)_i$ für alle i gilt, so gilt insbesondere

$$m_A = \prod_{f \in \mathcal{I}} f^{\Phi(f)_1}.$$

Sei $A \in GL_n(k)$ diagonalisierbar, so gilt nach Satz 4.1, dass $m_A(X) = (X - \lambda_1) \cdots (X - \lambda_r)$ mit paarweise verschiedenen λ_i. Das heißt nichts anderes, als dass $\Phi(f)_i = 0$ für alle $f \in \mathcal{I}$ mit $\deg(f) > 1$ ($i \in \mathbb{N}$) und $\Phi(f)_i \leq 1$ für alle $f \in \mathcal{I}_1$ ($i \in \mathbb{N}$). Somit haben wir $\sum_{f \in \mathcal{I}} deg(f)|\Phi(f)| = \sum_{f \in \mathcal{I}_1} |\Phi(f)| = n$. Da alle $f \in \mathcal{I}$ mit $\deg(f) > 1$ auf die Nullpartition abgebildet werden, lassen wir diese f im Definitionsbereich weg und da $\Phi(f) = (1, \dots, 1, 0, \dots)$ für $f \in \mathcal{I}_1$, verkleinern wir den Bildbereich entsprechend. Dass die Partitionsfunktionen der rechten Seite diagonalisierbare Klassen vertreten, ist trivial. $\square$

Bemerkung Man sieht sofort, dass durch

$$\mathrm{Par}_1 \to \mathbb{N}\,, \quad (\underbrace{1, \dots, 1}_{n-mal}, 0, \dots) \mapsto n$$

eine Bijektion gegeben ist.

Nun sind wir endlich bereit die Anzahl d_n der diagonalisierbaren Klassen in $GL_n(k)$ zu bestimmen.

$$\begin{aligned}
\sum_{n \geq 0} d_n(q) X^n &= \sum_{\Phi : \mathcal{I}_1 \to Par_1} X^{\sum_{f \in \mathcal{I}} |\Phi(f)|} \\
&= \prod_{f \in \mathcal{I}_1} \left(\sum_{\lambda \in Par_1} X^{|\lambda|} \right) \\
&= \prod_{a \in \mathbb{F}_q^*} \left(\sum_{\lambda \in Par_1} X^{|\lambda|} \right) \\
&= \left(\sum_{\lambda \in Par_1} X^{|\lambda|} \right)^{q-1} \\
&\overset{Bem.}{=} \left(\sum_{i=0}^{\infty} X^i \right)^{q-1} \\
&= \left(\frac{1}{1 - X} \right)^{q-1}.
\end{aligned}$$

Der verallgemeinerte binomische Lehrsatz liefert

$$\frac{1}{(1-X)^{q-1}} = \sum_{n\geq 0} \binom{q-2+n}{n} X^n.$$

Somit erhalten wir für die Anzahl der diagonalisierbaren Klassen d_n:

$$d_n(q) = \binom{q-2+n}{n}.$$

Da sich diese Arbeit aber allgemeiner mit Matrizen als nur mit Klassen beschäftigt, wollen wir nicht nur die Anzahl der diagonalisierbaren Klassen, sondern auch die Anzahl der diagonalisierbaren (invertierbaren) **Matrizen** oder zumindest -wie hier geschehen- eine Asymptotik bestimmen. Die Anzahl der diagonalisierbaren Matrizen bezeichnen wir mit $D_n(q)$.

Wir haben bei der Bestimmung der Anzahl der diagonalisierbaren Klassen schon gesehen, dass der Hauptterm $\frac{1}{n!}q^n$ ist. Für $D_n(q)$ könnte man somit $\frac{1}{n!}q^{n^2}$ als Hauptterm erwarten und genau das werden wir in den folgenden Seiten beweisen.

Proposition 4.3 *Es gilt*

$$D_n(q) = \sum_{\substack{\Phi:\mathcal{I}_1\to Par_1 \\ \sum|\Phi(f)|=n}} \frac{\gamma(n)}{a_\Phi(q)} = \sum_{\substack{n_1+n_2+\cdots+n_{q-1}=n \\ n_i\in\mathbb{N}}} \frac{\gamma(n)}{\gamma(n_1)\cdots\gamma(n_{q-1})}\text{ , dabei ist } \gamma(0)=1. \tag{4.1}$$

Beweis Die erste Gleichung ist klar. Für die zweite Gleichung betrachten wir a_Φ für $\Phi : \mathcal{I}_1 \to \mathrm{Par}_1$ mit $\sum_{f\in\mathcal{I}_1} |\Phi(f)| = n$. Es seien $\Phi(f)'$ die konjugierte Partition zu $\Phi(f)$ und $h_i(f) := \Phi(f)'_1 + \Phi(f)'_2 + \cdots + \Phi(f)'_i$. Nach Korollar 3.3 gilt dann:

$$a_\Phi = \prod_{f\in\mathcal{I}_1} \prod_{i\geq 1} \prod_{j=1}^{m_i(\Phi(f))} \left(q^{h_i(f)\deg f} - q^{(h_i(f)-j)\deg f}\right).$$

Da $\Phi(f) \in \mathrm{Par}_1\ \forall f \in \mathcal{I}_1$, haben wir $m_i(\Phi(f)) = 0$ für $i > 1$ und $\sum_{f\in\mathcal{I}_1} m_1(\Phi(f)) = n$. Zudem gilt $h_i(f) = m_1(\Phi(f))$ für alle $i \in \mathbb{N}$. Somit erhalten wir, wegen $\deg f = 1$ für $f \in \mathcal{I}_1$:

$$\begin{aligned} a_\Phi &= \prod_{f\in\mathcal{I}_1} \underbrace{\prod_{j=1}^{m_1(\Phi(f))} \left(q^{m_1(\Phi(f))} - q^{m_1(\Phi(f))-j}\right)}_{\gamma(m_1(\Phi(f)))} \\ &= \prod_{f\in\mathcal{I}_1} \gamma\left(m_1(\Phi(f))\right). \end{aligned}$$

Da die genannten Partitionsfunktionen, sowie die nicht-negativen ganzzahligen Lösungen von $n_1 + \ldots n_{q-1} = n$, gleichermaßen die diagonalisierbaren Klassen parametrisieren, sind wir fertig. □

Wir studieren nun Gleichung (4.1) um die gewünschte Asymptotik zu erhalten.

