Wahrscheinlichkeitsverteilungen von elliptischen Kurven über endlichen Primkörpern

Diplomarbeit
zur Erlangung des akademischen Grades eines Diplom-Mathematikers
der Naturwissenschaftlich-Technischen Fakultät I
der Universität des Saarlandes

Sascha Fischer

Saarbrücken
März 2007

Inhaltsverzeichnis

1 Übersicht **2**

2 Motivierung der Problemstellung **6**

3 $\mathbb{Z}_l$ - ein kompakter Ring **9**
3.1 Der projektive Limes 9
3.2 $\mathbb{Z}_l$- projektiver Limes von kompakten Ringen 11
3.3 Das Haar'sche Maß als Wahrscheinlichkeitsmaß auf den Mengen M und G 12

4 Ergebnisse **15**
4.1 Hilfssätze 15
4.2 Die Volumina der Mengen $X(\alpha, \beta)$ 18
4.3 Definition von Mengen, die von $X(\alpha, \beta)$ abhängen 20
4.4 Die Volumina $\nu(X_s(\alpha, \beta))$ 21
4.5 Die Volumina $\nu(X_r^{\lambda}(\alpha, \beta))$ 21
4.6 Die Volumina $\nu(X_{r,s}^{\lambda}(\alpha, \beta))$ 23

5 Herleitung von Tabelle 2 **26**
5.1 $\alpha = \beta = 0$ 26
5.2 $\alpha = 0 < \beta$ 28
5.3 $\alpha = \beta > 0$ 29
5.4 $0 < \alpha < \beta$ 30

6 Herleitung von Tabelle 4 **32**
6.1 $r = 0$ 32
6.2 $0 < r \leq \alpha$ 32
6.3 $0 \leq \alpha < r \leq \min(s, \beta)$ 33
6.4 $0 \leq \alpha \leq \min(\beta, s) < r \leq \max(\beta, s)$ 33
6.5 $r > \max(\beta, s)$ 34

7 Herleitung von Tabelle 3 **35**

8 Die Gleichverteilungsaussage **38**
8.1 Die Volumina der Mengen $X_{r,s}^{z}(\alpha, \beta)$ 38
8.2 Die bedingten Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ 43

A Appendix **47**
A.1 Definition eines Topologischen Raumes und einleitende Eigenschaften 47
A.2 Definition einer lokal-kompakten Gruppe 48
A.3 Die Existenz und Eindeutigkeit des Haar'schen Maßes für lokalkompakte Gruppen 49

B Mengenverzeichnis **51**

1 Übersicht

Zusammenfassung: Die vorliegende Arbeit löst für Primzahlen p und l mit $p \neq l$ das Problem der Wahrscheinlichkeitsverteilung für alle möglichen Gestalten des $l-$Torsionsanteils elliptischer Kurven $E/\mathbb{F}_p$ unter der Bedingung $p \equiv z \bmod l^r$ für $r \in \mathbb{N}$ und $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$. Die resultierenden Wahrscheinlichkeiten hängen in allen auftretenden Fällen nur von der abgeschnittenen $l-$adischen Bewertung $v_l^{(r)}(z-1)$ ab.

Die Übersicht vermittelt einen ersten Eindruck der Begrifflichkeit der vorliegenden Arbeit.
Die Motivierung der Problemstellung kennzeichnet den Bereich, aus dem die Problemstellung entstammt und nennt die Problemstellung. Der Bereich ist die Wahrscheinlichkeitstheorie elliptischer Kurven $E/\mathbb{F}_p$ und das Problem ist die Berechnung bedingter Wahrscheinlichkeiten über die Gestalt des $l-$Torsionsanteils $E(\mathbb{F}_p)[l^\infty]$ für Primzahlen $p \in \mathbb{P}$ mit $p \equiv z \bmod l^r$ für $r \in \mathbb{N}$ und $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$, welche auf vorherigen Ergebnissen aufbaut (vgl. [Ge]) und unter dem Eindruck dieser Ergebnisse leicht zu formulieren und mittels Haar'scher Maße anzugeben ist. Die Interpretation jener Haar'schen Maße als Wahrscheinlichkeiten für elliptische Kurven $E/\mathbb{F}_p$ ist durch eine bisher noch nicht bewiesene Hypothese über die Gleichverteilung der Frobeniuselemente $\mathcal{F}_l(E/\mathbb{F}_p)$ möglich.

Der Abschnitt über den kompakten Ring $\mathbb{Z}_l$ stellt den Ring der $l-$adischen Zahlen $\mathbb{Z}_l$ als kompakten Ring vor. Dieser Abschnitt (wie auch der Appendix) dient dem einzigen Zweck, Standardnotationen vorzustellen, um in späteren Abschnitten leichter damit arbeiten zu können. Im Zusammenspiel mit dem Appendix werden die normierten Haar'schen Maße für die Gruppen $\mathbb{Z}_l$, $M = Mat(2, \mathbb{Z}_l)$ und $G = GL(2, \mathbb{Z}_l)$ definiert und als Wahrscheinlichkeitsmaße auf diesen Gruppen interpretiert. Die Gruppe G ist geeignet zur Darstellung der Frobeniuselemente $\mathcal{F}_l(E/\mathbb{F}_p)$, wodurch die Berechenbarkeit von Wahrscheinlichkeiten für elliptische Kurven $E/\mathbb{F}_p$ gewährleistet wird. Die Einführung von $\mathbb{Z}_l$ über den projektiven Limes ist durch die Bücher [Ne] und [Se] motiviert. Der Appendix ist bis auf wenige Ausnahmen wortwörtlich aus dem Appendix des Buches [El] übernommen.

Der Abschnitt über die Ergebnisse enthält keine Rechnungen, sondern gibt Volumina von gewissen Konjugationsklassen $\mathcal{C}$ bzgl. des normierten Haar'schen Maßes ν auf G an. Im Abschnitt über die Gleichverteilungsaussage werden diese Volumina (besonders Tabelle 2) dann herangezogen, um zusammen mit zusätzlichen Rechnungen die gesuchten bedingten Wahrscheinlichkeiten in allen auftretenden Fällen vollständig anzugeben. Daneben wird die Parameterwahl diskutiert, wodurch gewährleistet wird, daß die auftretenden Konjugationsklassen nicht leer sind, und die (neben der Kombinatorik) wesentlichen technischen Hilfsmittel zur Berechnung aller auftretenden Volumina werden bereitgestellt (Hilfssätze zur Fortsetzung von Matrizen).
Die darauf folgenden drei Abschnitte dienen ausschließlich der Berechnung aller

im Abschnitt der Ergebnisse angegebenen Volumina (bis auf Tabelle 1). Durch die Herleitung der Tabellen 2, 3, 4 werden die wesentlichen Techniken zur Herleitung der Gleichverteilungsaussage vorgestellt, um dann im Abschnitt über die Gleichverteilungsaussage zur Lösung der Problemstellung eingesetzt zu werden.

Der Abschnitt über die Gleichverteilungsaussage interpretiert die Ergebnisse. Die Interpretation geschieht in Form der Formulierung einer Gleichverteilungsaussage mittels der Volumina des normierten Haar'schen Maßes ν über G. Der Name Gleichverteilungsaussage rechtfertigt sich durch die Tatsache, daß bei allen auftretenden Wahrscheinlichkeiten für Primzahlen $p \in \mathbb{P}$ mit $v_l(p-1) = s$ und $s \in \mathbb{N}$ dieselben Formeln resultieren. Mit Hilfe der Gleichverteilungsaussage werden die bedingten Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ für α, β, $r \in \mathbb{N}$ und $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ definiert, mit Hilfe derer wir die Wahrscheinlichkeiten für alle möglichen Formen $\mathbb{Z}/l^\alpha\mathbb{Z} \times \mathbb{Z}/l^\beta\mathbb{Z}$ des $l-$Torsionsanteils einer elliptischen Kurve $E/\mathbb{F}_p$ unter der Bedingung $p \equiv z \bmod l^r$ in Abhängigkeit von der abgeschnittenen $l-$adischen Bewertung von $(z-1)$ angeben werden. Beispiele mit Zahlenwerten, die das Verhalten der Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ in den Fällen $(\alpha = \beta)$ und $(\alpha < \beta)$ veranschaulichen, beschließen die Arbeit.

Danksagung: Mein Dank gilt meinem Betreuer Professor Doktor Ernst-Ulrich Gekeler für die Bereitschaft, die Arbeit während ihres Entstehungsprozesses zu besprechen und an vielen Stellen zu verbessern.

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, die vorliegende Arbeit selbst geschrieben und keine Hilfsmittel außer den angegebenen verwendet zu haben.

Sarbrücken, den

Standardnotationen

- $\mathbb{N}$ Menge der natürlichen Zahlen einschließlich der Null
- $\mathbb{Z}$ Menge der ganzen Zahlen
- $\mathbb{P}$ Menge aller Primzahlen
- $\mathbb{N}_n$ Menge der natürlichen Zahlen von 0 bis einschließlich $(n-1)$
- $\mathbb{F}_p$ Primkörper mit p Elementen für $p \in \mathbb{P}$
- $\mathbb{Z}_l$ Ring der $l-$adischen ganzen Zahlen für $l \in \mathbb{P}$
- $\mathbb{Z}_l^*$ Einheitengruppe von $\mathbb{Z}_l$
- $M = Mat(2, \mathbb{Z}_l)$ additive Gruppe der $2 \times 2-$Matrizen über $\mathbb{Z}_l$
- $G = GL(2, \mathbb{Z}_l)$ multiplikative Gruppe aller invertierbaren $2 \times 2-$Matrizen über $\mathbb{Z}_l$
- $M_n = Mat(2, \mathbb{Z}_l/l^n\mathbb{Z}_l)$ für ein $n \in \mathbb{N}$
- $G_n = GL(2, \mathbb{Z}_l/l^n\mathbb{Z}_l)$ für ein $n \in \mathbb{N}$
- $|X|$ die Anzahl der Restklassen (Mächtigkeit) einer Menge $X \subset M_n$ (bzw. $X \subset G_n$)
- v_l die $l-$adische Bewertung auf dem Ring $\mathbb{Z}_l$.
- $v_l^{(r)}$ die modulo l^r abgeschnittene $l-$adische Bewertung auf dem Ring $\mathbb{Z}_l$
- μ das normierte Haar'sche Maß auf der kompakten topologischen Gruppe M
- ν das normierte Haar'sche Maß auf der bzgl. der Relativtopologie kompakten topologischen Gruppe G
- $det(\delta)$ die Determinante einer Matrix $\delta \in M$
- $tr(\delta)$ die Spur einer Matrix $\delta \in M$
- $\hat{\mathbb{Z}}$ die proendliche Komplettierung von $\mathbb{Z}$
- $E/\mathbb{F}_p$ eine elliptische Kurve über $\mathbb{F}_p$ für $p \in \mathbb{P}$
- $\mathcal{F} = \{\mathbb{F}_p-$Isomorphieklassen von elliptischen Kurven $E/\mathbb{F}_p\}$,
- $E(\mathbb{F}_p)$ die Menge der rationalen Punkte von $E/\mathbb{F}_p$
- $E(\mathbb{F}_p)[l^\infty]$ der $l-$Torsionsanteil $(l \in \mathbb{P})$ einer elliptischen Kurve $E/\mathbb{F}_p$

2 Motivierung der Problemstellung

Problemstellung: Seien $l, p \in \mathbb{P}$ und $r, \alpha, \beta \in \mathbb{N}$ und sei $\alpha \leq \beta$. Sei $z \in \mathbb{Z}_l / l^r \mathbb{Z}_l$ gegeben. Wie wahrscheinlich ist es, daß der $l-$Torsionsanteil einer elliptischen Kurve $E/\mathbb{F}_p$ isomorph zu einer Gruppe der Form $\mathbb{Z}/l^\alpha\mathbb{Z} \times \mathbb{Z}/l^\beta\mathbb{Z}$ ist, falls wir p aus einer arithmetischen Progression $p \equiv z \bmod l^r$ gewählt haben?

Zur Beschreibung der Problemstellung der vorliegenden Arbeit bedienen wir uns der Notation und der Ergebnisse des Buches [Sil]. Hiernach ist eine elliptische Kurve über einem Körper K ein Paar (E, O), wobei E/K eine algebraische Kurve vom Geschlecht 1 und O ein ausgezeichneter $K-$rationaler Basispunkt von E ist. Wir lassen in unserer Notation den Basispunkt fort und schreiben E/K für eine elliptische Kurve über einem Körper K mit Basispunkt O. Außerdem gilt unsere Betrachtung ausschließlich elliptischen Kurven E über Primkörpern $\mathbb{F}_p$.

Sei eine elliptische Kurve $E/\mathbb{F}_p$ gegeben. Dann ist die Menge $E(\mathbb{F}_p)$ der rationalen Punkte von E eine abelsche Gruppe, für welche ein Isomorphismus der Form

$$E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

mit wohlbestimmten $m, n \in \mathbb{N}$, $m, n > 0$ und $m|n$ existiert (vgl. [Sil] Seite 145(5.6(a))). Wir definieren die Menge

$$\mathcal{F} = \{\mathbb{F}_p-\text{Isomorphieklassen von elliptischen Kurven } E/\mathbb{F}_p \mid p \in \mathbb{P}\}.$$

Sei eine algebraische Eigenschaft (A) gegeben und sei $\mathcal{A}$ die Menge aller $E/\mathbb{F}_p$, welche die Eigenschaft (A) besitzen. Wir definieren

$$P(\mathcal{F}, A) := \lim_{x \to \infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x, E/\mathbb{F}_p \in \mathcal{A}\}|}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|},$$

vorausgesetzt, daß der Limes existiert. Existiert der Limes, so definiert $P(\mathcal{F}, A)$ einen Inhalt auf der Menge $\mathcal{F}$ (vgl. [Ge] Bemerkung 4.6).

Die eingangs formulierte Problemstellung können wir nun wieder aufgreifen: Sei für $\alpha, \beta \in \mathbb{N}$ mit $\alpha \leq \beta$ und $p \in \mathbb{P}$ eine endliche abelsche $l-$Gruppe der Form

$$H = H_{\alpha,\beta}^{(l)} = \mathbb{Z}/l^\alpha\mathbb{Z} \times \mathbb{Z}/l^\beta\mathbb{Z}$$

gegeben. Sei nun $E/\mathbb{F}_p \in \mathcal{F}$ beliebig gewählt. Wie wahrscheinlich ist es dann, daß der $l-$Torsionsanteil $E(\mathbb{F}_p)[l^\infty]$ von $E(\mathbb{F}_p)$ isomorph ist zu H?

Satz(3.15) der Arbeit [Ge] zeigt, daß die Wahrscheinlichkeit $P(\mathcal{F}, E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta}^{(l)})$ immer existiert und mit dem (nicht-verschwindenden) Haar'schen Maß $\nu(X(\alpha, \beta))$ einer Teilmenge $X(\alpha, \beta)$ von $GL(2, \mathbb{Z}_l)$ übereinstimmt. Die Angabe dieser Haar'schen Maße ist durch Tabelle 1 gewährleistet. Die Wahrscheinlichkeiten dafür, daß die Bedingungen

$$E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta}^{(l)}, \quad p \equiv 1 \bmod l^s, \quad p \not\equiv 1 \bmod l^{s+1}$$

alle gleichzeitig erfüllt sind, sind durch Tabelle 2 gegeben, da auch sie nach Satz(3.15) der Arbeit [Ge] mit dem Volumen einer Teilmenge $X_s(\alpha, \beta)$ von $GL(2, \mathbb{Z}_l)$ übereinstimmen. Die Wahrscheinlichkeiten im Fall, daß die beiden Bedingungen

$$E(\mathbb{F}_p)[l^\infty] \cong H^{(l)}_{\alpha,\beta}, \quad p \equiv z \bmod l^r$$

für $z \in \mathbb{Z}_l / l^r \mathbb{Z}_l$ erfüllt sind, werden im Abschnitt über die Gleichverteilungsausage in Abhängigkeit von $v_l^{(r)}(z-1)$ angegeben.