Proposition 4.4 *Es seien $f, g \in \mathbb{Q}[X]$ mit $\deg f \geq \deg g$. Wir interpretieren $h := \frac{f}{g}$ als rationale Funktion. Existiert eine Folge natürlicher Zahlen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \to \infty$ für die gilt, dass $h(a_n) \in \mathbb{N}\ \forall n \in \mathbb{N}$, so gilt $g|f$. Insbesondere ist dann $h \in \mathbb{Q}[X]$ mit $\deg h = \deg f - \deg g$.*

Beweis Es sei

$$f = qg + r, \quad \text{mit } r, q \in \mathbb{Q}[X] \text{ und } \deg(r) < \deg(g).$$

Nun wählen wir ein $N \in \mathbb{N}$, sodass alle auftretenden Polynome in $\mathbb{Z}[X]$ sind. Nach Voraussetzung ist $\frac{Nf}{g}(a_n) \in \mathbb{N}$ für alle n, also auch $(Nq + \frac{Nr}{g})(a_n) \in \mathbb{N}$. Wir haben N so gewählt, dass $Nq \in \mathbb{Z}[X]$, also $Nq(a_n) \in \mathbb{Z}$. Damit muss nun aber auch $\frac{Nr}{g}(a_n) \in \mathbb{Z}$ für alle n gelten.
Mit $\deg r < \deg g$ folgt nun, dass $\frac{Nr}{g}(x) \xrightarrow{x\to\infty} 0$, d.h es existiert ein $N_1 \in \mathbb{N}$, sodass

$$\left|\frac{Nr}{g}(x)\right| < 1, \quad \forall x > N_1.$$

Insbesondere existiert ein $N_2 \in \mathbb{N}$ mit $\left|\frac{Nr}{g}(a_n)\right| < 1$ für alle $n > N_2$. Da $\frac{Nr}{g}(a_n) \in \mathbb{Z}$, haben wir stärker

$$\frac{Nr}{g}(a_n) = 0, \quad \forall n > N_2.$$

Somit hat $Nr \in \mathbb{Z}[X]$ unendlich viele Nullstellen; folglich gilt $r \equiv 0$. □

Diese Proposition besagt nun, dass alle Summanden aus (4.1) selbst wieder Polynome in q sind, denn:

Für Primzahlen (sogar für Primzahlpotenzen) stellen die Summanden in (4.1) die Größen von Konjugationsklassen in $GL_n(k)$ dar und dabei handelt es sich offensichtlich um natürliche Zahlen. Somit ist auch gleich gezeigt, dass $D_n(q)$ ein Polynom in q sein muss.

Sei $p = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ ein Polynom, so bezeichne $\mathrm{lt}(p) := a_nX^n$ den *Leitterm* von p. Weil $D_n(q)$ ein Polynom ist, müssen wir zur Untersuchung des asymptotischen Verhaltens nur den Leitterm dieses Polynoms bestimmen. Um dies zu tun, untersuchen wir zuerst die Leitterme der Summanden aus (4.1) und zählen dann wie oft der maximal auftretende Leitterm vorkommt. (Seien $\mathrm{lt}(p) = a_nX^n$ und $\mathrm{lt}(q) = b_mX^m$ so sagen wir, dass $\mathrm{lt}(p)$ größer ist als $\mathrm{lt}(q)$, falls $n > m$.) Aus Proposition 4.4 und der besonderen Form der folgenden rationalen Funktion (in q) folgt:

$$\mathrm{lt}\left(\frac{\gamma(n)}{\gamma(n_1)\cdots\gamma(n_{q-1})}\right) = q^{n^2-(n_1^2+\cdots+n_{q-1}^2)}.$$

Der Leitterm von $\frac{\gamma(n)}{\gamma(n_1)\cdots\gamma(n_{q-1})}$ ist genau dann maximal, wenn der Leitterm des Nenners minimal ist. Wir sind also auf der Suche nach den Diagonalmatrizen mit minimalem Zentralisator. Zu

minimieren ist nun also $n_1^2 + \cdots + n_{q-1}^2$ unter der Zusatzbedingung $n_1 + \cdots + n_{q-1} = n$.
Da wir nur an dem Verhalten von $D_n(q)$ für $q \to \infty$ interessiert sind, betrachten wir von vornherein die Situation $q > n$. Unter dieser Voraussetzung ist die Lösungsmenge dieses Minimierungsproblems offenbar

$$N_1 := \{\begin{pmatrix} n_1 \\ \vdots \\ n_{q-1} \end{pmatrix} \in \{0,1\}^{q-1} \mid n_1 + \cdots + n_{q-1} = n\}.$$

Bemerkung Die Suche nach Diagonalmatrizen mit kleinen Zentralisatoren, ist die Suche nach 'komplexen' (im Sinne von komplizierten) Diagonalmatrizen und die komplexesten Diagonalmatrizen sollten diejenigen sein, deren Diagonalelemente alle paarweise verschieden sind. Das ist das Ergebnis obiger Überlegung.

Es gilt $\mid N_1 \mid = \binom{q-1}{n}$, sodass die Vermutung nahe liegt, dass

$$\mathrm{lt}(D_n(q)) = \mathrm{lt}\left(\binom{q-1}{n}\frac{\gamma(n)}{\gamma(1)^n}\right) = \mathrm{lt}\left(\binom{q-1}{n}\right)\mathrm{lt}\left(\frac{\gamma(n)}{\gamma(1)^n}\right) = \frac{1}{n!}q^n q^{n^2-n} = \frac{1}{n!}q^{n^2}.$$

Wir müssen uns nur noch davon überzeugen, dass dies der einzig vorkommende q^{n^2} Term ist. Aus den anfänglichen Berechnungen diese Abschnitts wissen wir, dass (4.1) genau $d_n(q)$ viele Summanden hat und $\mathrm{lt}(d_n(q))=\frac{1}{n!}q^n$ ist.

Untersuchen wir in (4.1) die Summanden mit Leitterm q^{n^2-k}, wobei $k > n$, so kann die Summe dieser Terme höchstens einen $\frac{1}{n!}q^{n^2-k+n}$-Term liefern, da die Anzahl dieser Summanden maximal $d_n(q)$ sein kann. Natürlich können Terme mit Exponent $n^2 - k$ zusätzlich noch von $\binom{q-1}{n}\frac{\gamma(n)}{\gamma(1)^n}$ und anderen Termen dieser Bauart (mit größerem Leitterm als q^{n^2-k+n}) kommen, aber der Beitrag eines solchen Terms hängt nur von n ab, und die Anzahl solcher Terme hat wieder nur maximal den Leitterm $\frac{1}{n!}q^n$. Für $q \to \infty$ kann die Abhängigkeit von n vernachlässigt werden, sodass wir insgesamt zu folgendem Ergebnis kommen:

Satz 4.5 *Es gilt*

$$D_n(q) = \frac{1}{n!}q^{n^2} + O(q^{n^2-1}).$$

Für exakte Werte von $d_n(q)$ und dem Vergleich von $\mathrm{lt}(D_n(q))$ und $D_n(q)$ sei auf die Tabellen A.2, A.4 und A.5 verwiesen.

4.2 Jordan-normalisierbare Matrizen

Eine erste Verallgemeinerung der Diagonalisierbarkeit, stellt die Jordan-Normalisierbarkeit dar. Ziel ist es eine Normalform anzugeben, die eine größere Klasse von Matrizen umfasst, ohne dabei stark an Einfachheit einzubüßen.

Eine Matrix A heißt *jordan-normalisierbar*, falls eine Matrix $S \in GL_n(k)$ existiert, sodass

$$SAS^{-1} = \begin{pmatrix} J(\lambda_1, r_1^{(1)}) & & & & & \\ & \ddots & & & \mathbf{0} & \\ & & J(\lambda_1, r_{t_1}^{(1)}) & & & \\ & & & J(\lambda_2, r_1^{(2)}) & & \\ & \mathbf{0} & & & \ddots & \\ & & & & & J(\lambda_s, r_{t_s}^{(s)}) \end{pmatrix},$$

wobei

$$J(\lambda, r) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ & & & \lambda \end{pmatrix} \in Mat_r(k)$$

der *Jordan-Block* zu λ der Dimension r ist.

Genau wie im Fall diagonalisierbarer Klassen ist 'Jordan-Normalisierbarkeit' eine Klasseneigenschaft, sodass wir problemlos von *Jordan-Klassen* sprechen können. Durch ähnliche Festlegungen wie im vorherigen Kapitel erhalten wir auch hier ein einfaches Repräsentantensystem aus Matrizen der folgenden Form:

$$\begin{pmatrix} J(\lambda_1, r_1^{(1)}) & & & & & \\ & \ddots & & & \mathbf{0} & \\ & & J(\lambda_1, r_{t_1}^{(1)}) & & & \\ & & & J(\lambda_2, r_1^{(2)}) & & \\ & \mathbf{0} & & & \ddots & \\ & & & & & J(\lambda_s, r_{t_s}^{(s)}) \end{pmatrix}, \quad \begin{array}{l} \text{sodass } \lambda_1 > \lambda_2 > \cdots > \lambda_s \text{ und} \\ \forall i \in \{1, \ldots, s\} \text{ gilt:} \\ r_1^{(i)} \geq r_2^{(i)} \geq \cdots \geq r_{t_i}^{(i)}. \end{array}$$

Nun bezeichne $Par^n := Par \times \cdots \times Par$ wie üblich das n-fache kartesische Produkt. Dann hat man die offensichtliche

Proposition 4.6 *Es gilt*

$$\{\textit{Jordan-Klassen in } GL_n(k)\} \overset{1:1}{\longleftrightarrow} \{\begin{pmatrix} \lambda^{(1)} \\ \vdots \\ \lambda^{(q-1)} \end{pmatrix} \in Par^{q-1} \Big| \, |\lambda^{(1)}| + \cdots + |\lambda^{(q-1)}| = n\}.$$

Beweis Analog zur Aussage über diagonale Klassen. □

Auch hier bewährt sich zur tatsächlichen Abzählung der Jordan-Klassen wieder der Zugang durch Partitionsfunktionen. Welche Partitionsfunktionen zu den Jordan-Klassen gehören, beantwortet uns

Satz 4.7 *Eine Matrix A ist genau dann jordan-normalisierbar, wenn ihr charakteristisches Polynom in Linearfaktoren zerfällt.*

Daraus folgt direkt

Proposition 4.8 *Wir haben*

$$\{\textit{Jordan-Klassen in } GL_n(k)\} \xleftrightarrow{1:1} \{\Phi : \mathcal{I}_1 \to \ \textit{Par} \quad \textit{mit} \ \sum_{f \in \mathcal{I}_1} |\Phi(f)| = n\}.$$

Wir bezeichnen mit j_n die Anzahl der Jordan-Klassen in $GL_n(k)$. Die Proposition erlaubt uns nun wieder mit erzeugenden Funktionen zu arbeiten und wir erhalten:

$$\begin{aligned}
\sum j_n X^n &= \sum_{\Phi:\mathcal{I}_1 \to \mathrm{Par}} X^{\sum_{f\in\mathcal{I}_1} |\Phi(f)|} \\
&= \prod_{f\in\mathcal{I}_1} \left(\sum_{\lambda \in \mathrm{Par}} X^{|\lambda|} \right) \\
&= \prod_{a \in \mathbb{F}_q^\star} \left(\sum_{n=0}^{\infty} p(n) X^n \right) \\
&= \left(\sum_{n=0}^{\infty} p(n) X^n \right)^{q-1} \\
&= \left(\prod_{i \geq 1} \frac{1}{1-X^i} \right)^{q-1}.
\end{aligned}$$

Aus dem vorherigen Kapitel wissen wir, dass

$$\sum_{n=0}^{\infty} d_n X^n = \frac{1}{(1-X)^{q-1}}.$$

Somit erhalten wir für j_n:

$$\sum_{n=0}^{\infty} j_n X^n = \prod_{i \geq 1} \left(\sum_{n=0}^{\infty} d_n X^{in} \right). \qquad (\star)$$

Nun ist es sehr schwierig und uninteressant eine geschlossene Formel für j_n zu finden, also bemühen wir uns in dieser Richtung nicht weiter. Zumal wir für die angestrebte Asymptotik nur am Leitterm von j_n interessiert sind und der folgt ganz leicht aus ($\star$).

Proposition 4.9 *Es gilt*

$$lt(j_n) = lt(d_n) = \frac{1}{n!} q^n.$$

Wir bezeichnen die Anzahl der jordan-normalisierbaren Matrizen aus $GL_n(k)$ mit $J_n(q)$. Ganz offensichtlich haben wir:

$$J_n(q) = \sum_{\substack{\Phi:\mathcal{I}_1\to \mathrm{Par} \\ \sum|\Phi(f)|=n}} \frac{\gamma_n(q)}{a_\Phi(q)}.$$

Wie in Abschnitt 4.1 folgt, dass $J_n(q)$ ein Polynom in q ist. Wir müssen die obige Summe, also auf ihren Leitterm untersuchen. Dazu werden wir, wie im Fall der diagonalisierbaren Matrizen, zuerst untersuchen was der größtmögliche Leitterm unter den Summanden der Form $\frac{\gamma_n}{a_\Phi}$ ist, und zählen in einem zweiten Schritt dann die Anzahl dieser Summanden.

Nun gilt:

$$\begin{aligned}\mathrm{lt}\left(\frac{\gamma_n}{a_\Phi}\right) &= q^{n^2-\sum_{f\in\mathcal{I}_1}|\Phi(f)|+2n(\Phi(f))} \\ &= q^{n^2-n-\sum_{f\in\mathcal{I}_1}2n(\Phi(f))}.\end{aligned}$$