Sei $E/\mathbb{F}_p$ gegeben zusammen mit einer Primzahl $l \in \mathbb{P}$ mit $p \neq l$. Sei $F_l = F_l(E/\mathbb{F}_p)$ das Frobeniuselement von $E/\mathbb{F}_p$ in $GL(2, \mathbb{Z}_l)$, welches bis auf Konjugation eindeutig bestimmt ist. Das charakteristische Polynom

$$\chi_{F_l}(X) = X^2 - tr(F_l)X + \det(F_l)$$

genügt den Bedingungen

$$det(F_l) = p, \quad tr(F_l) = 1 + p - |E(\mathbb{F}_p)| \tag{1}$$

(vgl. [Sil] die Seiten(133-135)). Folgender Zusammenhang besteht zwischen dem Frobeniuselement F_l und der Gruppenstruktur der rationalen Punkte $E(\mathbb{F}_p)$:

$$E(\mathbb{F}_p)[l^\infty] \cong cok(F_l - 1), \tag{2}$$

wobei cok der Kokern einer Matrix definiert wie in Definition(4.12) ist. Zum Beweis von Gleichung(2) vergleiche [Co-Le], Appendix, Proposition 2.

Für jede elliptische Kurve $E/\mathbb{F}_p \in \mathcal{F}$ definieren wir ihr totales Frobeniuselement

$$F(E/\mathbb{F}_p) = (\ldots, F_l(E/\mathbb{F}_p), \ldots) \in \prod_{l \in \mathbb{P}} GL(2, \mathbb{Z}_l)$$

welches wohldefiniert ist bis auf Konjugation. Die $l = p-$Komponente von $F(E/\mathbb{F}_p)$ fällt bei allen nun folgenden Betrachtungen nicht ins Gewicht. Wir lassen sie daher undefiniert. Es sei

$$\hat{\mathbb{Z}} = \varprojlim_{N \in \mathbb{N}} \mathbb{Z}/N = \prod_{l \in \mathbb{P}} \mathbb{Z}_l,$$

die proendliche Komplettierung von $\mathbb{Z}$. Dann ist $GL(2, \hat{\mathbb{Z}}) = \prod GL(2, \mathbb{Z}_l)$ eine kompakte Gruppe, ausgestattet mit einer kanonischen Projektion $(\bmod N)$ auf die Gruppe $GL(2, \mathbb{Z}/N)$ für alle $N \in \mathbb{N}$ (vgl. Abschnitt(3)).

Wir benutzen zur Identifikation der in dieser Arbeit berechneten Haar'schen Maße und der gesuchten Wahrscheinlichkeiten die folgende Hypothese:

(H) Die Folge $(F(E/\mathbb{F}_p))_{E/\mathbb{F}_p \in \mathcal{F}}$ ist gleichverteilt in $GL(2, \hat{\mathbb{Z}})$.

Für unsere Situation bedeutet die Hypothese konkret:

(H') Sei $N \in \mathbb{N}$ gegeben zusammen mit einer Konjugationsklasse $\mathcal{C} \subset GL(2, \mathbb{Z}/N\mathbb{Z})$. Dann existiert der Limes

$$\lim_{x \to \infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid F(E/\mathbb{F}_p)(\mathrm{mod} N) \in \mathcal{C} \wedge p \leq x\}|}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|}$$

und ist gleich dem Wert $|\mathcal{C}|/|GL(2, \mathbb{Z}/N\mathbb{Z})|$.

Obwohl bisher soweit bekannt noch niemand durch eine Niederschrift die Hypothese (H) und damit auch (H') bewiesen hat, existiert ein Konsens, sie als gültig zu erachten. Die Hypothese (H) schreibt zusammen mit Satz(3.15) der Arbeit [Ge] Volumina von gewissen Haar'schen Maßen (vgl. Tabelle 2) als Wahrscheinlichkeiten für die Gestalt des $l-$Torsionsanteils $E(\mathbb{F}_p)[l^\infty]$ einer elliptischen Kurve $E/\mathbb{F}_p$ für $p \equiv 1 \bmod l^s$, $p \not\equiv 1 \bmod l^{s+1}$, $s \in \mathbb{N}$ vor.
Im diesem Sinne werden auch wir die Hypothese (H) dazu verwenden, die berechneten Haar'schen Maße (vgl. die Gleichverteilungsaussage) als Wahrscheinlichkeiten für die Gestalt des $l-$Torsionsanteils $E(\mathbb{F}_p)[l^\infty]$ einer elliptischen Kurve $E/\mathbb{F}_p$ unter der Bedingung $p \equiv z \bmod l^r$ in Abhängigkeit von der abgeschnittenen $l-$adischen Bewertung $v_l^{(r)}(z-1)$ für $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$, $r \in \mathbb{N}$ zu interpretieren.

3 $\mathbb{Z}_l$ - ein kompakter Ring

Das im folgenden vorzustellende Objekt, der Ring $\mathbb{Z}_l$ der $l-$adischen ganzen Zahlen, ist wohlbekannt. Die Einführung von $\mathbb{Z}_l$ dient der Hervorhebung der Kompaktheit von $\mathbb{Z}_l$ als topologischer Ring. Im Anhang finden sich zum Nachlesen Definitionen und einleitende Eigenschaften von topologischen Gruppen. Die Einführung von $\mathbb{Z}_l$ über den projektiven Limes zusammen mit den Aussagen über lokal-kompakte topologische Gruppen aus dem Anhang führen auf den Begriff des Haar'schen Maßes, welches sich auf den Restklassengruppen $\mathbb{Z}_l/l^n\mathbb{Z}_l$ für ein $n \in \mathbb{N}$ mit $n > 0$ als Zählmaß herausstellt.

3.1 Der projektive Limes

Definition 3.1 *Sei I eine geordnete Indexmenge. I heißt gerichtet geordnet, falls zu jedem Paar $(i, j) \in I \times I$ ein $k \in I$ existiert mit der Eigenschaft $k \geq i$ und $k \geq j$.*

Die folgenden Definitionen eines projektiven Systems sowie auch die des projektiven Limes eines projektiven Systems lassen sich für eine Vielzahl von Objekten definieren. Beispielsweise für topologische Gruppen, Ringe oder Moduln. Wir formulieren sie für topologische Räume explizit und denken sie uns für topologische Gruppen, Ringe, Moduln in gleicher Weise definiert.

Definition 3.2 *Sei I eine gerichtet geordnete Menge. Ein projektives System über I ist eine Familie von topologischen Räumen X_i, $i \in I$, zusammen mit einer für alle $i \leq j$, $i, j \in I$, definierten stetigen Abbildung f_{ij}, so daß für alle $i \leq j$ gilt:*

$$f_{ij} : X_j \to X_i, \quad f_{ik} = \begin{cases} id_{X_i}, & i = k \\ f_{ij} \circ f_{jk}, & i \leq j \leq k. \end{cases}$$

Definition 3.3 *Sei eine gerichtet geordnete Indexmenge I zusammen mit einem projektiven System $\{X_i, f_{ij}\}$, i, $j \in I$, gegeben. Dann ist der projektive Limes des projektiven Systems $\{X_i, f_{ij}\}$ definiert als die Teilmenge*

$$X_{pr} = \varprojlim_{i \in I} X_i = \{(x_i)_{i \in I} \in \prod_{i \in I} X_i \mid f_{ij}(x_j) = x_i \; \forall \; i \leq j\}$$

des cartesischen Produktes $X = \prod_{i \in I} X_i$ versehen mit der Produkttopologie.

Motivation für die Definition des projektiven Limes ist der Wunsch, den Durchschnitt von Mengen zu verallgemeinern. Dazu folgendes motivierende

Beispiel 3.4 *Sei I eine beliebige Indexmenge. Sei $\mathfrak{X} = \{X_i\}_{i \in I}$ eine Familie von Teilmengen eines topologischen Raumes X mit der Eigenschaft für i, $j \in I$*

$$X_i \in \mathfrak{X} \quad \wedge \quad X_j \in \mathfrak{X} \Longrightarrow X_i \cap X_j \in \mathfrak{X}.$$

Dann ist der Durchschnitt

$$\varprojlim_{i \in I} X_i = \bigcap_{i \in I} X_i$$

ein projektiver Limes der Familie $\{X_i\}_{i \in I}$ *im Sinn von Definition(3.3).*

Bemerkung 3.5 (Universelle Eigenschaft) *Sei eine gerichtet geordnete Indexmenge* I *zusammen mit einem projektiven System* $\{X_i, f_{ij} \mid i, j \in I\}$ *gegeben, und sei*

$$X_{pr} = \varprojlim_{i \in I} X_i$$

der projektive Limes des Systems. Sei T *ein topologischer Raum und sei für alle* $i \in I$ *eine Abbildung* $t_i : T \to X_i$ *gegeben, so daß für alle* $j \geq i$ *die Identität* $f_{ij} \circ t_j = t_i$ *gilt. Unter diesen Voraussetzungen existiert genau eine Abbildung* $t : T \to X_{pr}$*, so daß mit den kanonischen Projektionen*

$$p_i : X_{pr} \to X_i, \quad p_i((x_j)_{j \in I}) = x_i$$

für alle $i \in I$ *gilt:*

$$p_i \circ t = t_i.$$

Beweis: Sei $x \in T$ gegeben und setze $x_i = t_i(x)$ für alle $i \in I$. Das Produkt

$$\prod_{i \in I} t_i(x) = (x_i)_{i \in I}$$

ist nach Konstruktion ein Element des cartesischen Produktes der X_i. Mit der Bedingung $f_{ij} \circ t_j = t_i$ für alle $j \geq i$ folgt, daß $(x_i)_{i \in I}$ eine wohlbestimmtes Element von X_{pr} ist. Wir definieren daher für alle $x \in T$ die Abbildung $t(x) = \prod_{i \in I} t_i(x)$. Das Bild von t ist eine Teilmenge von X_{pr}. Die Abbildung t ist eindeutig bestimmt, da alle t_i für $i \in I$ eindeutig bestimmt sind. Außerdem gilt für alle $x \in T$ und alle $i \in I$:

$$p_i(t(x)) = x_i = t_i(x).$$

□

Bemerkung 3.6 *Sei* $\mathfrak{X} = (I, X_i, f_{ij})$ *wie oben, und für alle* X_i *gelte das Hausdorff'sche Trennungsaxiom. Dann sind die Mengen der Form* $X_{ij} = \{(x_k)_{k \in I} \in \prod_{k \in I} X_k \mid f_{ij}(x_j) = x_i\}$ *abgeschlossene Teilmengen des cartesischen Produktes* $X = \prod_{i \in I} X_i$ *(versehen mit der Produkttopologie) und nach Definition gilt:*

$$X_{pr} = \bigcap_{i \leq j} X_{ij}.$$

Insbesondere ist X_{pr} *ein abgeschlossener Unterraum von* X*.*

Beweis: Es reicht zu zeigen, daß die Mengen X_{ij} abgeschlossen in X sind. In dem Hausdorff-Raum X sind Einpunktmengen $\{x\}$ mit $x \in X$ abgeschlossene Mengen. Mit der Stetigkeit der kanonischen Projektionen und der Abbildungen f_{ij} folgt dann die Behauptung. □

Satz 3.7 *Der projektive Limes*

$$X_{pr} = \varprojlim_{i \in I} X_i$$

nicht-leerer, kompakter topologischer Räume X_i ist nicht leer und kompakt.

Beweis: Wenn alle X_i kompakt sind, so ist auch das Produkt $X = \prod_{i \in I} X_i$ kompakt nach dem Satz von Tychonoff, und damit die abgeschlossene Teilmenge X_{pr}. Aber $X_{pr} = \bigcap_{i \leq j} X_{ij}$ ist auch nicht leer, wenn die X_i in X nicht leer sind, denn da X kompakt ist, wäre sonst schon der Durchschnitt endlich vieler X_{ij} leer. Dies kann aber nicht sein, denn da alle dabei beteiligten Indizes i, j (endlich viele) sicher kleiner einem groß genug gewählten $n \in I$ sind, so liegt für ein solches n und $x_n \in X_n$ das Element $(x_i)_{i \in I}$ in dem Durchschnitt der endlich vielen X_{ij}, wenn wir $x_i = f_{in}(x_n)$ wählen, falls $i \leq n$ gilt, und sonst beliebig. □

3.2 $\mathbb{Z}_l$- projektiver Limes von kompakten Ringen

Wir arbeiten im folgenden unter der Voraussetzung, daß die Definitionen aus dem Abschnitt(3.1) für topologische Gruppen, Ringe und Moduln formuliert sind. Seien $m, n \in \mathbb{N}$ mit der Eigenschaft $n \geq 1$ und $m \leq n$. Sei $A_n = \mathbb{Z}/l^n\mathbb{Z}$ der Restklassenring modulo l^n von $\mathbb{Z}$. Dann ist die Abbildung

$$\phi_{m,n} : A_n \longrightarrow A_m, \quad \phi_{m,n}(x) = x \bmod l^m$$

ein surjektiver Homomorphismus mit Kern $l^m A_n$. Die Abbildung $\phi_{m,n}$ ist für alle $n \geq m$ stetig bzgl. der diskreten Topologie auf A_n und A_m. Das Paar $\{A_n, \phi_{m,n}\}$ bildet ein projektives System. Das gibt Anlaß zur folgenden

Definition 3.8 *Der Ring der $l-$adischen ganzen Zahlen $\mathbb{Z}_l$ ist der projektive Limes*

$$\mathbb{Z}_l = \varprojlim_{n \in \mathbb{N} \setminus \{0\}} A_n.$$

Mit dem Satz von Tychonoff folgt

Proposition 3.9 *$\mathbb{Z}_l$ ist ein kompakter topologischer Ring.*

Für die Mengen A_n versehen mit der diskreten Topologie gilt das Hausdorff'sche Trennungsaxiom, also auch für $\mathbb{Z}_l$. Durch Einsichtnahme in den Anhang und die dortigen Begriffsbildungen wissen wir: Auf der kompakten topologischen Gruppe $(\mathbb{Z}_l, +)$ (bzw. auf der bzgl. der Relativtopologie kompakten topologischen Gruppe $(\mathbb{Z}_l^*, \cdot)$) existiert ein lokal-endliches nichttriviales invariantes Maß. Ein solches Maß bezeichnen wir als Haar'sches Maß und wir halten fest:

Satz 3.10 (*a*) *Auf* $(\mathbb{Z}_l, +)$ *existiert ein normiertes Haar'sches Maß* μ_1 *so, daß* $\mu_1(\mathbb{Z}_l) = 1$ *gilt.*
(*b*) *Auf der Gruppe* $(\mathbb{Z}_l^*, \cdot)$ *existiert ein normiertes Haar'sches Maß* ν_1 *so, daß* $\nu_1(\mathbb{Z}_l^*) = 1$ *gilt.*

Zum Beweis vgl. die Sätze(A.30,A.31).

Bemerkung 3.11 *Für die Maße* μ_1 *und* ν_1 *aus Satz(3.10) gelten:*
(0) *Einpunktmengen und damit abzählbare Teilmengen von* $(\mathbb{Z}_l, +)$ *haben das Volumen* 0.
(1) *Seien* $k \in \mathbb{Z}_l$, $n \in \mathbb{N}$ *gegeben. Die Restklasse* $k + l^n\mathbb{Z}_l \subset \mathbb{Z}_l$ *hat bzgl. des Haar'schen Maßes* μ_1 *das Volumen*

$$\mu_1(k + l^n\mathbb{Z}_l) = \mu_1(l^n\mathbb{Z}_l) = l^{-n}.$$

(2) *Seien* $k \in \mathbb{Z}$, $n \in \mathbb{N}$ *gegeben. Es gelte* $k \not\equiv 0 \bmod l$. *Die Restklasse* $k + l^n\mathbb{Z}_l \subset \mathbb{Z}_l$ *hat bzgl. des Haar'schen Maßes* ν_1 *für festes* n *das Volumen*

$$\nu_1(k + l^n\mathbb{Z}_l) = \nu_1(l^n\mathbb{Z}_l) = \frac{l}{l-1} \cdot l^{-n}.$$

Beweis: Teil(0): Wäre das Volumen einer Einpunktmenge echt größer als Null, so wäre $\mu_1(\mathbb{Z}_l) = \infty$ im Widerspruch zu Satz(A.31). Die $\sigma-$Additivität als eine definierende Eigenschaft des Maßes μ_1 impliziert, daß jede abzählbare Teilmenge B von $\mathbb{Z}_l$ das Volumen $\mu_1(B) = 0$ hat.
Teil(1) und (2): Die Zählmaße auf den Gruppen $(\mathbb{Z}_l/l^n\mathbb{Z}_l, +)$ und $(\mathbb{Z}_l^*/l^n\mathbb{Z}_l, \cdot)$, welche die Anzahl der Restklassen modulo l^n zählen, sind Haar'sche Maße. Daher folgt die Behauptung aus Satz(A.31) und der Forderung der Normiertheit an μ_1 und ν_1 aus Satz(3.10). □

3.3 Das Haar'sche Maß als Wahrscheinlichkeitsmaß auf den Mengen M und G

Wir vereinbaren für diesen und alle folgenden Abschnitte - sofern nicht anders verlautbart - für eine Matrix $\gamma \in M$ und ihre Einträge a, b, c, d die folgende Notation, wobei die Koeffizienten $a_i, \ldots, d_i$ für alle $i \geq 0$ nur Werte aus der Menge $\mathbb{N}_l$ annehmen.

$$a = \sum_{i\geq 0} a_i l^i,\ b = \sum_{i\geq 0} b_i l^i,\ c = \sum_{i\geq 0} c_i l^i,\ d = \sum_{i\geq 0} d_i l^i,\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M.$$

Mit (Stufe k) bezeichnen wir das Tupel (a_k, b_k, c_k, d_k). Die Einträge des Tupels a_k, b_k, c_k, d_k heißen die Koeffizienten der Stufe k. Für die Grundbegriffe der Wahrscheinlichkeitstheorie Ereignis, Unabhängigkeit, Wahrscheinlichkeitsraum, Meßbarkeit vgl. im Appendix die Definitionen(A.23,A.24,A.25).