Wegen $n(\lambda) = \sum_{i\geq 1}(i-1)\lambda_i$ (für $\lambda = (\lambda_1, \lambda_2, \dots)$) ist $\mathrm{lt}\left(\frac{\gamma_n}{a_\Phi}\right)$ maximal, wenn die Partitionen $\Phi(f)$ von der Form $(\lambda_1, 0, \dots)$ sind, denn dann gilt offensichtlich $2n(\Phi(f)) = 0$ und wir erhalten

$$\mathrm{lt}\left(\frac{\gamma_n}{a_\Phi}\right) = q^{n^2-n}.$$

Im zweiten Schritt müssen wir somit

$$\left|\{\Phi : \mathcal{I}_1 \to \mathrm{Par}| \sum|\Phi(f)| = n \text{ und } \Phi(f)_i = 0, \text{ falls } i \geq 2\}\right|$$

bestimmen. Es gilt

$$\begin{aligned}\{\Phi : \mathcal{I}_1 \to \mathrm{Par}| \sum|\Phi(f)| = n \text{ und } \Phi(f)_i = 0, \text{ falls } i \geq 2\} &\to \{\Phi : \mathcal{I}_1 \to \mathrm{Par}_1| \sum|\Phi(f)| = n\} \\ \Phi &\mapsto \left(\Phi^\star : \mathcal{I}_1 \to \mathrm{Par}_1, f \mapsto (\underbrace{1,\dots,1}_{\Phi(f)_1-mal}, 0, \dots)\right)\end{aligned}$$

ist eine Bijektion, sodass beide Mengen gleichmächtig sind. In Abschnitt 4.1 haben wir aber schon gezeigt, dass

$$\left|\{\Phi : \mathcal{I}_1 \to \mathrm{Par}_1| \sum|\Phi(f)| = n\}\right| = d_n$$

und $\mathrm{lt}(d_n) = \frac{1}{n!}q^n$.

Insgesamt haben wir nun also

$$\begin{aligned}\mathrm{lt}(J_n) &= \mathrm{lt}(d_n q^{n^2-n}) \\ &= \frac{1}{n!}q^{n^2}.\end{aligned}$$

Die Zweifel über eine mögliche Rebellion der Summanden mit kleineren Leittermen als q^{n^2-n}, zerschlägt man genauso wie im Fall der diagonalisierbaren Matrizen.
Man erhält somit den

Satz 4.10 *Für $q \to \infty$ gilt*

$$J_n(q) = \frac{1}{n!} q^{n^2} + O\left(q^{n^2-1}\right).$$

Zusammen mit Satz 4.5 haben wir nun:

Die Wahrscheinlichkeit, zufällig eine diagonalisierbare invertierbare Matrix aus der Familie der jordan-normalisierbaren invertierbaren Matrizen auszuwählen, geht für $q \to \infty$ gegen 1.

Die nächste Frage ist nun, wie groß die Differenz $B_n(q) := J_n(q) - D_n(q)$ ist. Dabei erlaubt uns die vorgestellte Methode $B_n(q)$ zu untersuchen, ohne weitere Terme von $J_n(q)$ oder $D_n(q)$ bestimmen zu müssen. Mit $b_n(q) := j_n(q) - d_n(q)$ bezeichnen wir die Anzahl aller jordan-normalisierbaren Klassen, die nicht diagonalisierbar sind. Wir wissen, dass

$$\sum_{n \geq 0} j_n X^n = \prod_{i \geq 1} \left(\sum_{n=0}^{\infty} d_n X^n \right).$$

Wir untersuchen nun

$$\begin{array}{lllllllll}
(1 & +d_1X & +d_2X^2 & +d_3X^3 & +d_4X^4 & +d_5X^5 & +d_6X^6 & +d_7X^7 & +\dots \\
(1 & & +d_1X & & +d_2X^4 & & +d_3X^6 & & +\dots \\
(1 & & & +d_1X^3 & & & +d_2X^6 & & +\dots \\
(1 & & & & +d_1X^4 & & & & +\dots \\
(1 & & & & & +d_1X^5 & & & +\dots \\
(1 & & & & & & +d_1X^6 & & +\dots \\
(1 & & & & & & & +d_1X^7 & +\dots
\end{array}$$

um $b_n(q) = j_n(q) - d_n(q)$ für kleine n zu bestimmen.
Daraus folgt:

$$\begin{aligned}
j_1 &= d_1 \\
j_2 &= d_2 + d_1 \\
j_3 &= d_3 + d_1 + d_1^2 \\
j_4 &= d_4 + d_2 + d_1 + d_1^2 + \mathbf{d_1 d_2} \\
j_5 &= d_5 + d_1 + d_1^2 + 2d_1 d_2 + \mathbf{d_1 d_3} \\
j_6 &= d_6 + d_3 + d_2 + d_1 + d_1^2 + 2d_1 d_2 + d_1 d_3 + \mathbf{d_1 d_4} + d_1^3 \\
j_7 &= d_7 + d_1 + 3d_1^2 + 2d_1 d_2 + d_1 d_3 + d_1 d_4 + \mathbf{d_1 d_5} + d_2 d_3 + d_1^3 + d_1^2 d_2.
\end{aligned}$$

Wir suchen offensichtlich nach den Summanden mit Leittermen der Form cq^{n-1} ($c \in \mathbb{Q}$) (ab $n = 4$ fett gedruckt) und wie man am Beispiel sieht, sind die interessanten Terme von der Form $d_1 d_{n-2}$. Man überlegt sich sofort, dass dies für alle n gilt. Somit haben wir schonmal:

$$\operatorname{lt}(b_n(q)) = \frac{1}{(n-2)!} q^{n-1}.$$

Bei der Bestimmung von $\mathrm{lt}(B_n(q))$ gehen wir genauso vor, wie auch schon für $J_n(q)$ und $D_n(q)$. Es gilt:

$$B_n(q) = \sum_{\substack{\Phi:\mathcal{I}_1 \to \mathrm{Par} \\ \sum|\Phi(f)|=n \\ \exists f \text{ mit } \Phi(f)\notin \mathrm{Par}_1}} \frac{\gamma_n(q)}{a_\Phi(q)}. \qquad (\star)$$

Der größtmögliche Leitterm der Summanden $\frac{\gamma(n)}{a_\Phi}$ aus $(\star)$ ist q^{n^2-n} und die Anzahl solcher Summanden entspricht

$$\begin{aligned} z(n,q) := &\left|\{\Phi : \mathcal{I}_1 \to \mathrm{Par} \mid \sum_{f\in\mathcal{I}_1} |\Phi(f)| = n, \exists f \in \mathcal{I}_1 \text{ mit } \Phi(f)_1 > 1 \text{ und } \Phi(f)_i = 0 \ \forall f \in \mathcal{I}_1, i \geq 2\}\right| \\ = &\left|\{\Phi : \mathcal{I}_1 \to \mathbb{N} \mid \sum_{f\in\mathcal{I}_1} \Phi(f) = n, \Phi(f) > 1 \text{ für mind. ein } f\}\right| \\ = &\underbrace{\left|\{\Phi : \mathcal{I}_1 \to \mathbb{N} \mid \sum_{f\in\mathcal{I}_1} \Phi(f) = n\}\right|}_{(1)} - \underbrace{\left|\{\Phi : \mathcal{I}_1 \to \{0,1\} \mid \sum_{f\in\mathcal{I}_1} \Phi(f) = n\}\right|}_{(2)}. \end{aligned}$$

Aus den vorherigen Kapiteln wissen wir schon, dass $(1) = d_n$ und $(2) = \binom{q-1}{n}$ (falls wir von vornherein $q > n$ voraussetzen) und für beide ist der Leitterm $\frac{1}{n!}q^n$, sodass der Leitterm von $z(n,q)$ maximal noch cq^{n-1} sein kann ($c \in \mathbb{Q}$). Mit

$$d_n(q) = \binom{q+n-2}{n} = \frac{1}{n!}(q-1)q(q+1)(q+1)\cdots(q+(n-2)),$$

folgt für den Koeffizienten c_1 von q^{n-1} in $d_n(q)$:

$$\begin{aligned} c_1 &= \frac{1}{n!}\left[(n-2)+(n-3)+(n-4)+\cdots+1-1\right] \\ &= \frac{1}{n!}\left[\frac{((n-2)+1)}{2}(n-2)-1\right]. \end{aligned}$$

Mit

$$\begin{aligned} \binom{q-1}{n} &= \frac{1}{n!}(q-1)((q-1)-1)\cdots((q-1)-(n-2))((q-1)-(n-1)) \\ &= \frac{1}{n!}(q-1)\cdots(q-n), \end{aligned}$$

folgt für den Koeffizienten c_2 von q^{n-1} in (2):

$$\begin{aligned} c_2 &= \frac{1}{n!}\left[-n-(n-1)-(n-2)-\cdots-1\right] \\ &= -\frac{1}{n!}\frac{(n+1)n}{2}. \end{aligned}$$

Insgesamt erhalten wir nun für den Leitterm von $z(n, q)$:

$$\begin{aligned}\mathrm{lt}(z(n,q)) &= \frac{1}{n!}\left[\frac{(n-2)+1}{2}(n-2) - 1 + \frac{n+1}{2}n\right] q^{n-1}\\ &= \frac{1}{n!}n(n-1)q^{n-1}\\ &= \frac{1}{(n-2)!}q^{n-1}.\end{aligned}$$

Mit denselben Argumenten wie zuvor erhalten wir nun den

Satz 4.11 *Für $q \to \infty$ gilt*

$$B_n(q) = \frac{1}{(n-2)!}q^{n^2-1} + O\left(q^{n^2-2}\right).$$

Der Satz sagt uns, dass die Differenz von $J_n(q)$ und $D_n(q)$ in gewissem Sinn so groß wie möglich ist. Sie stimmen zwar im Leitterm überein, aber schon der nächstgrößere Term der Polynome unterscheidet sich. Bemerkenswert ist dabei, dass wir dieses Ergebnis erlangen konnten, ohne die q^{n^2-1} Terme dieser beiden Polynome zu bestimmen; eine Aufgabe die sehr viel Rechenarbeit erfordert hätte.

4.3 Halbeinfache Matrizen

Nun kommen wir zur wohl interessantesten Familie von Matrizen die in dieser Arbeit studiert wurden. Die *Halbeinfachheit* stellt dabei eine sinnvolle Verallgemeinerung der Diagonalisierbarkeit dar, sodass die halbeinfachen Matrizen zumindest schon einmal die diagonalisierbaren Matrizen umfassen.

Definitionen
(a) Ein Modul heißt *einfach*, falls er keine echten Untermoduln $\neq \{0\}$ besitzt.
(b) Ein Modul heißt *halbeinfach*, falls er die direkte Summe von einfachen Moduln ist.
(c) Eine Matrix A heißt halbeinfach, falls V_A ein halbeinfacher $k[X]$-Modul ist.

Die Halbeinfachheit lässt sich auf viele weitere, äquivalente Weisen definieren, aber für unsere Bedürfnisse ist diese Definition die handlichste; sie erlaubt uns die bisher entwickelten Beweismethoden ganz einfach zu übernehmen. Zudem wissen wir, dass die $k[X]$-Modulstruktur von V_A nur von der Konjugationsklasse c mit $A \in c$ abhängt, weshalb die Halbeinfachheit auch eine Klasseneigenschaft ist. Wir sprechen dann von *halbeinfachen Klassen*. Die Anzahl dieser Klassen in $GL_n(k)$ bezeichnen wir mit s_n (s für semisimple).

Bemerkung Jeder einfache $k[X]$-Modul hat die Form $k[X]/(f(X))$, wobei f ein normiertes, irreduzibles Polynom ist.

Beweis:
Sei allgemein M ein einfacher R-Modul (R kommutativer Ring) und $0 \neq x \in M$. Dann gilt $M = Rx$. Hätten wir $y \in M \setminus Rx$, so hätten wir

$$0 \subsetneq < x > \subsetneq < x, y > \subset M,$$

ein Widerspruch. Wir erhalten durch

$$R \to M, \quad \lambda \mapsto \lambda x$$

den Isomorphismus $M \cong R/Ann(x)$, wobei Ann(x):= $\{\lambda \in R | \lambda x = 0\}$ den Annihilator von x bezeichnet. Wegen der Einfachheit von M ist Ann(x) ein maximales Ideal. In der Situation $R = k[X]$ sind die maximalen Ideale erzeugt durch die normierten, irreduziblen Polynome, sodass die Behauptung folgt.

Somit ergibt sich leicht die

Proposition 4.12 *Sei $c = c_\Phi$ eine Konjugationsklasse mit zugehöriger Partitionsfunktion Φ. Dann gilt:*

$$V_c \textit{ ist halbeinfach } \Leftrightarrow \Phi(f)_i \leq 1 \;\; \forall f \in \mathcal{I}, i \in \mathbb{N}.$$

Beweis Klar mit Bemerkung. □

Diese Proposition erlaubt uns nicht nur die halbeinfachen Klassen wie gewohnt mit Hilfe erzeugender Funktionen abzuzählen, sondern sie offenbart auch eine rein matrizentheoretische Definition der Halbeinfachheit.

Proposition 4.13 *Eine Matrix $A \in Mat_n(k)$ ist halbeinfach, falls sie über einer endlichen Körpererweiterung $L|k$ diagonalisierbar ist.*

Proof Sei c die Konjugationsklasse der A angehört, dann wissen wir aus der vorherigen Proposition, dass V_c die direkte Summe von endlichen Körpererweiterungen von k ist. Seien die Grade dieser Erweiterungen $d_1, \ldots, d_m$. Dann sind alle auftretenden Körpererweiterungen in $L := F_{q^{kgV(d_1,\ldots,d_m)}}$ enthalten. Weil endliche Körper perfekt sind, zerfällt jedes irreduzible Polynom f über k vom Grad d_i in d_i viele paarweise verschiedene Linearfaktoren über L.
Nach dem chinesischen Restsatz zerlegt sich V_c, betrachtet als $L[X]$-Modul, also noch weiter. Zu dieser neuen, feineren Zerlegung gehört nun eine Partitionsfunktion $\Phi : \mathcal{I}(q^{kgV(d_1,\ldots,d_m)})_1 \cup \{X\} \to Par_1$. Nach Proposition 4.2 (in der man $\mathcal{I}_1$ hier nun durch $\mathcal{I}_1 \cup \{X\}$ ersetzen muss) ist A also diagonalisierbar über L. □