Definition 3.12 *Wir definieren die Menge* M_n *als die Mengen aller* $2\times 2-$*Matrizen über* $\mathbb{Z}_l$ *modulo* l^n *für alle* $n \in \mathbb{N}$ *mit* $n \geq 1$.

$$M_n = \{\lambda \bmod l^n \mid \lambda \in M\} = Mat(2, \mathbb{Z}_l/l^n\mathbb{Z}_l).$$

Wir definieren die Menge G_n als die Menge aller invertierbaren $2\times 2-$Matrizen über $\mathbb{Z}_l$ modulo l^n für alle $n \in \mathbb{N}$ mit der Eigenschaft $n \geq 1$.

$$G_n = \{\gamma \in M_n \mid \det\gamma \not\equiv 0 \bmod l\} = GL(2, \mathbb{Z}_l/l^n\mathbb{Z}_l).$$

Induktiv sind Zählmaße für die Anzahl der Restklassen auf den Mengen M_n und G_n definiert. Diese definieren aufgrund ihrer lokalen Endlichkeit und Translationsinvarianz Haar'sche Maße auf den Mengen M_n und G_n. Die Anzahl der Restklassen der Mengen M_n ersehen wir aus der folgenden

Bemerkung 3.13 *Sei $\gamma \in M$ gegeben. Für ein festes $k \in \mathbb{N}$ gibt es l^4 Möglichkeiten, die Koeffizienten der Stufe k zu wählen. Für die Mächtigkeit der Menge M_n gilt:*

$$|M_n| = l^{4n}, \quad n \in \mathbb{N}.$$

Die Anzahl der Restklassen der Gruppe G_n ist aus folgendem Lemma ersichtlich:

Lemma 3.14 *$|G_{n+1}| = |G_1| \cdot l^{4n}$, wobei $|G_1| = l(l-1)(l^2-1)$ für ein $n \in \mathbb{N}$.*

Beweis: Die Eigenschaft der Invertierbarkeit einer Matrix $\gamma \in M_{n+1}$ ist genau dann gegeben, wenn $det(\gamma)$ eine Einheit in $\mathbb{Z}_l$ ist, was mit der von uns vereinbarten Notation äquivalent zu der Bedingung $a_0d_0 - b_0c_0 \neq 0$ ist, die wir an die Koeffizienten einer Matrix $\gamma \in G_{n+1}$ auf der Stufe 0 stellen. Der Wahlmöglichkeiten für b_0, d_0 unter der Voraussetzung $b_0 \neq 0 \vee d_0 \neq 0$ sind (l^2-1) viele. Sei o.B.d.A. $b_0 \neq 0$. Dann ist a_0 frei wählbar. Gleichzeitig gibt es für c_0 noch $(l-1)$ Wahlen, so daß $a_0d_0 - b_0c_0 \neq 0$ erfüllt ist. Wir erhalten für die möglichen Wahlen der Koeffizienten auf der Stufe 0 in allen Fällen den Wert $|G_1| = l(l^2-1)(l-1)$. Da dies die einzigen Einschränkungen sind, denen die Einträge einer Matrix $\gamma \in M_{n+1}$ bei Invertierbarkeit unterworfen sind, folgt mit Bemerkung(3.13):

$$|G_{n+1}| = |\{\gamma \in M_{n+1} \mid det(\gamma) \not\equiv 0 \bmod l\}| = |G_1| \cdot l^{4n}.$$

□

Bemerkung 3.15 *(a) Auf der Gruppe $M = Mat(2, \mathbb{Z}_l)$ der $2\times 2-$Matrizen über dem Ring $\mathbb{Z}_l$ existiert ein Haar'sches Maß μ mit der Eigenschaft $\mu(M) = 1$. (b) Auf der Gruppe $G = GL(2, \mathbb{Z}_l)$ der invertierbaren $2\times 2-$Matrizen über dem Ring $\mathbb{Z}_l$ existiert ein Haar'sches Maß ν mit der Eigenschaft $\nu(G) = 1$.*

Beweis: $(\mathbb{Z}_l, +)$ ist eine kompakte topologische Gruppe. Mit Induktion folgt, daß auch M eine kompakte topologische Gruppe ist. Dann ist $G \subset M$ bzgl. der Relativtopologie kompakt. Die Teile (a) und (b) folgen dann wegen der Kompaktheit von M bzw. G aus den Sätzen(A.30,A.31). □

Bemerkung 3.16 *Wir fassen die normierten Haar'schen Maße μ und ν auf den kompakten topologischen Gruppen M und G als Wahrscheinlichkeitsmaße auf den Gruppen M und G auf. Bis auf Normierung ist ν die Einschränkung von μ auf G. Es gilt die Gleichung*

$$\mu(G) = \frac{l(l-1)(l^2-1)}{l^4}.$$

Beweis: Wegen Satz(A.31) können wir die Maße μ und ν so definieren, daß

$$\mu(M) = 1, \quad \nu(G) = 1$$

gilt. Dann sind μ und ν Wahrscheinlichkeitsmaße auf M bzw. G. Des weiteren gilt für eine Matrix $\gamma \in M$:

$$\begin{aligned} \gamma \in G \Leftrightarrow det(\gamma) \in \mathbb{Z}_l^* &\Leftrightarrow det(\gamma) \text{ ist eine Einheit modulo } l \\ &\Leftrightarrow \gamma \bmod l \text{ ist invertierbar} \\ &\Leftrightarrow \gamma \bmod l \in G_1 \end{aligned}$$

Deshalb ist

$$\mu(G) = \frac{|G_1|}{|M_1|} = \frac{l(l-1)(l^2-1)}{l^4}.$$

□

Ähnlich wie im eindimensionalen Fall haben wir für Restklassen modulo l^n die folgende

Bemerkung 3.17 *Sei $n \in \mathbb{N}$. Sei $\lambda \in G_n$ und*

$$X_n^\lambda = \{\gamma \in G \mid \gamma \equiv \lambda \bmod l^n\}$$

gegeben. Dann gilt im Fall $(n > 0)$:

$$\nu(X_n^\lambda) = \frac{1}{|G_n|}.$$

Im Fall $(n = 0)$ ist die Bedingung aus der Definition der Mengen X_n^λ leer und es gilt $X_0^\lambda = G$ und daher $\nu(X_0^\lambda) = 1$.

Beweis: Der Fall $(n = 0)$ ist klar. Im Fall $(n > 0)$ kommt jeder Restklasse bzgl. des Wahrscheinlichkeitsmaßes ν in G dasselbe Volumen zu. Da es in G modulo l^n für $(n > 0)$ genau $|G_n|$ viele Restklassen gibt, folgt die Behauptung. □

Zur Erinnerung die

Definition 3.18 (Bedingte Wahrscheinlichkeit) *Seien zwei Ereignisse A und $B \subset M$ gegeben. Wir definieren die bedingte Wahrscheinlichkeit $\mu(A \mid B)$ des Ereignisses A unter der Bedingung, daß das Ereignis B eingetreten ist, als den Quotienten*

$$\mu(A \mid B) = \frac{\mu(A \cap B)}{\mu(B)}.$$

Eine Zusammenführung der Definition der bedingten Wahrscheinlichkeit und der Bemerkung(3.16) führt zu folgendem

Korollar 3.19 *Sei eine meßbare Teilmenge $S \subset G$ gegeben. Dann gilt:*

$$\mu(S) = \nu(S) \cdot \frac{l(l-1)(l^2-1)}{l^4}.$$

Bemerkung 3.20 *Der Begriff der Meßbarkeit von Mengen in M oder G ist in der vorliegenden Arbeit kein kritischer Begriff: Die zu berechnenden Volumina sind als Quotienten von Mächtigkeiten endlicher Mengen - nämlich von Teilmengen von M_n - darstellbar.*

4 Ergebnisse

4.1 Hilfssätze

Definition 4.1 *Sei $a \in \mathbb{Z}_l$ eine $l-$adische Zahl. Sei a durch eine $l-$adische Entwicklung der Form*

$$a = \sum_{i \geq 0} a_i \cdot l^i \tag{1}$$

mit Koeffizienten $0 \leq a_i < l$ für alle Indizes $i \in \mathbb{N}$ gegeben. Die $l-$adische Bewertung v_l von $a \neq 0$ ist derjenige Index m in der $l-$adischen Entwicklung von a, für den $a_m \neq 0$ und zugleich $a_j = 0$ für alle $j < m$, $j \in \mathbb{N}$ ist. In Zeichen:

$$v_l : \mathbb{Z}_l \to \mathbb{N}, \quad v_l(a) = m \quad \Longleftrightarrow \quad a_m \neq 0 \quad \wedge \quad a_j = 0 \quad \forall \quad 0 \leq j < m.$$

Wir definieren zudem $v_l(0) = \infty$. Sei $r \in \mathbb{N}$. Wir definieren für eine $l-$adische Zahl a mit der durch Gleichung(1) gegebenen $l-$adischen Entwicklung die bei r abgeschnittene $l-$adische Bewertung $v_l^{(r)}(a)$ als

$$v_l^{(r)} : \mathbb{Z}_l \to \mathbb{N}, \quad v_l^{(r)}(a) = \begin{cases} v_l(a), & v_l(a) < r \\ r, & v_l(a) \geq r \end{cases} .$$

Bemerkung 4.2 *Seien α, $\beta \in \mathbb{N}$ gegeben und angeordnet durch die Ungleichung $0 \leq \alpha \leq \beta$. Sei $n \in \mathbb{N}$ mit der Eigenschaft $n > \beta$ zusammen mit einer Matrix $\delta \in M_n$ gegeben. Für die Matrix $\delta \in M_n$ sei die Bedingung $\delta \equiv 0 \bmod l^\alpha$ erfüllt. Dann ist $v_l^{(\alpha+\beta+1)}(det(\delta)) \in \mathbb{N}$ wohldefiniert. Insbesondere können wir im Fall $n > \beta$, $\delta \equiv 0 \bmod l^\alpha$ prüfen, ob*

$$v_l^{(\alpha+\beta+1)}(\det(\delta)) = \alpha + \beta$$

ist. Die Bedingungen $v_l(\det(\delta)) = \alpha + \beta$ und

$$v_l^{(\beta-\alpha+1)}(l^{-2\alpha} det(\delta)) = v_l^{(\beta-\alpha+1)}(\det(l^{-\alpha}\delta)) = \beta - \alpha$$

sind unter den Voraussetzungen $(n > \beta)$ und $\delta \equiv 0 \bmod l^\alpha$ äquivalent.

Die folgenden Lemmata verwenden gemischte Notation: Wir fassen die Einträge a, b, c, d einer Matrix $\delta \in M_n$ sowohl als Restklassen modulo l^n als auch als Elemente des Ringes $\mathbb{Z}/l^n\mathbb{Z}$ auf.

Lemma 4.3 *Seien n, $\alpha \in \mathbb{N}$ mit der Eigenschaft $(n > \alpha \geq 0)$ gegeben. Sei durch $\delta \in M_n$ eine Matrix mit Einträgen a, b, c, d unter den Bedingungen*

$$\delta \equiv 0 \bmod l^\alpha, \delta \not\equiv 0 \bmod l^{\alpha+1}, l^{-2\alpha} det(\delta) \equiv 0 \bmod l^{n-\alpha}$$

gegeben. Dann gibt es genau l^3 Matrizen $\overline{\delta} \in M_{n+1}$ mit

$$\overline{\delta} \equiv \delta \bmod l^n \text{ und } l^{-2\alpha} det(\overline{\delta}) \equiv 0 \bmod l^{n-\alpha+1}.$$

Beweis: Zur Vereinfachung der Notation sei ($\alpha = 0$) gewählt. Der allgemeine Fall ($\alpha \geq 0$) folgt mit Induktion über α. Seien a, b, c, d die Einträge der Matrix $\delta \in M_n$. Seien $\overline{a} = a + a_n \cdot l^n$, $\overline{b} = b + b_n \cdot l^n$, $\overline{c} = c + c_n \cdot l^n$, $\overline{d} = d + d_n \cdot l^n$ die Einträge der Matrix $\overline{\delta} \in M_{n+1}$, so gewählt, daß die Kongruenzbedingung $\overline{\delta} \equiv \delta \bmod l^n$ erfüllt ist. Ist ($\alpha = 0$) der Fall, so gilt die Bedingung $\delta \not\equiv 0 \bmod l$. Einer der Koeffizienten a_0 , b_0, c_0, d_0 der Stufe 0 ist ungleich Null. Sei o.B.d.A. $a_0 \neq 0$. Dann können wir die Kongruenzbedingung

$$\overline{a}\overline{d} - \overline{b}\overline{c} \equiv (a + a_n \cdot l^n)(d + d_n \cdot l^n) - (b + b_n \cdot l^n)(c + c_n \cdot l^n)$$

$$\equiv ad - bc + (a_n \cdot d_0 + d_n \cdot a_0 - b_n \cdot c_0 - c_n \cdot b_0)l^n \bmod l^{n+1}$$

als definierende Bedingung für d_n lesen, um der Bedingung $\overline{a}\overline{d} - \overline{b}\overline{c} \equiv 0 \bmod l^{n+1}$ gerecht zu werden. Die übrigen Koeffizienten der Stufe n sind dann beliebig wählbar. In jedem Fall ergeben sich so l^3 Wahlmöglichkeiten für die Koeffizienten der Stufe n. □

Lemma 4.4 *Seien $k \in \mathbb{N}_l$, $n \in \mathbb{N}$, $n > 0$ und sei $\delta \in M_n$ mit den Einträgen a, b, c, d und unter der Bedingung $det(\delta) + tr(\delta) \equiv 0 \bmod l^n$ gegeben. Dann gibt es genau l^3 Matrizen $\overline{\delta} \in M_{n+1}$ mit $\overline{\delta} \equiv \delta \bmod l^n$ und $det(\overline{\delta}) + tr(\overline{\delta}) \equiv k \cdot l^n \bmod l^{n+1}$.*

Beweis: Seien $\overline{a} = a + a_n \cdot l^n$, $\overline{b} = b + b_n \cdot l^n$, $\overline{c} = c + c_n \cdot l^n$, $\overline{d} = d + d_n \cdot l^n$ die Einträge der Matrix $\overline{\delta} \in M_{n+1}$ so gewählt, daß die Kongruenzbedingung $\overline{\delta} \equiv \delta \bmod l^n$ erfüllt ist. Wir schreiben die zu erfüllende Kongruenzbedingung auf.

$$\overline{a}\overline{d} - \overline{b}\overline{c} + \overline{a} + \overline{d} \equiv k \cdot l^n \bmod l^{n+1}$$

$$\Leftrightarrow$$

$$ad - bc + a + d + (a_n d_0 + a_0 d_n - c_0 b_n - c_n b_0)l^n + (a_n + d_n)l^n \equiv k \cdot l^n \bmod l^{n+1}. \quad (2)$$