Kommen wir nun zur Abzählung der halbeinfachen Klassen. Es gilt:

$$\begin{aligned}
\sum s_n X^n &= \sum_{\Phi:\mathcal{I}\to Par_1} X^{\sum_{f\in\mathcal{I}} |\Phi(f)| \deg(f)} \\
&= \prod_{f\in\mathcal{I}} \left(\sum_{\lambda\in Par_1} X^{|\lambda| \deg f} \right) \\
&= \prod_{f\in\mathcal{I}} \left(\sum_{i=0}^{\infty} X^{i \deg f} \right) \\
&= \prod_{f\in\mathcal{I}} \frac{1}{1 - X^{\deg f}} \\
&= \prod_{n\geq 1} \left(\frac{1}{1 - X^n} \right)^{\beta(n,q)} .
\end{aligned}$$

Nun arbeiten wir mit dem formalen Logarithmus beider Seiten weiter. Wir haben dann

$$\begin{aligned}
\log \sum s_n X^n &= \log \prod_{n\geq 1} (1 - X^n)^{-\beta(n,q)} \\
&= \sum_{n\geq 1} -\beta(n,q) \log(1 - X^n) \\
&= \sum_{n\geq 1} -\beta(n,q) \sum_{i\geq 1} (-1)^{i-1} \frac{(-X^n)^i}{i} \\
&= \sum_{n\geq 1} \beta(n,q) \sum_{i\geq 1} \frac{X^{in}}{i} \\
&= \sum_{N\geq 1} \left(\sum_{d|N} \beta(d,q) \frac{1}{N/d} \right) X^N \\
&= \sum_{N\geq 1} \frac{1}{N} \left(\sum_{d|N} d\beta(d,q) \right) X^N \\
&= \sum_{N\geq 1} \frac{1}{N} \left(-1 + \sum_{d|N} d \frac{1}{d} \sum_{j|d} \mu(\frac{d}{j}) q^j \right) X^N.
\end{aligned}$$

Es bezeichne $a(j,N)$ den Koeffizienten vor $q^j X^N$. Offensichtlich ist $a(j,N) = 0$, falls $j \nmid N$. Ansonsten gilt

$$a(j,N) = \sum_{k|\frac{N}{j}} \mu(k).$$

Mit der bekannten Identität

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{für } n > 1, \end{cases}$$

erhalten wir somit

$$\begin{aligned}\log \sum s_n X^n &= \sum_{N\geq 1} \frac{1}{N}\left(-1+q^N\right)X^N\\ &= \sum_{N\geq 1} -\frac{1}{N}X^N + \sum_{N\geq 1}\frac{1}{N}q^N X^n\\ &= \log(1-X) - \log(1-qX)\\ &= \log\left(\frac{1-X}{1-qX}\right).\end{aligned}$$

Insgesamt haben wir also

$$\begin{aligned}\sum s_n X^n &= \frac{1-X}{1-qX}\\ &= (1-X)\sum_{n=0}^{\infty} q^n X^n\\ &= 1 + \sum_{n=1}^{\infty}(q^n - q^{n-1})X^n.\end{aligned}$$

Somit hat man eine einfache kleine Formel zur Bestimmung der Anzahl aller halbeinfacher Klassen in $GL_n(k)$, die wir der Vollständigkeit halber nochmals notieren.

Satz 4.14 *Notation wie zuvor. Für $n \geq 2$ gilt:*

$$s_n = q^n - q^{n-1}.$$

Nun bezeichne $S_n(q)$ die Anzahl der halbeinfachen Matrizen in $GL_n(k)$. Offensichtlich hat man wieder

$$S_n(q) = \sum_{\substack{\Phi:\mathcal{I}\to \mathrm{Par}_1\\ \sum|\Phi(f)|=n}} \frac{\gamma_n(q)}{a_\Phi(q)}.$$

Diese Summe untersuchen wir genauso wie zuvor. Zuerst untersuchen wir die Summanden auf den größtmöglichen Leitterm und danach untersuchen wir, wie oft dieser Leitterm unter allen Summanden auftritt. Damit erhalten wir den Leitterm und letztendlich die angestrebte Asymptotik für S_n.

Wie im Fall der jordan-normalisierbaren Matrizen ist auch hier der Exponent im Leitterm $\mathrm{lt}\left(\frac{\gamma_n}{a_\Phi}\right)$ maximal, falls $n(\Phi(f)) = 0$ für alle $f \in \mathcal{I}$. Der maximal auftretende Exponent ist also wieder $n^2 - n$. Die Anzahl der Summanden mit dem Leitterm q^{n^2-n} entspricht dann der Anzahl der Partitionsfunktionen $\Phi : \mathcal{I} \to \mathrm{Par}_1$ mit $\sum_{f\in\mathcal{I}} |\Phi(f)| \deg(f) = n$ und $\Phi(f)_i = 0$ für $i > 1$. Kurz gesagt suchen wir

$$z(n,q) := \left|\{\Phi : \mathcal{I} \to \{0,1\} | \sum_{f\in\mathcal{I}} \Phi(f)\deg(f) = n\}\right|.$$

Zuvor benötigen wir aber noch die etwas unbekannte aber einfache Identität

Proposition 4.15 *Es bezeichne μ, wie schon zuvor, die Möbiusfunktion. Dann gilt*

$$\sum_{k|d}(-1)^{\frac{d}{k}-1}\mu(k) = \begin{cases} 1 & \textit{für } d = 1 \\ -2 & \textit{für } d = 2 \\ 0 & \textit{für } d > 2. \end{cases}$$

Beweis Die Werte für $d = 1$ und $d = 2$ sieht man sofort. Für $d > 2$ ungerade haben wir ganz klassisch $\sum_{k|d}\mu(k) = 0$. Ist $d > 2$ gerade, so müssen wir nur zeigen, dass die Anzahl der $k|d$ mit $(-1)^{\frac{d}{k}-1} = (-1)$ und $\mu(k) \neq 0$ gerade ist. Dann ist die Anzahl an 'echten' Vorzeichenwechseln gerade, also ändert man nichts am Wert der üblichen Identität.
(i) Sei $d = 2p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$ die Primfaktorzerlegung von d mit $p_i \neq 2$ paarweise verschieden. Man hat die einfache Bijektion

$$\{k|d \text{ mit } \mu(k) \neq 0 \text{ und } (-1)^{\frac{d}{k}-1} = -1\} \xleftrightarrow{1:1} \{\text{Teilmengen von } \{p_1, p_2 \ldots, p_t\}\}.$$

Wir wissen aber, dass $\left|\{\text{Teilmengen von } \{p_1, p_2 \ldots, p_t\}\}\right| = 2^t$. Also ist die Anzahl der Vorzeichenwechsel gerade.
(ii) Sei $d = 2^l p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$ mit $l > 1$ (Rest wie zuvor). Dann hat man analog die Bijektion

$$\{k|d \text{ mit } \mu(k) \neq 0 \text{ und } (-1)^{\frac{d}{k}-1} = -1\} \xleftrightarrow{1:1} \{\text{Teilmengen von } \{2, p_1, p_2 \ldots, p_t\}\}.$$