Wir unterscheiden die Fälle ($d_0 = a_0 = l - 1$) und ($d_0 \neq l - 1 \vee a_0 \neq l - 1$). Sei der Fall ($d_0 = a_0 = l - 1$) gegeben. Dann folgt aus der Bedingung $a_0 d_0 - b_0 c_0 + a_0 + d_0 \equiv 0 \bmod l$ sofort $b_0 c_0 \equiv -1 \bmod l$. Wir können daher die Bedingung(2) als definierende Bedingung für einen der Koeffizienten b_n oder c_n lesen. Die verbleibenden drei Koeffizienten der Stufe n sind dann frei wählbar. Im Fall ($d_0 = a_0 = l - 1$) sind so stets l^3 Möglichkeiten zur Bestimmung der Koeffizienten der Stufe n gegeben.
Im Fall ($d_0 \neq l-1 \vee a_0 \neq l-1$) können wir die Bedingung(2) immer zumindest entweder als definierende Bedingung für a_n oder d_n lesen. Die verbleibenden drei Koeffizienten der Stufe n sind dann immer frei wählbar. Im Fall ($d_0 \neq l-1 \vee a_0 \neq l-1$) sind stets l^3 Möglichkeiten zur Bestimmung der Koeffizienten der Stufe n gegeben. Die Fallunterscheidung ist vollständig und die Behauptung bewiesen. □

Korollar 4.5 *Seien r, $n \in \mathbb{N}$, $r > n > 0$, $z = \sum_{i=0}^{r-n-1} k_i \cdot l^i$, $k_i \in \mathbb{N}_l$ für alle $0 \leq i \leq (r - n - 1)$ und sei $\delta \in M_n$ mit $det(\delta) + tr(\delta) \equiv 0 \bmod l^n$. Dann gibt es genau $l^{3(r-n)}$ Matrizen $\overline{\delta} \in M_r$ mit $\overline{\delta} \equiv \delta \bmod l^n$ und $det(\overline{\delta}) + tr(\overline{\delta}) \equiv z \cdot l^n \bmod l^r$.*

Lemma 4.6 *Seien α, $n \in \mathbb{N}$ mit der Ungleichung $(0 \leq \alpha < n)$ sowie $k \in \mathbb{N}_l$ gegeben. Sei $\delta \in M_n$ mit Einträgen a, b, c, d unter den Bedingungen*

$$\delta \equiv 0 \bmod l^\alpha, \delta \not\equiv 0 \bmod l^{\alpha+1}, l^{-2\alpha} \det(\delta) \equiv l^{-\alpha} tr(\delta) \equiv 0 \bmod l^{n-\alpha}$$

gegeben. Dann gibt es genau l^2 Matrizen $\overline{\delta} \in M_{n+1}$ mit $\overline{\delta} \equiv \delta \bmod l^n$ und

$$l^{-2\alpha} det(\overline{\delta}) \equiv 0 \bmod l^{n-\alpha+1} \text{ und } l^{-\alpha} tr(\overline{\delta}) \equiv k \bmod l^{n-\alpha+1}.$$

Beweis: Sei $(\alpha = 0)$ zur Vereinfachung der Notation. Der allgemeine Fall $(\alpha \geq 0)$ folgt durch Induktion über α. Seien $\overline{a} = a + a_n \cdot l^n$, $\overline{b} = b + b_n \cdot l^n$, $\overline{c} = c + c_n \cdot l^n$, $\overline{d} = d + d_n \cdot l^n$ die Einträge der Matrix $\overline{\delta} \in M_{n+1}$, so daß die Bedingung $\overline{\delta} \equiv \delta \bmod l^n$ erfüllt ist. Die Bedingung $tr(\overline{\delta}) \equiv a + a_n \cdot l^n + d + d_n \cdot l^n \equiv k \cdot l^n \bmod l^{n+1}$ lesen wir als eine definierende Bedingung für genau einen der Koeffizienten a_n bzw. d_n der Stufe n, nachdem wir entsprechend der Argumentation im Beweis zu Lemma(4.3) genau einen Koeffizienten der Stufe n durch die Bedingung $det(\overline{\delta}) \equiv 0 \bmod l^{n+1}$ festgelegt haben. Durch diese Vorgehensweise sind in jedem Fall genau zwei der vier Koeffizienten der Stufe n eindeutig bestimmt, und für die verbleibenden zwei Koeffizienten bleiben in allen Fällen l^2 Möglichkeiten, sie zu bestimmen. □

Korollar 4.7 *Seien α, $n \in \mathbb{N}$ mit der Ungleichung $0 \leq \alpha < n$ gegeben. Sei $r \in \mathbb{N}$, $(r > n > 0)$ und $z = \sum_{i=0}^{r-n-1} k_i \cdot l^i$, $k_i \in \mathbb{N}_l$ für alle $(0 \leq i \leq (r-n-1))$ gegeben. Sei $\delta \in M_n$ mit Einträgen a, b, c, d und unter den Bedingungen*

$$\delta \equiv 0 \bmod l^\alpha,\ \delta \not\equiv 0 \bmod l^{\alpha+1},\ l^{-2\alpha} \det(\delta) \equiv l^{-\alpha} tr(\delta) \equiv 0 \bmod l^{n-\alpha}$$

gegeben. Dann gibt es genau $l^{2(r-n)}$ Matrizen $\overline{\delta} \in M_r$ mit $\overline{\delta} \equiv \delta \bmod l^n$ und

$$l^{-2\alpha} det(\overline{\delta}) \equiv 0 \bmod l^{r-\alpha}, \quad l^{-\alpha} tr(\overline{\delta}) \equiv z \cdot l^{n-\alpha} \bmod l^{r-\alpha}.$$

Definition 4.8 *Seien zwei Matrizen $\delta \in M_n$ und $\overline{\delta} \in M_{n+1}$ gegeben unter der Bedingung $\delta \equiv \overline{\delta} \bmod l^n$. Dann heißt die Matrix $\overline{\delta}$ eine Fortsetzung der Matrix δ auf die Stufe n.*

Korollar 4.9 *(a) Sei $\delta \in M_n$ gegeben wie in Lemma(4.3). Dann existieren l^3 Fortsetzungen $\overline{\delta} \in M_{n+1}$ der Matrix δ auf die Stufe n unter der Bedingung $l^{-2\alpha} \det(\overline{\delta}) \equiv 0 \bmod l^{n-\alpha+1}$.*
(b) Sei $\delta \in M_n$ gegeben wie in Lemma(4.4). Dann existieren l^3 Fortsetzungen $\overline{\delta} \in M_{n+1}$ der Matrix δ auf die Stufe n unter der Bedingung $\det(\overline{\delta}) + tr(\overline{\delta}) \equiv 0 \bmod l^{n+1}$.
(c) Sei $\delta \in M_n$ gegeben wie in Lemma(4.6). Dann existieren l^2 Fortsetzungen $\overline{\delta} \in M_{n+1}$ der Matrix δ auf die Stufe n unter den Bedingungen $\overline{\delta} \equiv \delta \bmod l^n$ und $l^{-2\alpha} det(\overline{\delta}) \equiv l^{-\alpha} tr(\overline{\delta}) \equiv 0 \bmod l^{n-\alpha+1}$.

Lemma 4.10 *Seien $k_0 \in \mathbb{N}_{l-1}$ und $\gamma \in G_1$, $\delta \in M_1$ gegeben mit $\gamma - 1 = \delta$ und δ mit den Einträgen a_0, b_0, c_0, d_0 unter der Bedingung*

$$a_0 d_0 - b_0 c_0 + a_0 + d_0 \equiv k_0 \bmod l.$$

Dann gibt es l^3 *Fortsetzungen* $\overline{\delta} = \begin{pmatrix} a_0 + a_1 \cdot l & b_0 + b_1 \cdot l \\ c_0 + c_1 \cdot l & d_0 + d_1 \cdot l \end{pmatrix} \in M_2$, *so daß für ein fest gewähltes* $k_1 \in \mathbb{N}_l$ *gilt:*

$$a_0 d_1 + a_1 d_0 - b_1 c_0 - b_0 c_1 + a_1 + d_1 \equiv k_1 \bmod l. \tag{3}$$

Beweis: Wir unterscheiden die beiden Fälle ($a_0 = l - 1 = d_0$) und ($a_0 \neq l - 1 \vee d_0 \neq l - 1$). Im ersten Fall sind sowohl c_0 als auch b_0 ungleich Null wegen $\gamma = \delta + 1 \in G_1$. Deshalb können wir Bedingung(3) als definierende Bedingung entweder für b_1 oder c_1 lesen. Im zweiten Fall ist mindestens entweder $a_0 + 1 \not\equiv 0 \bmod l$ oder $d_0 + 1 \not\equiv 0 \bmod l$ und wir lesen Bedingung(3) als definierende Bedingung für a_1 oder d_1. In allen Fällen wird so genau eine Variable der Stufe(1) der Matrix $\overline{\delta}$ auf einen Wert festgelegt und die übrigen 3 Variablen der Stufe(1) der Matrix $\overline{\delta}$ sind in jedem Fall frei wählbar. □

Korollar 4.11 *Sei* $z = \sum_{i=0}^{n} k_i \cdot l^i$, $k_i \in \mathbb{N}_l$ *für alle* $(1 \leq i \leq n)$, $k_0 \in \mathbb{N}_{l-1}$ *gegeben. Seien* $\gamma \in G_1$, $\delta \in M_1$ *gegeben mit* $\gamma - 1 = \delta$ *und* δ *mit den Einträgen* a_0, b_0, c_0, d_0 *unter der Bedingung*

$$det(\gamma) - 1 \equiv a_0 d_0 - b_0 c_0 + a_0 + d_0 \equiv k_0 \bmod l.$$

Dann gibt es l^{3n} *Fortsetzungen* $\overline{\delta} \in M_{n+1}$ *von* δ, *so daß gilt:*

$$det(\overline{\delta}) + tr(\overline{\delta}) \equiv z \bmod l^{n+1}.$$

4.2 Die Volumina der Mengen $X(\alpha, \beta)$

Seien $\alpha, \beta \in \mathbb{N}$ gegeben. Die Gruppe

$$\mathbb{Z}_l/l^\alpha\mathbb{Z}_l \times \mathbb{Z}_l/l^\beta\mathbb{Z}_l \cong \mathbb{Z}/l^\alpha\mathbb{Z} \times \mathbb{Z}/l^\beta\mathbb{Z}$$

hängt nur von der Wahl von α und β ab. Wir verwenden im folgenden die Bezeichnung $H_{\alpha,\beta}$ für Gruppen der Form $\mathbb{Z}_l/l^\alpha\mathbb{Z}_l \times \mathbb{Z}_l/l^\beta\mathbb{Z}_l$. Ist eine Gruppe der Form $H_{\alpha,\beta}$ gegeben, so setzen wir im folgenden stets $\alpha \leq \beta$ voraus.

Definition 4.12 *Sei* $\omega : \mathbb{Z}_l \times \mathbb{Z}_l \to \mathbb{Z}_l \times \mathbb{Z}_l$ *eine* $\mathbb{Z}_l-$*lineare Abbildung. Für jedes* ω *ist das Bild* $\omega(\mathbb{Z}_l \times \mathbb{Z}_l)$ *ein* $\mathbb{Z}_l-$*Untermodul von* $\mathbb{Z}_l \times \mathbb{Z}_l$. *Der Restklassenmodul*

$$(\mathbb{Z}_l \times \mathbb{Z}_l)/\omega(\mathbb{Z}_l \times \mathbb{Z}_l)$$

heißt der Kokern $cok(\omega)$ *von* ω.

Proposition 4.13 *Sei* $\gamma \in G$ *eine Matrix und sei eine abelsche Gruppe der Form* $H_{\alpha,\beta}$ *mit* $\alpha \leq \beta$ *und* α, $\beta \in \mathbb{N}$ *gegeben. Dann gilt folgende Äquivalenz:*

$$cok(\gamma - 1) \cong H_{\alpha,\beta} \Leftrightarrow \begin{cases} (\gamma - 1) \equiv 0 \bmod l^\alpha & \wedge \\ (\gamma - 1) \not\equiv 0 \bmod l^{\alpha+1} & \wedge \\ v_l(\det(\gamma - 1)) = \alpha + \beta. \end{cases}$$

Mit der Definition der $l-$*adischen Bewertung* v_l *schreiben wir etwas ausführlicher*

$$cok(\gamma - 1) \cong H_{\alpha,\beta} \Leftrightarrow \begin{cases} (\gamma - 1) \equiv 0 \bmod l^\alpha & \wedge \\ (\gamma - 1) \not\equiv 0 \bmod l^{\alpha+1} & \wedge \\ (\det(\gamma - 1)) \equiv 0 \bmod l^{\alpha+\beta} & \wedge \\ (det(\gamma - 1)) \not\equiv 0 \bmod l^{\alpha+\beta+1}. \end{cases}$$

Beweis: Seien zwei Matrizen $\gamma \in G$ und $\delta \in M$ mit $\gamma - 1 = \delta$ gegeben. Nach dem Elementarteilersatz können wir die Matrix δ (und damit auch γ) durch Zeilen- und Spaltenumformungen[1] auf Diagonalgestalt bringen. Sei o.B.d.A. δ in Elementarteilergestalt gegeben. Erfüllt nun $\delta \in M$ die Bedingungen aus Proposition(4.13), so ist der kleinste Exponent des $l-$Anteils des oberen Diagonaleinträges der Matrix $\delta = \gamma - 1$ durch die Bedingungen

$$(\gamma - 1) \equiv 0 \bmod l^{\alpha} \quad \wedge \quad (\gamma - 1) \not\equiv 0 \bmod l^{\alpha+1} \tag{4}$$

eindeutig zu α bestimmt. Der kleinste Exponent des $l-$Anteils des unteren Diagonaleintrages der Matrix δ wird durch die Bedingung $v_l(\det(\gamma - 1)) = \alpha + \beta$ als β festgesetzt, so daß die Bedingung $cok(\delta) \cong H_{\alpha,\beta}$ erfüllt ist. Umgekehrt erfüllt nun jede Matrix $\gamma \in G$ in Elementarteilergestalt mit den Diagonaleinträgen

$$a = 1 + a_{\alpha} \cdot l^{\alpha} + a_{\alpha+1} \cdot l^{\alpha+1} + \ldots \qquad | \ (a_{\alpha} \neq 0)$$

und

$$d = 1 + d_{\beta} \cdot l^{\beta} + d_{\beta+1} \cdot l^{\beta+1} + \ldots \qquad | \ (d_{\beta} \neq 0)$$

die Bedingung $cok(\gamma - 1) \cong H_{\alpha,\beta}$. □

Die Äquivalenzbedingungen aus Proposition(4.13) hängen für $\gamma \in G$ und $n \in \mathbb{N}$ mit $n \geq \beta + 1$ nur von $\gamma \bmod l^n$ ab. Wir definieren

Definition 4.14 *Seien $\alpha, \beta \in \mathbb{N}$ gegeben und sei $\alpha \leq \beta$. Sei $X(\alpha, \beta)$ die Menge aller Matrizen $\gamma \in G$, für die $cok(\gamma - 1) \cong H_{\alpha,\beta}$ gilt. Wir schreiben*

$$X(\alpha, \beta) = \{\gamma \in G \mid cok(\gamma - 1) \cong H_{\alpha,\beta}\}.$$

Sei $n \in \mathbb{N}$ und $n > \beta$ gegeben. Die Gültigkeit von $cok(\gamma - 1) \equiv H_{\alpha,\beta}$ hängt wegen Proposition(4.13) nur von $\gamma \bmod l^{\beta+1}$ ab. Wir definieren deshalb für $n \geq \beta + 1$ die Mengen

$$X^{(n)}(\alpha, \beta) = \left\{ \gamma \in G_n \;\middle|\; \begin{array}{ll} (\gamma - 1) \equiv 0 \bmod l^{\alpha} & \wedge \\ (\gamma - 1) \not\equiv 0 \bmod l^{\alpha+1} & \wedge \\ v_l^{(\beta-\alpha+1)}(l^{-2\alpha} det(\gamma - 1)) = \beta - \alpha & \end{array} \right\}$$

$X^{(n)}(\alpha, \beta)$ heißt für feste Werte von n, α, $\beta \in \mathbb{N}$ mit $\alpha \leq \beta$, $n > \beta$ die von der Menge $X(\alpha, \beta)$ abgeleitete Menge modulo l^n.

Wir verwenden im folgenden die Begriffe Wahrscheinlichkeit und Volumen als zueinander äquivalent.

Bemerkung 4.15 *Seien n, α, $\beta \in \mathbb{N}$ gegeben mit der Eigenschaft $\alpha \leq \beta$ und sei $n > \beta$. Die Wahrscheinlichkeiten $\mu(X(\alpha, \beta))$ und $\nu(X(\alpha, \beta))$ sind wohldefiniert durch die Gleichungen*

$$\mu(X(\alpha, \beta)) = \lim_{n \to \infty} \frac{|X^{(n)}(\alpha, \beta)|}{|M_n|} = \frac{|X^{(n)}(\alpha, \beta)|}{|M_n|}, \tag{5}$$

[1] Multiplikation von links und rechts mit invertierbaren Matrizen, welche nicht notwendigerweise zueinander konjugiert sind.

$$\nu(X(\alpha,\beta)) = \lim_{n\to\infty} \frac{|X^{(n)}(\alpha,\beta)|}{|G_n|} = \frac{|X^{(n)}(\alpha,\beta)|}{|G_n|}, \tag{6}$$

wobei jeweils rechts ein festes n mit der Eigenschaft $n > \beta$ gewählt sei.

Mittels Korollar(3.19) können wir immer ein durch α und β gegebenes Volumen $\nu(X(\alpha,\beta))$ in ein Volumen der Form $\mu(X(\alpha,\beta))$ umrechnen. Wir beschränken uns im folgenden darauf, alle Wahrscheinlichkeiten ausschließlich bzgl. ν anzugeben.

Satz 4.16 *Die Volumina der Mengen $X(\alpha,\beta)$ bzgl. des Haar'schen Maßes ν sind in der folgenden Tabelle zusammengetragen.*

	$\alpha=\beta=0$	$0=\alpha<\beta$	$0<\alpha=\beta$	$0<\alpha<\beta,$
$\nu(X(\alpha,\beta))$	$\frac{l^3-2l^2-l+3}{(l-1)^2(l+1)}$	$\frac{l^2-l-1}{l(l-1)}\cdot l^{-\beta}$	$l^{-4\alpha}$	$\frac{l+1}{l}\cdot l^{-3\alpha-\beta}$

Tabelle 1: $\nu(X(\alpha,\beta))$

Beweis: Die Herleitung dieser Tabelle ist in Abschnitt 2 der Arbeit [Ge] durchgeführt.

4.3 Definition von Mengen, die von $X(\alpha,\beta)$ abhängen

Definition 4.17 *Wir definieren für n, α, β, r, $s \in \mathbb{N}$ mit $\alpha \le \beta$ und $n > \max(\beta, r, s)$ die Mengen*

$$X_s(\alpha,\beta) = \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \quad \wedge \quad v_l(det(\gamma)-1) = s\}. \tag{7}$$

Wir definieren

$$X_s^{(n)}(\alpha,\beta) = \{\gamma \in G_n \mid \gamma \in X^{(n)}(\alpha,\beta) \quad \wedge \quad v_l(det(\gamma)-1) = s\}.$$

Sei $\lambda \in G_r$ gegeben. Wir definieren die Mengen

$$X_r^{\lambda}(\alpha,\beta) = \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \wedge \quad (\gamma-\lambda) \equiv 0 \bmod l^r\}. \tag{8}$$

Wir definieren

$$X_r^{\lambda,(n)}(\alpha,\beta) = \{\gamma \in G_n \mid \gamma \in X^{(n)}(\alpha,\beta) \quad \wedge \quad (\gamma-\lambda) \equiv 0 \bmod l^r\}.$$

Nehmen wir die an γ gestellten Bedingungen aus den Gleichungen(7) und (8) zusammen, so führt dies zu Mengen der Form

$$X_{r,s}^{\lambda}(\alpha,\beta) = \{\gamma \in X_s(\alpha,\beta) \mid (\gamma-\lambda) \equiv 0 \bmod l^r\}. \tag{9}$$

Wir definieren Mengen der Form

$$X_{r,s}^{\lambda,(n)}(\alpha,\beta) = \{\gamma \in X_s^{(n)}(\alpha,\beta) \mid (\gamma-\lambda) \equiv 0 \bmod l^r\}.$$

Die oben zusätzlich mit einem (n) indizierten Mengen nennen wir die von den jeweils direkt vorher definierten Mengen abgeleiteten Mengen modulo l^n.

Proposition 4.18 *Seien n, α, β, r, $s \in \mathbb{N}$ mit den Einschränkungen $\alpha \leq \beta$ und $n > \max(\beta, r, s)$ gegeben. Die Wahrscheinlichkeiten (Volumina) bzgl. des normierten Haar'schen Maßes ν der Mengen $X_s(\alpha,\beta)$, $X_r^\lambda(\alpha,\beta)$ und $X_{r,s}^\lambda(\alpha,\beta)$ sind gegeben durch die Gleichungen*

$$\nu(X_s(\alpha,\beta)) = |X_s^{(n)}(\alpha,\beta)| \cdot |G_n|^{-1},$$

$$\nu(X_r^\lambda(\alpha,\beta)) = |X_r^{\lambda,(n)}(\alpha,\beta)| \cdot |G_n|^{-1},$$

$$\nu(X_{r,s}^\lambda(\alpha,\beta)) = |X_{r,s}^{\lambda,(n)}(\alpha,\beta)| \cdot |G_n|^{-1}.$$

Beweis: Die Zahl n ist so groß gewählt, daß die Mengen $X_s(\alpha,\beta)$, $X_r^\lambda(\alpha,\beta)$ und $X_{r,s}^\lambda(\alpha,\beta)$ durch Kongruenzbedingungen modulo l^n beschrieben werden können.

4.4 Die Volumina $\nu(X_s(\alpha,\beta))$

Bemerkung 4.19 *Sei $0 < \alpha \leq \beta$ und $\gamma \in X(\alpha,\beta)$. Dann ist $\gamma \equiv 1 \bmod l^\alpha$. Deshalb ist $X_s(\alpha,\beta)$ leer für $0 \leq s < \alpha$.*

Satz 4.20 *Seien $0 \leq \alpha \leq \beta \in \mathbb{N}$ und $s \in \mathbb{N}$ mit $s \geq \alpha$ gegeben. Die Volumina $X_s(\alpha,\beta)$ sind durch folgende Tabelle gegeben:*

	$s = \alpha$	$s > \alpha$
$\alpha = \beta = 0$	$\frac{(l-2)^2}{(l-1)^2}$	$\frac{l^2-l-1}{l^2-1} \cdot l^{-s}$
$\alpha = 0 < \beta$	$\frac{l-2}{l-1} \cdot l^{-\beta}$	$\frac{l-1}{l} \cdot l^{-\beta-s}$
$\alpha = \beta > 0$	$\frac{l^2-l-1}{l^2-1} \cdot l^{-4\alpha}$	$\frac{l}{l+1} \cdot l^{-3\alpha-s}$
$0 < \alpha < \beta$	$l^{-3\alpha-\beta}$	$\frac{l-1}{l} \cdot l^{-2\alpha-\beta-s}$

Tabelle 2: vol$(X_s(\alpha,\beta))$

Beweis: Die Vollständigkeit der Tabelle folgt aus Bemerkung(4.19). Für die Herleitung der einzelnen Werte verweisen wir auf den Abschnitt der Herleitung von Tabelle 2 weiter hinten. □

4.5 Die Volumina $\nu(X_r^\lambda(\alpha,\beta))$

Bemerkung 4.21 *Seien α, $\beta \in \mathbb{N}$ gegeben mit $\alpha \leq \beta$. Sei zusätzlich $r = 0$. Dann ist die Kongruenzbedingung $\gamma \equiv \lambda \bmod l^r$ leer und deshalb gilt $X_0^\lambda(\alpha,\beta) = X(\alpha,\beta)$.*

Ob die Mengen $X_r^\lambda(\alpha,\beta)$ nicht leer sind, hängt für $(r > 0)$ sehr stark von der Wahl der Matrix $\lambda \in G_r$ ab. Das zeigt die folgende

Proposition 4.22 *Seien α, $\beta \in \mathbb{N}$ mit $0 \leq \alpha \leq \beta$ gegeben. Seien r, $n \in \mathbb{N}$ mit der Eigenschaft $n > r > 0$. Wir wollen eine Matrix $\lambda \in G_r$ so wählen, daß $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$ gilt. Wir unterscheiden die Fälle*
(a) $0 < r \leq \alpha$: Es gilt

$$X_r^\lambda(\alpha,\beta) \neq \emptyset \quad \Leftrightarrow \quad \lambda = 1 \in G_r.$$

(b) $\alpha < r \leq \beta$: Es gilt

$$X_r^\lambda(\alpha,\beta) \neq \emptyset \quad \Leftrightarrow \quad \begin{cases} (\lambda - 1) \equiv 0 \bmod l^\alpha & \wedge \\ (\lambda - 1) \not\equiv 0 \bmod l^{\alpha+1} & \wedge \\ l^{-2\alpha} \det(\lambda - 1) \equiv 0 \bmod l^{r-\alpha}. \end{cases}$$

(c) $r > \beta$: Es gilt

$$X_r^\lambda(\alpha,\beta) \neq \emptyset \quad \Leftrightarrow \quad \lambda \in X^{(r)}(\alpha,\beta).$$

In allen Fällen ist $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$ genau dann, wenn die Bedingung $X_r^\lambda(\alpha,\beta) \neq \emptyset$ erfüllt ist.

Beweis: Wir arbeiten Fall um Fall ab.
Der Fall $(0 < r \leq \alpha)$: In diesem Fall wissen wir aus Bemerkung(4.19), daß γ die Einheitsmatrix modulo l^α ist. Eine Matrix $\lambda \in G_r$ für $(0 < r \leq \alpha)$ so zu wählen, daß $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$ ist, heißt dann, sie als das Einselement in G_r zu wählen.

Der Fall $(\alpha < r \leq \beta)$: Zu zeigen ist, daß die Bedingungen, die in Proposition(4.22) auf der rechten Seite des Äquivalenzzeichens im vorliegenden Fall $(\alpha < r \leq \beta)$ angegeben sind, notwendig und hinreichend dafür sind, daß $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$ ist. Notwendig: Vergleichen wir die Bedingungen aus Proposition(4.22) in vorliegendem Fall mit der Definition der Mengen $X(\alpha,\beta)$ für den Fall $(\alpha < \beta)$, so stellen wir mit Hilfe von Bemerkung(4.2) fest, daß jede Matrix $\gamma \in X(\alpha,\beta)$ die Bedingungen, die an $\lambda \in G_r$ auf der rechten Seite des Äquivalenzzeichens in Proposition(4.22) im Fall $(\alpha < r \leq \beta)$ gestellt sind, erfüllt. Hinreichend: Mit Definition(3.18,4.17) und Proposition(4.18) genügt es, für ein $n \in \mathbb{N}$ mit der Eigenschaft $(n > \beta)$ eine einzige Matrix $\gamma \in G_n$ anzugeben, die unter der Bedingung $\gamma - \lambda \equiv 0 \bmod l^r$ ein Element von $X^{(n)}(\alpha,\beta)$ ist. Sei eine Matrix $\lambda \in G_r$ den Bedingungen von Proposition(4.22) im Fall $(\alpha < r \leq \beta)$ unterworfen und sei $\gamma \in G_n$ so gewählt, daß $\gamma - \lambda \equiv 0 \bmod l^r$ ist mit $(\alpha < r \leq \beta)$. Aus der Kongruenzbedingung $\gamma - \lambda \equiv 0 \bmod l^r$ und den an λ gestellten Bedingungen von Proposition(4.22) folgt, daß γ bis zur Stufe $(r-1)$ eindeutig bestimmt ist und auf der Stufe α einen Koeffizienten K_α ungleich Null besitzt. Wir setzen γ nun auf den Stufen r bis $(\beta - 1)$ fort, indem wir allen Koeffizienten jeder Stufe $k \in \mathbb{N}$ mit $(r \leq k \leq \beta - 1)$ den Wert Null zuordnen. Auf der Stufe β addieren wir zu dem Eintrag, der diagonal zum Eintrag mit dem Summanden $K_\alpha \cdot l^\alpha$ in γ positioniert ist, den Wert $1 \cdot l^\beta$. Die verbliebenen drei Koeffizienten der Stufe β setzen wir gleich Null. Auf den Stufen $k > \beta$ wählen wir die Koeffizienten beliebig. Die so definierte Matrix γ ist ein Element der Menge $X^{(n)}(\alpha,\beta)$. Wir können von einer Matrix $\lambda \in G_r$ unter den Bedingungen von Proposition(4.22) und von der Bedingung $\gamma - \lambda \equiv 0 \bmod l^r$ ausgehend immer eine Matrix $\gamma \in X^{(n)}(\alpha,\beta)$ angeben. Das zeigt die Behauptung.

Der Fall $r > \beta$: Im Fall $(r > \beta)$ unter den Bedingungen von Proposition(4.22) eine Matrix $\gamma \in G_n$ anzugeben, die den beiden Bedingungen $\gamma \in X^{(n)}(\alpha,\beta)$ und $\gamma - \lambda \equiv 0 \bmod l^r$ genügt, ist denkbar einfach. Wir interpretieren die Matrix $\lambda \in X^{(r)}(\alpha,\beta)$ als ein Element $\lambda' \in G_n$, indem wir λ von der Stufe r

an bis einschließlich der Stufe $n-1$ durch Null fortsetzen. Dann setzen wir $\gamma = \lambda' \in X^{(n)}(\alpha,\beta)$ und mit Definition(4.17) und Proposition(4.18) folgt, daß die Bedingung $\lambda \in X^{(r)}(\alpha,\beta)$ hinreichend dafür ist, daß $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$ ist. Notwendig ist sie sowieso, denn wäre $\lambda \notin X^{(r)}(\alpha,\beta)$, dann wäre eine der in der Definition der Mengen $X^{(r)}(\alpha,\beta)$ gestellten Bedingungen verletzt, und für ein $\gamma \in G_n$ mit $\gamma - \lambda \equiv 0 \bmod l^r$ wäre stets die Bedingung $\gamma \notin X(\alpha,\beta)$ erfüllt. Ist also $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$, so muß im Fall $(r > \beta)$ stets die Bedingung $\lambda \in X^{(r)}(\alpha,\beta)$ erfüllt sein. □

Satz 4.23 *Seien s, r, α, $\beta \in \mathbb{N}$ mit $(0 \leq \alpha \leq \beta)$. Sei weiterhin $\lambda \in G_r$ entsprechend Proposition(4.22) so gewählt, daß $\nu(X_r^\lambda(\alpha,\beta)) \neq 0$ gilt. Unter der Bedingung, eine solche Wahl für $\lambda \in G_r$ getroffen zu haben, sind die Volumina $\nu(X_r^\lambda(\alpha,\beta))$ unter der Bedingung $v_l^{(r)}(det(\lambda)-1) = s$ in den einzelnen Fällen für α und β durch folgende Tabelle gegeben.*

	$(0 = \alpha = \beta)$	$(0 < \alpha = \beta)$
$\alpha = s = r$	$\frac{l^3-2l^2-l+3}{(l^2-1)(l-1)}$	$\frac{l-1}{l} \cdot l^{-3\alpha}$
$\alpha = s < r$	$\frac{l^3}{(l^2-1)(l-2)} \cdot l^{-4r}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+\alpha}$
$\alpha < s < r$	$\frac{l^3}{(l^2-1)((l-1))} \cdot l^{-4r+s}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+s}$
$\alpha < s = r$	$\frac{l^2}{l^2-1} \cdot l^{-3r}$	$\frac{l^2}{l^2-1} \cdot l^{-3r}$