Mit $\left|\{\text{Teilmengen von } \{2, p_1, p_2 \ldots, p_t\}\}\right| = 2^{t+1}$ folgt die Behauptung. Die Identität ist somit bewiesen. $\square$

Nun kommen wir zur ursprünglichen Abzählung unserer Funktionen $\Phi : \mathcal{I} \to \{0, 1\}$.

$$\begin{aligned} \sum z(n,q)X^n &= \sum_{\Phi:\mathcal{I}\to\{0,1\}} X^{\sum_{f\in\mathcal{I}} \Phi(f)\deg(f)} \\ &= \prod_{f\in\mathcal{I}}\left(\sum_{\lambda\in\{0,1\}} X^{\lambda\deg(f)}\right) \\ &= \prod_{f\in\mathcal{I}}\left(1 + X^{\deg(f)}\right) \\ &= \prod_{n=1}^{\infty}(1 + X^n)^{\beta(n,q)}. \end{aligned}$$

Nun gehen wir wieder zum formalen Logarithmus über.

$$\begin{aligned}
\log \sum z(n,q)X^n &= \log\left(\prod_{n=1}^{\infty}(1+X^n)^{\beta(n,q)}\right) \\
&= \sum_{n=1}^{\infty}\beta(n,q)\log(1+X^n) \\
&= \sum_{n=1}^{\infty}\beta(n,q)\sum_{k\geq 1}(-1)^{k-1}\frac{X^{nk}}{k} \\
&= \sum_{N\geq 1}\left(\sum_{d|N}\beta(d,q)\frac{(-1)^{\frac{N}{d}-1}}{N/d}\right)X^N \\
&= \sum_{N\geq 1}\frac{1}{N}\left(\sum_{d|N}(-1)^{\frac{N}{d}-1}d\beta(d,q)\right)X^N \\
&= \sum_{N\geq 1}\frac{1}{N}\left((-1)^N+\sum_{d|N}(-1)^{\frac{N}{d}-1}\sum_{l|d}\mu(\frac{l}{d})q^l\right)X^N.
\end{aligned}$$

Mit unserer Identität erhalten wir nun (genau wie bei der Bestimmung von s_n):

$$\log \sum z(n,q)X^n = \sum_{N\geq 1}\frac{1}{N}b_N(q)X^N,\ \text{wobei } b_N(q) = \begin{cases} q^N+(-1)^N & \text{für } N \text{ ungerade} \\ q^N-2q^{N/2}+(-1)^N & \text{für } N \text{ gerade.}\end{cases}$$

Weiterhin gilt also

$$\begin{aligned}
\log \sum z(n,q)X^n &= \sum_{N\geq 1}\frac{1}{N}(-1)^N X^N + \sum_{N\geq 1}\frac{1}{N}q^N X^N - 2\sum_{N\geq 1}\frac{1}{N}q^N X^{2N} \\
&= -\log(1+X)-\log(1-qX)+2\log(1-qX^2).
\end{aligned}$$

Daraus folgt

$$\sum z(n,q)X^n = \frac{(1-qX^2)^2}{(1+X)(1-qX)}.$$

Mit

$$\begin{aligned}
\frac{1}{(1+X)}\frac{1}{(1-qX)} &= \left(\sum_{n\geq 0}(-1)^n X^n\right)\left(\sum_{n\geq 0}q^n X^n\right) \\
&= \sum_{n\geq 0}\left(\sum_{k=0}^{n}(-1)^k q^{n-k}\right)X^n,
\end{aligned}$$

erhalten wir direkt, dass

$$\mathrm{lt}(z(n,q)) = q^n.$$

Somit erhalten wir insgesamt den

Satz 4.16 *Für die Anzahl $S_n(q)$ der halbeinfachen Matrizen in $GL_n(k)$ gilt*

$$S_n(q) = q^{n^2} + O\left(q^{n^2-1}\right).$$

Die Art des Ergebnisses unterscheidet sich nicht von den Ergebnissen der vorherigen Kapitel. Wir können aus der obigen Asymptotik, die Wahrscheinlichkeit ablesen, zufällig aus der $GL_n(k)$, eine halbeinfache Matrix ausgewählt zu haben. Die Aussage ist in diesem Fall aber wesentlich interessanter, denn unser Satz besagt, dass die Wahrscheinlichkeit, zufällig eine halbeinfache invertierbare Matrix auszuwählen, für $q \to \infty$ gegen 1 geht. Anders ausgedrückt: Für sehr große q sind *fast alle* invertierbaren Matrizen halbeinfach. Da $\mathrm{lt}(GL_n(k))=\mathrm{lt}(Mat_n(k))$ gilt insbesondere, dass sogar *fast alle* Matrizen halbeinfach und invertierbar sind.

Bemerkung In einer analogen Form gilt obige Aussage insbesondere auch für $k = \mathbb{R}, \mathbb{C}$ und $k = \bar{\mathbb{F}}_q$. Die Aussage lautet in diesen Fällen:

Die Menge der halbeinfachen (invertierbaren) k-Matrizen liegt dicht in $Mat_n(k)$ ($GL_n(k)$) bezüglich der Zariskitopologie.

Für exakte Werte von $s_n(q)$ und dem Vergleich von $S_n(q)$ mit $\mathrm{lt}(S_n(q))$ sei auf die Tabellen A.6, A.7 und A.8 verwiesen.

Zusammenfassung und Ausblick

Wir haben nun alle interessanten, arithmetischen Größen bestimmt, die im Zusammenhang mit der Konjugation in $GL_n(\mathbb{F}_q)$ stehen. Der erste Schritt war die Parametrisierung der Konjugationsklassen durch gewisse Partitionsfunktionen. Diese Parametrisierung ermöglichte die Bearbeitung der Probleme mit Hilfe erzeugender Funktionen. Ausgangslage unserer Asymptotiken war dabei immer jeweils die Formel der Bauart:

$$\begin{aligned}\text{untersuchte Größe} = {} & \text{Summe von Konjugationsklassengrößen} \\ & \text{über dazugehörige Partitionsfunktionen.}\end{aligned}$$

Nachdem man gezeigt hat, dass diese Formel ein Polynom in q liefert, muss man nur noch den Leitterm dieses Polynoms herleiten.

Kapitel 3 nimmt eine Sonderstellung ein; hier wurden andere Argumente verwendet. Die Bestimmung der Konjugationsklassengröße, wurde auf die Bestimmung der Größen besonderer Automorphismengruppen reduziert, welche genügend Struktur aufwiesen, um die Berechnung mit elementaren Mitteln durchzuführen.