Tabelle 3 für $0 \leq \alpha = \beta$

	$(0 = \alpha < \beta)$	$(0 < \alpha < \beta)$
$\alpha = s = r < \beta$	$\frac{l^2-l-1}{l(l-1)} \cdot l^{-\beta}$	$\frac{l^2-1}{l^2} \cdot l^{-2\alpha-\beta}$
$\alpha = s < r \leq \beta$	$\frac{l^2}{(l+1)(l-2)} \cdot l^{-3r-\beta}$	$\frac{l^2}{l^2-1} \cdot l^{-3r+\alpha-\beta}$
$\alpha < s < r \leq \beta$	$\frac{l^2}{l^2-1} \cdot l^{-3r+s-\beta}$	$\frac{l^2}{l^2-1} \cdot l^{-3r+s-\beta}$
$\alpha < s = r \leq \beta$	$\frac{l}{l+1} \cdot l^{-2r-\beta}$	$\frac{l}{l+1} \cdot l^{-2r-\beta}$
$\alpha < \beta < s = r$	$\frac{l^2}{l^2-1} \cdot l^{-3r}$	$\frac{l^2}{l^2-1} \cdot l^{-3r}$
$\alpha = s < \beta < r$	$\frac{l^3}{(l^2-1)(l-2)} \cdot l^{-4r}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+\alpha}$
$\alpha < \beta < s < r$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+s}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+s}$
$\alpha < s \leq \beta < r$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+s}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r+s}$
$\alpha < \beta < s = r$	$\frac{l^2}{l^2-1} \cdot l^{-3r}$	$\frac{l^2}{l^2-1} \cdot l^{-3r}$

Tabelle 3 für $0 \leq \alpha < \beta$

Beweis: Wir verweisen auf den Abschnitt der Herleitung von Tabelle 3 weiter hinten. □

4.6 Die Volumina $\nu(X_{r,s}^\lambda(\alpha,\beta))$

Bemerkung 4.24 *Seien r und s, α, $\beta \in \mathbb{N}$ gegeben mit $\alpha \leq \beta$. Dann gilt $X_{0,s}^\lambda(\alpha,\beta) = X_s(\alpha,\beta)$ sowie $X_{r,s}^\lambda(\alpha,\beta) = \emptyset$ im Fall $s < \alpha$.*

Ob die Mengen $X_{r,s}^\lambda(\alpha,\beta)$ nicht leer sind, hängt für $(r > 0)$ sehr stark von der Wahl der Matrix $\lambda \in G_r$ ab. Das zeigt die folgende

Proposition 4.25 *Seien s, α, $\beta \in \mathbb{N}$ mit $0 \leq \alpha \leq \beta$ und $\alpha \leq s$ gegeben. Sei $r \in \mathbb{N}$ mit der Eigenschaft $(r > 0)$. Wir wollen eine Matrix $\lambda \in G_r$ so wählen, daß $\nu(X^{\lambda}_{r,s}(\alpha,\beta)) \neq 0$ gilt. Wir unterscheiden die Fälle, zu denen wir jeweils eine notwendige und hinreichende Bedingung für $X^{\lambda}_{r,s}(\alpha,\beta) \neq \emptyset$ angeben:*
(a) $(0 < r \leq \alpha)$: Notwendig und hinreichend dafür, daß $X^{\lambda}_{r,s}(\alpha,\beta) \neq \emptyset$ ist, ist die Bedingung

$$\lambda = 1 \in G_r.$$

(b) $(\alpha < r \leq \min(s,\beta))$: Hier sind die folgenden vier Bedingungen notwendig und hinreichend dafür, daß $X^{\lambda}_{r,s}(\alpha,\beta) \neq \emptyset$ ist.

$$\begin{array}{ll} (\lambda - 1) \equiv 0 \bmod l^{\alpha}, & (\lambda - 1) \not\equiv 0 \bmod l^{\alpha+1}, \\ l^{-2\alpha} \det(\lambda - 1) \equiv 0 \bmod l^{r-\alpha}, & v_l^{(r)}(\det(\lambda) - 1) = r. \end{array}$$

(c) $(\alpha \leq s < r \leq \beta)$: Hier sind die folgenden vier Bedingungen notwendig und hinreichend dafür, daß $X^{\lambda}_{r,s}(\alpha,\beta) \neq \emptyset$ ist.

$$\begin{array}{ll} (\lambda - 1) \equiv 0 \bmod l^{\alpha}, & (\lambda - 1) \not\equiv 0 \bmod l^{\alpha+1}, \\ l^{-2\alpha} \det(\lambda - 1) \equiv 0 \bmod l^{r-\alpha}, & v_l^{(r)}(\det(\lambda) - 1) = s. \end{array}$$

(d) $(\alpha \leq \beta < r \leq s)$: Hier sind die folgenden Bedingungen notwendig und hinreichend dafür, daß $X^{\lambda}_{r,s}(\alpha,\beta) \neq \emptyset$ ist.

$$\begin{array}{ll} \lambda \in X^{(r)}(\alpha,\beta), & v_l^{(r)}(\det(\lambda) - 1) = r. \end{array}$$

(e) $(r > max(\beta, s))$: Die folgende Bedingung ist notwendig und hinreichend dafür, daß $X^{\lambda}_{r,s}(\alpha,\beta) \neq \emptyset$ ist.

$$\lambda \in X_s^{(r)}(\alpha,\beta).$$

Beweis: Wir stellen in allen Fällen fest, daß die an $\lambda \in G_r$ gestellten Bedingungen genau die Bedingungen aus der Definition der Mengen $X_s^{(n)}(\alpha,\beta)$ modulo l^r sind. Daher sind sie in jedem Fall notwendig dafür, eine Matrix $\gamma \in X_s^{(n)}(\alpha,\beta)$ unter der Bedingung $\lambda - \gamma \equiv 0 \bmod l^r$ angeben zu können, so daß $\nu(X^{\lambda}_{r,s}(\alpha,\beta)) \neq 0$ ist. Andererseits läßt sich jede Matrix $\lambda \in G_r$, die in einem der Fälle den Bedingungen aus Proposition(4.25) genügt, mittels der Lemmata(4.3,4.4,4.6) zu einer Matrix $\gamma \in X_s^{(n)}(\alpha,\beta)$ fortsetzen, woraus mittels der Definitionen(3.18,4.17) und Proposition(4.18) folgt, daß $\nu(X^{\lambda}_{r,s}(\alpha,\beta)) \neq 0$ gilt.

□

Satz 4.26 *Seien r, s, α, $\beta \in \mathbb{N}$ mit $0 \leq \alpha \leq \beta$, $\alpha \leq s$, $r > 0$. Sei weiterhin $\lambda \in G_r$ entsprechend Proposition(4.25) so gewählt, daß $\nu(X^{\lambda}_{r,s}(\alpha,\beta)) \neq 0$ ist. Unter der Bedingung, eine solche Wahl für $\lambda \in G_r$ getroffen zu haben, sind die Volumina $\nu(X^{\lambda}_{r,s}(\alpha,\beta))$ durch Tabelle 4 gegeben. Gibt es keine entsprechende Wahl von λ, so ist das Volumen in allen Fällen gleich Null. Tabelle 4 enthält für festgelassene α, β, r, s die Abkürzung*

$$|\lambda| = |\{\lambda \in G_r \mid \nu(X^{\lambda}_{r,s}(\alpha,\beta) \neq 0\}|,$$

die Abkürzung

$$M_X = |X_s^{(\max(s,\beta)+1)}(\alpha,\beta)|,$$

sowie die Funktion $w = w(s,\alpha,\beta) : \mathbb{N}^3 \to \mathbb{N}$*, welche die Anzahl der* $\lambda \in G_{\alpha+1}$ *mit* $\nu(X^\lambda_{\alpha+1,s}(\alpha,\beta)) \neq 0$ *beschreibt. Für* w *gilt:*

	$\alpha = s$	$\alpha < s$
$0 = \alpha = \beta$	$(l+1)l(l-2)^2$	$l(l^2-l-1)$
$0 < \alpha = \beta$	$l(l-1)(l^2-l-1)$	$l^2(l-1)$
$0 = \alpha < \beta$	$(l+1)l(l-2)$	(l^2-1)
$0 < \alpha < \beta$	$l(l^2-1)$	(l^2-1)

Tabelle der Werte der Funktion $w = w(s,\alpha,\beta)$

Wir erhalten für die Volumina der Mengen $X^\lambda_{r,s}(\alpha,\beta)$ *bei festgehaltenen* s*,* α*,* β *und die Wahlmöglichkeiten für* λ *im jeweiligen Fall dann die folgende Tabelle:*

	$0 \leq \alpha = \beta$	$\lvert\lambda\rvert$
$0 < r \leq \alpha$	$\nu(X_s(\alpha,\beta))$	1
$\alpha < r \leq \min(s,\beta)$	$-$	0
$min(s,\beta) < r \leq \max(s,\beta)$	$\frac{l^2}{l^2-1} \cdot l^{-3r-s}$	$w \cdot (l-1)l^{3(r-1)-\beta-2\alpha}$
$r > max(s,\beta)$	$\frac{1}{\lvert G_r\rvert}$	$M_X \cdot l^{4(r-\max(s,\beta)-1)}$

Tabelle 4: $\nu(X^\lambda_{r,s}(\alpha,\beta))$

	$0 \leq \alpha < \beta$	$\lvert\lambda\rvert$
$0 < r \leq \alpha$	$\nu(X_s(\alpha,\beta))$	1
$\alpha < r \leq \min(s,\beta)$	$\frac{l}{l+1} \cdot l^{-2r-\beta-s}$	$w \cdot l^{2(r-\alpha-1)}$
$min(s,\beta) < r \leq \max(s,\beta)$	$\frac{l^2}{l^2-1} \cdot l^{-3r-\max(s,\beta)}$	$w \cdot (l-1)l^{3(r-1)-\min(s,\beta)-2\alpha}$
$r > max(s,\beta)$	$\frac{1}{\lvert G_r\rvert}$	$M_X \cdot l^{4(r-\max(s,\beta)-1)}$

Tabelle 4: $\nu(X^\lambda_{r,s}(\alpha,\beta))$

Beweis: Die Vollständigkeit der Tabelle 4 folgt aus Bemerkung(4.24). $|\lambda|$ ist in allen Fällen durch die Herleitung von Tabelle 2 gegeben. Für die Herleitung der übrigen Werte verweisen wir auf den Abschnitt der Herleitung von Tabelle 4 weiter hinten.

□

5 Herleitung von Tabelle 2

Seien s, α, $\beta \in \mathbb{N}$ im gesamten Abschnitt der Herleitung von Tabelle 2 stets unter der Voraussetzung $\alpha \leq \beta$ gegeben. Sei $n \in \mathbb{N}$ stets mit der Eigenschaft $n > \max(\beta, s)$ gegeben. Wir vereinbaren für den gesamten Abschnitt der Herleitung der Tabelle 2 für zwei Matrizen $\delta \in M_n$ und $\gamma \in M_n$ mit der Eigenschaft $\gamma = \delta + 1$, sofern nicht anders verlautbart, die Notation

$$a = \sum_{i=0}^{n-1} a_i l^i, \quad b = \sum_{i=0}^{n-1} b_i l^i, \quad c = \sum_{i=0}^{n-1} c_i l^i, \quad d = \sum_{i=0}^{n-1} d_i l^i, \quad \delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_n.$$

Wir werden in der nun folgenden Herleitung von Fall zu Fall sowohl mit den Einträgen a, b, c, d als den Einträgen der Matrix $\gamma \in G_n$ als auch als den Einträgen der Matrix $\delta = \gamma - 1 \in M_n$ arbeiten, um möglichst einfache Fallunterscheidungen zu erhalten und Notation zu sparen. Um die unterschiedlichen Darstellungen der Bedingungen aus der Definition der Mengen $X_s(\alpha, \beta)$ im jeweiligen Fall nachvollziehen zu können, haben wir die folgende

Bemerkung 5.1 *Seien γ, $\delta \in M_n$ gegeben unter der Voraussetzung $\gamma = \delta + 1$. Dann gilt:*

$$det(\gamma) = det(\delta + 1) = det(\delta) + tr(\delta) + 1.$$

5.1 $\alpha = \beta = 0$

Wir setzen in der Definition der Mengen $X_s(\alpha, \beta)$ die Variablen α und β durch die Gleichung $(\alpha = \beta = 0)$ fest. Dann lesen sich die Bedingungen der Definition der Mengen $X_s(\alpha, \beta)$ für ein $\gamma \in G_n$ als

$$\det(\gamma) \not\equiv 1 \bmod l \quad \wedge \quad \det(\gamma - 1) \not\equiv 0 \bmod l, \tag{1}$$

falls $(s = \alpha = \beta = 0)$ ist, oder

$$det(\gamma) \equiv 1 \bmod l^s \quad \wedge \quad \det(\gamma) \not\equiv 1 \bmod l^{s+1} \quad \wedge \quad \det(\gamma - 1) \not\equiv 0 \bmod l, \tag{2}$$

falls $(s > 0)$ der Fall ist.
Alle Matrizen, welche die Bedingung $det(\gamma - 1) \not\equiv 0 \bmod l$ erfüllen, zu zählen heißt, alle Matrizen aus G_1 ohne Eigenwert 1 zu zählen. Wir ermitteln das Komplement, also alle invertierbaren Matrizen aus G_1 mit Eigenwert 1, und subtrahieren dann die Mächtigkeit des Komplementes von $|G_1|$. Um diesen Schritt anzugehen, ermitteln wir jetzt zuallererst die Anzahl derjenigen Matrizen $\gamma \in M_1$, die überhaupt einen Eigenwert 1 aufweisen können. Wir wissen, daß die Spur einer Matrix γ die Summe, die Determinante das Produkt ihrer Eigenwerte ist. Ist der Eigenwert 1 ein Eigenwert von $\gamma \in M_1$, so lassen sich folgende Bedingungen für die Koeffizienten der Stufe 0 aufstellen, wenn wir den zweiten Eigenwert modulo l von $\gamma \in M_1$ mit x bezeichnen:

$$a_0 + d_0 \equiv x + 1 \bmod l \quad \textit{und} \quad a_0 d_0 - b_0 c_0 \equiv x \bmod l$$

Durch elementare Umformungen erhalten wir die folgende Bedinung

$$a_0 + d_0 - (a_0 d_0 - b_0 c_0) \equiv 1 \bmod l. \tag{3}$$

Die Fälle $(a_0 = d_0 = 1)$, $(a_0 \neq d_0 = 1)$, $(a_0 = 1 \neq d_0)$ und $(a_0 \neq 1 \neq d_0)$ unterscheidend, zählen wir nacheinander $(2l-1)$, $(l-1)(2l-1)$, $(l-1)(2l-1)$ und $(l-1)^3$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe 0, was in der Summe (l^3+l^2-l) Möglichkeiten sind. Von diesen (l^3+l^2-l) Möglichkeiten zur Bestimmung der Koeffizienten der Stufe 0 ist in genau (l^2+l) vielen Fällen die Bedingung $x \equiv 0 \bmod l$ erfüllt. Daher sind invertierbarer Matrizen mit Eigenwert 1 genau $(l^3+l^2-l)-(l^2+l) = (l^3-2l)$ viele. Die Mächtigkeit des Komplements, also die Mächtigkeit der Menge aller invertierbaren Matrizen $\gamma \in G_1$ ohne Eigenwert 1, berechnet sich dann als die Differenz

$$|G_1| - (l^3-2l) = l(l^2-1)(l-1) - (l^3-2l) = l(l^3-2l^2-l+3) = |X^{(1)}(0,0)|. \tag{4}$$

Wir berechnen das Volumen $\nu(X_0(0,0))$. Sei o.B.d.A. $n = 1$ und $\gamma \in G_1$. Dann muß zusätzlich zu der Bedingung $det(\gamma - 1) \not\equiv 0 \bmod l$ die Bedingung $v_l(\det(\gamma) - 1) = 0 \Leftrightarrow det(\gamma) \not\equiv 1 \bmod l$ erfüllt sein. Was wir direkt berechnen können, ist die Anzahl der Matrizen $\gamma \in G_1$ mit $\det(\gamma) \equiv 1 \bmod l$: Wir wissen, G_1 hat $l(l^2-1)(l-1)$ viele Elemente. Wir können von den vier zu wählenden Elementen a_0, b_0, c_0, d_0 immer das letzte zu wählende Element so wählen, daß die Bedingung $\det(\gamma) \equiv 1 \bmod l$ erfüllt ist. Dann bleiben von den $l(l^2-1)(l-1)$ Möglichkeiten in jedem Fall noch genau $l(l^2-1)$ Möglichkeiten zur Wahl der Koeffizienten auf der Stufe 0 erhalten. Eine kurzer Blick auf Gleichung(3) zeigt, daß von den $l(l^2-1)$ Möglichkeiten für $\det(\gamma) \equiv 1 \bmod l$ genau l^2 viele einen Eigenwert 1 besitzen, was bedeutet, daß es $l(l^2-l-1)$ viele Matrizen $\gamma \in G_1$ mit $det(\gamma) \equiv 1 \bmod l$ ohne Eigenwert 1 gibt. Subtrahieren wir diesen Wert von $X(0,0)$, so erhalten wir als Volumen

$$\nu(X_0(0,0)) = \frac{l(l^3-2l^2-l+3) - l(l^2-l-1)}{|G_1|} = \left(\frac{l-2}{l-1}\right)^2. \tag{5}$$

Sei $\gamma \in G_1$ mit $det(\gamma) \equiv 1 \bmod l$ und 1 kein Eigenwert von γ. Dann gibt es, wie gerade berechnet, $l(l^2-l-1)$ viele Möglichkeiten zur Bestimmung der Koeffizienten der Stufe 0 im Fall $(s > 0)$.
Für den Rest der Argumentation in Betrachtung der Stufe s zur Berechnung des Volumens $X_s(0,0)$ für $(s > 0)$ betrachten wir eine Fortsetzung der Matrix $\gamma \in G_1$ unter der Bedingung $det(\gamma) \equiv 1 \bmod l^s$ bis zur Stufe $s-1$. Dafür gibt es laut Lemma(4.4) genau $l^{3(s-1)}$ Möglichkeiten. Bezeichne $\overline{\gamma} \in G_{s+1}$ eine solche Fortsetzung. Auf der Stufe s wird die Wahl der Koeffizienten dann durch die zu $det(\overline{\gamma}) - 1 \equiv 0 \bmod l^{s+1}$ entgegengesetzte Bedingung, nämlich $det(\overline{\gamma}) - 1 \not\equiv 0 \bmod l^{s+1}$ bestimmt. Lemma(4.4) zufolge gibt es l^3 Möglichkeiten der Wahl der Koeffizienten auf der Stufe s, so daß die Bedingung $det(\overline{\gamma}) - 1 \equiv 0 \bmod l^{s+1}$ erfüllt ist. Unter der Bedingung $det(\overline{\gamma}) - 1 \not\equiv 0 \bmod l^{s+1}$ gibt es dann $(l^4 - l^3)$ Möglichkeiten der Wahl der Koeffizienten auf der Stufe s. Alle Überlegungen bezüglich des Volumens $X_s(0,0)$ für $(s > 0)$ zusammengenommen münden für $n = s+1$ in der Gleichung

$$\nu(X_s(0,0)) = \frac{l(l^2-l-1)}{|G_1|} \cdot \frac{l^{3(s-1)}(l^4-l^3)}{l^{4s}} = \frac{l^2-l-1}{l^2-1} \cdot l^{-s} \tag{6}$$

5.2 $\alpha = 0 < \beta$

Sei $n \in \mathbb{N}$ und die Bedingung $(\alpha = 0 < \beta)$ für α, $\beta \in \mathbb{N}$ erfüllt. Unter der Festsetzung von α und β durch $(\alpha = 0 < \beta)$ resultieren aus der Definition der Mengen $X_s(0, \beta)$ für ein $\gamma \in G_n$, $n > \max(\beta, s)$ die Bedingungen

$$(s = 0): \quad \gamma - 1 \not\equiv 0 \bmod l, \quad v_l(det(\gamma - 1)) = \beta, \quad und \quad v_l(det(\gamma) - 1) = 0, \tag{7}$$

$$(s > 0): \quad \gamma - 1 \not\equiv 0 \bmod l, \quad v_l(det(\gamma - 1)) = \beta, \quad und \quad v_l(det(\gamma) - 1) = s. \tag{8}$$

Wir berechnen die Volumina der Mengen $X_0(0, \beta)$. Sei $\gamma \in G_n$ gegeben. γ erfülle die Bedingungen(7). Die Bedingungen $\gamma \not\equiv 0 \bmod l$ und $\beta = v_l(det(\gamma - 1)) > 0$ zu erfüllen, bedeutet für $\gamma \in G_n$ in Worten ausgesprochen, genau einen Eigenwert 1 modulo l zu besitzen. Sei x_0 der zweite Eigenwert der Matrix $\gamma \in G_n$ modulo l. Genau einen Eigenwert 1 modulo l zu besitzen, entspricht dann der Bedingung $x_0 \not\equiv 1 \bmod l$, falls der erste Eigenwert von γ kongruent zu 1 modulo l gewählt ist. Die Invertierbarkeit der Matrix $\gamma \in G_n$ zu gewährleisten bedeutet dann, den zweiten Eigenwert der Matrix $\gamma \in G_n$ modulo l so zu wählen, daß zusätzlich die Bedingung $x_0 \not\equiv 0 \bmod l$ erfüllt ist. Insgesamt sind für den zweiten Eigenwert die Einschränkungen $x_0 \not\equiv 1 \bmod l \ \wedge \ x_0 \not\equiv 0 \bmod l$ durch die Stufe 0 der Matrix $\gamma \in G_n$ gegeben. Die Spur einer Matrix ist die Summe, die Determinante das Produkt ihrer Eigenwerte. Wir formulieren für die Stufe 0 der Matrix $\gamma \in G_n$ die Gleichungen

$$a_0 + d_0 \equiv 1 + x_0 \bmod l, \quad a_0 d_0 - b_0 c_0 \equiv x_0 \bmod l$$

entsprechend der Wahl der Eigenwerte. Elementare Umformungen führen auf die Gleichung

$$(d_0 - x_0)(1 - d_0) \equiv b_0 c_0 \bmod l. \tag{9}$$

Wir unterscheiden die Fälle $b_0 c_0 \equiv 0 \bmod l$ und $b_0 c_0 \not\equiv 0 \bmod l$. Im ersten Fall stehen $(4l - 2)$ Möglichkeiten zur Wahl des Koeffizienten d_0 und des Produktes $b_0 c_0$ offen, im zweiten Fall sind $(l - 1)(l - 2)$ Wahlen für den Koeffizienten d_0 und das Produkt $b_0 c_0$ möglich. Zusammengenommen sind das $l(l + 1)$ viele Möglichkeiten der Wahl. Vergessen wir nicht die Variable x_0, die, den Bedingungen $x_0 \not\equiv 1 \bmod l \ \wedge \ x_0 \not\equiv 0 \bmod l$ unterworfen, in jedem Fall modulo l genau $(l - 2)$ Wahlen für die Koeffizienten der Stufe 0 ermöglicht. Insgesamt sind das letztlich $l(l+1)(l-2)$ Möglichkeiten der Wahl der Koeffizienten der Stufe 0, um der Bedingung(9) zu genügen. Wenn wir noch bemerken, daß $\gamma - 1 \not\equiv 0 \bmod l$ für diese Wahlen immer erfüllt ist, so haben wir allen Bedingungen(7) aus der Definition der Mengen $X_0(0, \beta)$ Genüge geleistet.
Lemma(4.3) besagt, daß für eine Matrix $\gamma \in G_1$ unter der Bedingung $det(\gamma - 1) \equiv 0 \bmod l^\beta$ genau $l^{3(\beta-1)}$ Fortsetzungen auf die Stufe $(\beta - 1)$ existieren. Sei im folgenden die Matrix $\gamma \in G_1$ unter der Bedingung $det(\gamma - 1) \equiv 0 \bmod l^\beta$ bis auf die Stufe $\beta - 1$ fortgesetzt. Bezeichne $\overline{\gamma} \in G_{\beta+1}$ eine solche Fortsetzung. Mit einschließlich der Stufe β muß die Bedingung $det(\overline{\gamma} - 1) \not\equiv 0 \bmod l^{\beta+1}$ erfüllt sein. Die Koeffizienten der Stufe β sind daher so zu wählen, daß die Matrix $\overline{\gamma}$ unter der Bedingung $det(\overline{\gamma} - 1) \not\equiv 0 \bmod l^{\beta+1}$ auf die Stufe

β fortgesetzt wird, dafür gibt es $l^4 - l^3$ Möglichkeiten der Wahl der Koeffizienten der Stufe β. Wir führen im Fall $(n = \beta + 1)$ alle Überlegungen zu einer Gleichung zusammen:

$$\nu(X_0(0,\beta)) = \frac{(l-2)l(l+1)}{l(l^2-1)(l-1)} \cdot \frac{l^{3(\beta-1)}(l^4-l^3)}{l^{4\beta}} = \frac{l-2}{l-1} \cdot l^{-\beta}. \qquad (10)$$

Wir berechnen die Volumina $\nu(X_s(0,\beta)$ für $(s > 0)$. Die Bedingungen(8) aus der Definition der Mengen $X_s(0,\beta)$ für $(s > 0)$ führen auf die Gleichung(9). Im Gegensatz zum Fall $(s = 0)$, um der Bedingung $s = v_l(det(\gamma) - 1) > 0$ gerecht zu werden, muß für den zweiten Eigenwert x_0 der Matrix $\gamma \in G_n$ die Bedingung $x_0 \equiv 1 \bmod l$ erfüllt sein. Beide Eigenwerte der Matrix γ sind kongruent zu 1 modulo l. Aus dem Fall $\alpha = \beta = 0$ wissen wir, daß es dann l^2 viele Möglichkeiten der Wahl der Koeffizienten der Stufe 0 gibt. Unter diesen Wahlen der Koeffizienten der Stufe 0 ist auch das Einselement modulo l. Sehen wir von dem Einselement modulo l ab, so daß $\gamma - 1 \not\equiv 0 \bmod l$ immer erfüllt ist, bleiben noch $l^2 - 1$ Möglichkeiten der Wahl der Koeffizienten der Stufe 0. Nehmen wir nun alle Erkenntnisse aus den Lemmata(4.3, 4.4, 4.6) zusammen, um für ein $k \in \mathbb{N}$ für eine Matrix $\gamma \in G_k$ unter den Bedingungen $det(\gamma - 1) \equiv 0 \bmod l^k$ und $det(\gamma) - 1 \equiv 0 \bmod l^k$ Fortsetzungen zu wählen, so wissen wir: Solange $k < \min(\beta, s)$ der Fall ist, gibt es laut Lemma(4.6) l^2 Fortsetzungen der Matrix γ auf die Stufe k. Bezeichne $\gamma_1 \in G_{min(\beta,s)}$ eine Fortsetzung von $\gamma \in G_1$ auf die Stufe $(min(\beta, s)-1)$. Für eine derartige Fortsetzung gibt es $l^{2(min(s,\beta)-1)}$ Möglichkeiten. Dann gibt es entweder $l^3 - l^2$ Möglichkeiten der Fortsetzung im Fall $(s \neq \beta)$ oder im Fall $(s = \beta)$ genau $(l(l-1))^2$ Fortsetzungen γ_2 der Matrix γ_1 auf die Stufe $\min(\beta, s)$. Im Fall $s \neq \beta$ gibt es den Lemmata(4.3,4.4) zufolge auf den Stufen k mit der Eigenschaft $\min(\beta, s) \leq k < \max(\beta, s)$ immer genau l^3 Fortsetzungen einer Matrix $\overline{\gamma} \in G_k$ auf die Stufe k. Das bedeutet, daß es $l^{3(\max(s,\beta)-\min(s,\beta)-1)}$ Fortsetzungen γ_3 von γ_2 auf die Stufe $(\max(\beta, s) - 1)$ im Fall $\beta \neq s$ gibt. Im Fall $\beta \neq s$ gibt es genau $l^4 - l^3$ Fortsetzungen von γ_3 auf die Stufe $(max(\beta, s))$. Nehmen wir alle Überlegungen zusammen, so werden wir der Bedingung(8) gerecht, indem wir für $n = (max(\beta, s) + 1)$ schreiben:

$$\nu(X_s(0,\beta)) = \frac{l^2-1}{l(l^2-1)(l-1)} \cdot \frac{l^{2(\min(s,\beta)-1)}(l^3-l^2)}{l^{4\min(s,\beta)}}$$

$$\cdot \frac{l^{3(\max(s,\beta)-\min(s,\beta)-1)}(l^4-l^3)}{l^{4(\max(s,\beta)-\min(s,\beta))}} = \frac{l-1}{l} \cdot l^{-\beta-s}. \qquad (11)$$

5.3 $\alpha = \beta > 0$

Sei $\gamma \in G_n$ gegeben. Seien a, b, c, d die Einträge von $\delta = \gamma - 1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, wobei die Notation der $l-$adischen Entwicklungen der Einträge a, b, c, d der Matrix δ vom Anfang des Abschnittes der Herleitung von Tabelle 2 erhalten bleibe. Wir wollen die Volumina der Mengen $X_s(\alpha, \alpha)$ in den Fällen $(s > \alpha = \beta)$ und $(s = \alpha = \beta)$ in dieser Reihenfolge, aber doch im wesentlichen zusammen herleiten. Dazu wollen wir bemerken, daß zur Erfüllung der Kokernbedingung $cok(\gamma - 1) \cong H_{\alpha,\alpha}$ in jedem Fall $\gamma \equiv 1 \bmod l^\alpha$ gelten muß nach

Bemerkung(4.19). Die Bedingungen aus der Definition der Mengen $X_s(\alpha,\alpha)$ im Fall $(s>\alpha)$ für die Stufe α sind zusammengestellt in den Gleichungen

$$a_\alpha d_\alpha - b_\alpha c_\alpha \not\equiv 0 \bmod l \quad \wedge$$

$$(a_\alpha d_\alpha - b_\alpha c_\alpha)\cdot l^{2\alpha} + (a_\alpha + d_\alpha)\cdot l^\alpha + 1 \equiv 1 \bmod l^{\alpha+1}, \tag{12}$$

Bedingung(12) führt auf die Bedingung $a_\alpha + d_\alpha \equiv 0 \bmod l$. Eine Art, im Fall $(s>\alpha)$ die Möglichkeiten der Wahl für die Koeffizienten auf der Stufe α zu zählen, bietet die Fallunterscheidung in die beiden Fälle $(a_\alpha \equiv d_\alpha \equiv 0 \bmod l)$ und $(a_\alpha \equiv -d_\alpha \not\equiv 0 \bmod l)$. Im ersten Fall zählen wir $(l-1)^2$ Möglichkeiten zur Wahl von $b_\alpha c_\alpha$, im zweiten Fall, welcher $(l-1)$ mal auftritt, zählen wir (l^2-l+1) Möglichkeiten der Wahl von $b_\alpha c_\alpha$. Die Gesamtzahl der Möglichkeiten zur Bestimmung der Koeffizienten der Stufe α, die aus diesen beiden Fällen resultiert, ist $l^2(l-1)$.
Den Fall $(s=\alpha)$ gewinnen wir formal dadurch, daß wir in Bedingung(12) das Kongruenzzeichen durch das Zeichen der Inkongruenz ersetzen. Diese Vorgehensweise läßt darauf schließen, daß der Fall $(s=\alpha)$ durch Komplementbildung aus dem Fall $(s>\alpha)$ auf der Stufe α hergeleitet werden kann. Auf der Stufe α, wo $a_\alpha d_\alpha - b_\alpha c_\alpha \not\equiv 0 \bmod l$ gilt, bedeutet dies, daß die Möglichkeiten zur Bestimmung der Koeffizienten der Stufe $(s=\alpha)$ sich als Differenz aller Möglichkeiten zur Bestimmung der Koeffizienten der Stufe α, die der Bedingung $a_\alpha d_\alpha - b_\alpha c_\alpha \not\equiv 0 \bmod l$ genügen ($|G_1|$ viele) und derer, die zusätzlich der Bedingung(12) genügen ($l^2(l-1)$ viele), ermitteln läßt.
Wir setzen im Fall $(s>\alpha)$ die Matrix $\gamma \in G_{\alpha+1}$ unter der Bedingung $det(\gamma) - 1 \equiv 0 \bmod l^s$ mittels Lemma(4.4) auf die Stufe $(s-1)$ fort. Bezeichne $\overline{\gamma} \in G_{s+1}$ eine solche Fortsetzung. Dann gilt $det(\overline{\gamma}) - 1 \equiv 0 \bmod l^s$. Die Anzahl der Möglichkeiten einer solchen Fortsetzung (Fortsetzung bis einschließlich der Stufe $(s-1)$) ist $l^{3(s-(\alpha+1))}$. Wie in allen vorherigen Fällen $(\alpha = 0 \le \beta)$ sind unter der Voraussetzung, daß die Bedingung $det(\overline{\gamma}) - 1 \equiv 0 \bmod l^s$ gilt, auf der Stufe s durch die Bedingung $det(\overline{\gamma}) - 1 \not\equiv 0 \bmod l^{s+1}$ genau $(l^4 - l^3)$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe s von $\overline{\gamma}$ gegeben. Alle Argumente zusammenführend schreiben wir die Gleichungen der Volumina $\nu(X_s(\alpha,\alpha))$ im Fall $(\alpha>0)$ für $n=(s+1)$ als

$$(s=\alpha): \quad \nu(X_\alpha(\alpha,\alpha)) = \frac{|G_1| - l^2(l-1)}{|G_1|}\cdot l^{-4\alpha} = \frac{l^2-l-1}{l^2-1}\cdot l^{-4\alpha},$$

$$(s>\alpha): \quad \nu(X_s(\alpha,\alpha)) = \frac{l^2(l-1)}{|G_1|}\cdot\frac{l^{3(s-(\alpha+1))}(l^4-l^3)}{l^{4s}} = \frac{l}{l+1}\cdot l^{-3\alpha-s}. \tag{13}$$