Die vorliegende Arbeit lässt sich auf mehrere Weisen ergänzen. Zum einen könnte man die Problemstellung ein wenig modifizieren, indem man z.B nicht alle diagonalisierbaren Matrizen aus $GL_n(k)$ abzählt, sondern nur diejenigen mit einem vorgegebenen Eigenwert $a \in k$. Das Vorgehen bei der Bearbeitung dieser einfachen Modifikationen ist aber genau dasselbe, weswegen sie nach Bearbeitung der drei wichtigsten Fälle (diagonalisierbar, jordannormalisierbar, halbeinfach) nicht mehr beachtet wurden.

Eine andere natürliche Fortsetzung wäre die analoge Untersuchung der klassischen Untergruppen ($SL_n(k), O(n), SO(n), U(n)$, etc.) von $GL_n(k)$. Da $SL_n(k)$ ein Normalteiler von $GL_n(k)$ ist, hat man hier noch etwas Angriffsfläche, aber die anderen Untergruppen erfordern gänzlich neue Methoden. Zu Ergebnissen über $SL_n(k), PSL_n(k)$ und ähnlichen Gruppen sei auf [Mac81] verwiesen.

Tabellen

In diesem Abschnitt werden nun einige Werte explizit berechnet und die bewiesenen Asymptotiken auf die Probe gestellt. Die Tabellen zu den Matrizenanzahlen zeigen, dass die Asymptotik schon für kleine q brauchbare Abschätzungen liefert. Die exakten Formeln für $D_2(q)$, $J_2(q)$, $S_2(q)$ kann man problemlos mit ein wenig Spielerei mit Matrizen herausfinden. Für die Formeln im Fall $n = 3$ ist das nicht mehr so einfach, weshalb ich mir diese Arbeit gespart habe und hier nur auf [Geb96, S.91] verweisen möchte. Es folgt die Auflistung aller verwendeten, exakten Formeln:

$$\begin{aligned}
D_2(q) &= \frac{1}{2}q^4 - q^3 - \frac{1}{2}q^2 + 2q - 1,\\
J_2(q) &= \frac{1}{2}q^4 - \frac{3}{2}q^2 + q,\\
S_2(q) &= q^4 - 2q^3 + 2q - 1,\\
D_3(q) &= \frac{1}{6}q^9 - \frac{2}{3}q^8 + \frac{7}{6}q^7 - \frac{7}{6}q^6 + \frac{2}{3}q^5 - \frac{7}{6}q^4 + q^3 + q - 1,\\
J_3(q) &= \frac{1}{6}q^9 + \frac{1}{3}q^8 + \frac{1}{6}q^7 - \frac{19}{6}q^6 + \frac{5}{3}q^5 + \frac{5}{6}q^4 + 2q^3 - 2q^2,\\
S_3(q) &= q^9 - 2q^8 + 2q^6 - q^4 - 2q^3 + 2q^2 + q - 1.
\end{aligned}$$

Konjugationsklassen

q	$c(2,q)$	$c(3,q)$	$c(4,q)$	$c(5,q)$	$c(6,q)$
2	3	6	14	27	60
3	8	24	78	232	720
4	15	60	252	1005	4080
5	24	120	620	3096	15600
7	48	336	2394	16752	117600
9	80	720	6552	58960	531360
11	120	1320	14630	160920	1771440
13	168	2184	28548	371112	4826640

Tabelle A.1: Einige exakte Werte von $c_n(q)$

Diagonalisierbare und Jordan-normalisierbare Matrizen

q	$d_2(q)$	$d_3(q)$	$d_4(q)$	$d_5(q)$	$d_6(q)$
2	1	1	1	1	1
3	3	4	5	6	7
4	6	10	15	21	28
5	10	20	35	56	84
7	21	56	126	252	462
9	36	120	330	792	1716
11	55	220	715	2002	5005
13	78	364	1365	4368	12376

Tabelle A.2: Einige exakte Werte von $d_n(q)$

q	$j_2(q)$	$j_3(q)$	$j_4(q)$	$j_5(q)$	$j_6(q)$
2	2	3	5	6	10
3	5	10	20	32	58
4	9	22	51	99	194
5	14	40	105	236	498
7	27	98	315	882	2141
9	44	192	726	2400	6632
11	65	330	1430	5412	16840
13	90	520	2535	10764	37322

Tabelle A.3: Einige exakte Werte von $j_n(q)$

q	$D_2(q)$	$J_2(q)$	$\frac{1}{2}q^4$
2	1	4	8
3	14	30	$40,5$
5	184	280	$312,5$
7	846	1134	$1200,5$
11	5950	7150	$7320,5$
13	12024	14040	$14280,5$
17	36736	41344	$41760,5$
113	80074624	81504640	$81523680,5$

Tabelle A.4: Vergleich von $D_2(q), J_2(q)$ mit ihrem Leitterm

q	$D_3(q)$	$J_3(q)$	$\frac{1}{6}q^9$
2	1	64	$85,3$
3	704	4032	$3280,5$
5	139504	425200	$325520,83$
7	3714696	8442504	$6725601,17$
11	270845200	462365200	$392991281,83$
13	1291387824	2035146672	$1767416568,17$
17	15565563136	22084297984	$19764646082,83$
113	483222748834465024	509567785063843072	$500673656330711378,83$

Tabelle A.5: Vergleich von $D_3(q)$, $J_3(q)$ mit ihrem Leitterm

Halbeinfache Matrizen

q	$s_2(q)$	$s_3(q)$	$s_4(q)$	$s_5(q)$	$s_6(q)$
2	2	4	8	16	32
3	6	18	54	162	486
4	12	48	192	768	3072
5	20	100	500	2500	12500
7	42	294	2058	14406	100842
9	72	648	5832	52488	472392
11	110	1210	13310	146410	1610510
13	156	2028	26364	342732	4455516

Tabelle A.6: Einige exakte Werte von $s_n(q)$

q	$S_2(q)$	q^4
2	3	16
3	32	81
5	384	625
7	1728	2401
11	12000	14641
13	24192	28561
17	73728	83521
113	160161792	163047361

Tabelle A.7: Vergleich von $S_2(q)$ mit seinem Leitterm

q	$S_3(q)$	q^9
2	105	512
3	7904	19683
5	1202304	1953125
7	29056320	40353607
11	1932756000	2357947691
13	8982658944	10604499373
17	104684544000	118587876497
113	2950877217863737344	3004041937984268273

Tabelle A.8: Vergleich von $S_3(q)$ mit seinem Leitterm

Literaturverzeichnis

[Geb96] Max Gebhardt. Operationen arithmetischer Untergruppen der GL(3) auf Bruhat-Tits-Gebäuden. Master's thesis, Universität des Saarlandes, 1996.

[Mac81] I.G. MacDonald. Numbers of conjugacy classes in some finite classical groups. *Bull. Austral. Math. Soc.*, 23:23–48, 1981.

[Mac98] I.G. Macdonald. *Symmetric Functions and Hall Polynomials*. Oxford mathematical monographs. Clarendon Press, 1998.

[Sta02] R.P. Stanley. *Enumerative Combinatorics*. Number v. 1 in Cambridge studies in advanced mathematics. Cambridge University Press, 2002.