5.4 $0<\alpha<\beta$

Sei δ wie im vorherigen Abschnitt(5.3) definiert. Dann erhalten wir aus der Definition der Mengen $X_s(\alpha,\beta)$ im Fall $(s=\alpha)$ die Bedingungen

$$a_\alpha d_\alpha - b_\alpha c_\alpha \equiv 0 \bmod l$$

$$(a_\alpha d_\alpha - b_\alpha c_\alpha)\cdot l^{2\alpha} + (a_\alpha + d_\alpha)\cdot l^\alpha + 1 \not\equiv 1 \bmod l^{\alpha+1}. \tag{14}$$

Wir behandeln die Fälle $(s = \alpha)$ und $(s > \alpha)$ zusammen. In jedem Fall gilt $\delta \equiv 0 \bmod l^\alpha$ mit Bemerkung(4.19). Des weiteren resultiert im Fall $(s = \alpha)$ aus der Bedingung(14) die Bedingung $a_\alpha + d_\alpha \not\equiv 0 \bmod l$. Außerdem wissen wir, daß mindestens einer der vier Koeffizienten der Stufe α ungleich Null sein muß, der Bedingung $\delta \not\equiv 0 \bmod l^{\alpha+1}$ aus der Definition der Mengen $X(\alpha, \beta)$ zufolge. Mit diesem Wissen erhalten wir in den Fällen $(a_\alpha = 0)$, $(d_\alpha = 0)$ und $(a_\alpha \neq 0 \neq d_\alpha)$ nacheinander $(l-1)(2l-1)$, $(l-1)(2l-1)$ und $(l-1)^2(l-2)$ Möglichkeiten, die Koeffizienten der Stufe α zu wählen. Zusammengenommen sind das $l(l^2-1)$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe α im Fall $(s = \alpha)$.
Ersetzen wir das Inkongruenzzeichen der Bedingung(14) durch ein Kongruenzzeichen, so sind wir im Fall $(s > \alpha)$. Wir zählen $(l^3 + l^2 - l)$ Möglichkeiten, die der Bedingung $a_\alpha d_\alpha - b_\alpha c_\alpha \equiv 0 \bmod l$ genügen. Unter Zuhilfenahme der Regeln zur Berechnung der Mächtigkeiten von komplementären Mengen finden wir so $(l^3 + l^2 - l) - (l^3 - l) = l^2$ Möglichkeiten, welche die Bedingung $a_\alpha d_\alpha - b_\alpha c_\alpha \equiv 0 \bmod l$ erfüllen und zugleich die Bedingung(14) nicht. Unter diesen ist auch die Matrix, die der Bedingung $\delta \equiv 0 \bmod l^{\alpha+1}$ genügt, welche nicht zulässig ist, da sonst ein Widerspruch zu der Bedingung $\delta \not\equiv 0 \bmod l^{\alpha+1}$ bestünde. Verbleiben also letztlich noch $l^2 - 1$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe α im Fall $(s > \alpha)$.
Mittels der Lemmata(4.3, 4.4, 4.6) bzw. mittels der sich an diese Lemmata anschließenden Korollare zählen wir die Möglichkeiten der Fortsetzung einer Matrix $\gamma \in G_{\alpha+1}$ unter den Bedingungen $l^{-2\alpha} det(\gamma - 1) \equiv 0 \bmod l$ und $l^{-\alpha}(det(\gamma) - 1) \equiv 0 \bmod l$ auf die Stufe $\max(\beta, s)$. Die dazugehörende Fallunterscheidung ist wortwörtlich durch den Fall $(\alpha = 0 < \beta)$ gegeben, nur um α viele Stufen verschoben. Wir fassen zusammen und schreiben für $n = (max(\beta, s) + 1)$

$$(s = \alpha) : \ \nu(X_\alpha(\alpha, \beta)) = \frac{l(l^2-1)}{|G_1|} \cdot \frac{l^{3(\beta-\alpha-1)}(l^4 - l^3)}{l^{4\beta}} = l^{-3\alpha-\beta},$$

$$\begin{aligned}(s > \alpha) : \ \nu(X_s(\alpha, \beta)) &= \frac{l^2-1}{|G_1|} \cdot \frac{l^{2(\min(\beta,s)-\alpha-1)}(l^3 - l^2)}{l^{4\min(\beta,s)}} \\ &\quad \cdot \frac{l^{3(\max(\beta,s)-\min(\beta,s)-1)}(l^4 - l^3)}{l^{4(\max(\beta,s)-\min(\beta,s))}} \\ &= \frac{l-1}{l} \cdot l^{-2\alpha-\beta-s}.\end{aligned}$$

□

6 Herleitung von Tabelle 4

Seien α, β, r, s und λ wie in Satz(4.26). Sei $n \in \mathbb{N}$ für den gesamten Abschnitt der Herleitung von Tabelle 4 unter der Bedingung $n > max(\beta, r, s)$ gegeben. Im Prinzip ist Tabelle 4 aus der Herleitung von Tabelle 2 bereits ersichtlich. Das wollen wir deutlich machen. Zur Abkürzung der Notation beginnen wir diesen Abschnitt mit einer

Definition 6.1 *Wir definieren die beiden Ereignisse A und B durch*

$$B = \{\gamma \in G_n \mid \gamma \in X_s^{(n)}(\alpha, \beta)\},$$

$$A = \{\gamma \in G_n \mid (\gamma - \lambda) \equiv 0 \bmod l^r\}.$$

Korollar 6.2 *Es gelten die Identitäten*

$$B = X_s^{(n)}(\alpha, \beta),$$

$$A \cap B = X_{r,s}^{\lambda,(n)}(\alpha, \beta),$$

$$\nu(X_{r,s}^{\lambda}(\alpha, \beta)) = \frac{|A \cap B|}{|B|} \cdot \nu(X_s(\alpha, \beta)). \tag{1}$$

6.1 $r = 0$

Im Fall $(r = 0)$ ist die Kongruenzbedingung $\gamma \equiv \lambda \bmod l^r$ aus der Definition der Mengen $X_{r,s}^{\lambda}(\alpha, \beta)$ gleich der leeren Bedingung. Die übrigen Bedingungen aus der Definition der Mengen $X_{r,s}^{\lambda}(\alpha, \beta)$ sind genau die Bedingungen aus der Definition der Mengen $X_s(\alpha, \beta)$. Daher gilt

$$X_{0,s}^{\lambda}(\alpha, \beta) = X_s(\alpha, \beta)$$

und deshalb $\nu(X_{0,s}^{\lambda}(\alpha, \beta)) = \nu(X_s(\alpha, \beta))$.

6.2 $0 < r \leq \alpha$

Im Fall $(0 < r \leq \alpha)$ gilt mit Proposition(4.25):

$$\nu(X_{r,s}^{\lambda}(\alpha, \beta)) \neq 0 \quad \Leftrightarrow \quad \lambda = 1 \in G_r.$$

Sei $\lambda = 1 \in G_r$, dann folgt aus der Definition der Mengen $X_{r,s}^{\lambda}(\alpha, \beta)$ die Gleichheit der Mengen $X_{r,s}^{\lambda}(\alpha, \beta)$ und $X_s(\alpha, \beta)$ und entsprechend gilt für die Volumina:

$$\nu(X_{r,s}^{\lambda}(\alpha, \beta)) = \nu(X_s(\alpha, \beta)). \tag{2}$$

6.3 $0 \leq \alpha < r \leq \min(s, \beta)$

Es ist klar, daß dieser Fall nur für $\alpha < \beta$ Sinn macht, sei λ den passenden Bedingungen aus Bemerkung(4.25) unterworfen. In diesem Fall gebe eine Tabelle Aufschluß über die Wahlmöglichkeiten auf den einzelnen Stufen von γ unter den Bedingungen $A \wedge B$ und B. Die Wahlmöglichkeiten für die Koeffizienten der einzelnen Stufen von $\gamma \in G_n$ für das Ereignis B sind durch die Herleitung von Tabelle 2 gegeben. Wir arbeiten mit den Abkürzungen $S := \min(\beta, s)$ und $T := \max(\beta, s)$ und geben nur die Stufen an, auf denen sich die Anzahl der Wahlmöglichkeiten für γ verändert. Dabei setzen wir o.B.d.A. $(S \neq T)$ und $(\alpha = 0)$ voraus, um die Darstellung zu erleichtern. Zwischen den in der Tabelle angegebenen Stufen sind der Wahlmöglichkeiten für γ auf jeder Stufe gleich viele, und zwar genau so viele, wie die diesen Zwischenraum begrenzenden Stufen angeben. Sei $\lambda \in G_r$ entsprechend Proposition(4.25) so gewählt, daß $X^{\lambda}_{r,s}(\alpha, \beta) \neq 0$ gilt. Dann wissen wir, daß $\gamma \in X^{(n)}_s(\alpha, \beta)$ durch die Bedingung A bis zur Stufe $(r-1)$ eindeutig bestimmt ist. Ab der Stufe r ist γ dann so zu wählen, wie die Bedingungen der Definition der Mengen $X^{(n)}_s(\alpha, \beta)$ vorschreiben.
Die folgende Tabelle enthält in der ersten Zeile die Angabe der relevanten Stufen der Matrix γ, in der zweiten Zeile die Wahlmöglichkeiten der Koeffizienten der jeweiligen Stufe von γ für das Ereignis $A \cap B$, die dritte Zeile enthält die aus der Herleitung von Tabelle 2 bekannten Wahlmöglichkeiten auf den jeweiligen Stufen von $\gamma \in G_n$ zur Erfüllung der Bedingung $\gamma \in X^{(n)}_s(\alpha, \beta)$.

Stufe	0	1	$(r-1)$	r	$(S-1)$	S	$(S+1)$	$(T-1)$	T
$\lvert A \cap B \rvert$	1	1	1	l^2	l^2	$l^3 - l^2$	l^3	l^3	$l^4 - l^3$
$\lvert B \rvert$	$l^2 - 1$	l^2	l^2	l^2	l^2	$l^3 - l^2$	l^3	l^3	$l^4 - l^3$

Wir berechnen mittels Gleichung(1) im Fall $(0 = \alpha < \beta)$ und $n = T + 1$

$$\nu(X^{\lambda}_{r,s}(0, \beta)) = \frac{|A \cap B|}{|B|} \cdot \nu(X_s(0, \beta)) = \frac{1}{l^2 - 1} \cdot l^{-2(r-1)} \cdot \nu(X_s(0, \beta))$$

$$= \frac{l^2}{l^2 - 1} \cdot \frac{l - 1}{l} \cdot l^{-2r-\beta-s} = \frac{l}{l+1} \cdot l^{-2r-\beta-s}.$$

Im Fall $(\alpha > 0)$ ist die Tabelle um α viele Stufen nach rechts verschoben. Auf den Stufen 0 bis einschließlich $(\alpha - 1)$ steht im Fall $\nu(X^{\lambda}_{r,s}(\alpha, \beta)) \neq 0$ sowohl in der zweiten als auch in der dritten Zeile auf jeder Stufe eine 1 aufgrund der Bedingung $\gamma - 1 \equiv 0 \bmod l^{\alpha}$ aus der Definition der Mengen $X^{(n)}(\alpha, \beta)$. Auf der Stufe $\alpha > 0$ verändert sich der Wert in der dritten Zeile im Vergleich zum Fall $(\alpha = 0)$, was durch die Multiplikation mit $\nu(X_s(\alpha, \beta))$ wieder aufgehoben wird, so daß insgesamt gilt:

$$(0 \leq \alpha < r \leq \min(s, \beta)): \quad \nu(X^{\lambda}_{r,s}(\alpha, \beta)) = \frac{l}{l+1} \cdot l^{-2r-\beta-s}. \tag{3}$$

6.4 $0 \leq \alpha \leq \min(\beta, s) < r \leq \max(\beta, s)$

Sei $\lambda \in G_r$ entsprechend den Bedingungen von Proposition(4.25) gewählt, so daß $\nu(X^{\lambda}_{r,s}(0, \beta)) \neq 0$ gilt im vorliegenden Fall. Im Fall, daß $\alpha = \beta \geq 0$ gilt, ist das Volumen wohldefiniert über die Gleichsetzung $\min(\beta, s) = \beta$, $\max(\beta, s) = s$. Wir wollen zur Vereinfachung der Darstellung $(0 = \alpha < s < r \leq \beta)$ annehmen und eine Tabelle mit Rechnung anbieten.

Stufe	0	1	$(s-1)$	s	$(s+1)$	$(r-1)$	r	$(\beta-1)$	β
$\lvert A\cap B\rvert$	1	1	1	1	1	1	l^3	l^3	l^4-l^3
$\lvert B\rvert$	l^2-1	l^2	l^2	l^3-l^2	l^3	l^3	l^3	l^3	l^4-l^3

Mittels Gleichung(1) berechnen wir die Wahrscheinlichkeit

$$\nu(X^{\lambda}_{r,s}(0,\beta)) = \frac{1}{(l^2-1)(l^3-l^2)} \cdot l^{-2(s-1)} l^{-3(r-s-1)} \cdot \nu(X_s(0,\beta))$$

$$= \frac{l^3(l-1)}{(l^2-1)(l-1)l} \cdot l^{s-3r} \cdot l^{-\beta-s} = \frac{l^2}{l^2-1} \cdot l^{-3r-\beta}.$$

Daß auch in allen anderen Fällen dieselbe Formel für die Volumina $\nu(X^{\lambda}_{r,s}(\alpha,\beta))$ resultiert, liegt in der Natur der Sache: Die Tabellen sind in allen Fällen fast identisch, was die Anzahl der Wahlmöglichkeiten für die Koeffizienten der einzelnen Stufen von γ anbelangt. Links der Stufe ($\alpha > 0$) steht jeweils eine 1 in der zweiten und dritten Zeile, so daß der Quotient aller Stufen ($k < \alpha$) aus zweiter und dritter Zeile immer 1 ist. Auf der Stufe ($\alpha \geq 0$) selbst treten in der dritten Zeile für $|B|$ Unterschiede auf, welche sich aber durch die Multiplikation mit dem Volumen $\nu(X_s(\alpha,\beta))$ jedenfalls aufheben. Auf den Stufen $k > \alpha$ können wir die Rollen von s und β tauschen, ohne daß sich die zweite und dritte Zeile verändern (beachte die Lemmata(4.3,4.4). Für ($n = max(\beta, s) + 1$) können wir daher das Ergebnis in der folgenden allgemeinen Form erfassen:

$$(0 \leq \alpha \leq \min(\beta,s) < r \leq \max(\beta,s)): \quad \nu(X^{\lambda}_{r,s}(\alpha,\beta)) = \frac{l^2}{l^2-1} \cdot l^{-3r-\max(\beta,s)}. \tag{4}$$

6.5 $r > \max(\beta, s)$

In diesem Fall ist bis einschließlich der Stufe $(r-1) \geq \beta$ genau eine Matrix als Wahlmöglichkeit für $\gamma \in X^{(n)}_s(\alpha,\beta)$ vorhanden, wenn $\lambda \in G_r$ entsprechend den Bedingungen von Proposition(4.25) so gewählt ist, daß $\nu(X^{\lambda}_{r,s}(\alpha,\beta)) \neq 0$ gilt. Das Volumen schreibt sich für ($n = r$) dann als

$$(r > \max(\beta,s)): \quad \nu(X^{\lambda}_{r,s}(\alpha,\beta)) = \frac{1}{|G_r|} = \frac{1}{|G_1|} \cdot l^{-4(r-1)}. \tag{5}$$

7 Herleitung von Tabelle 3

Die Einträge von Tabelle 3 ergeben sich aus den Einträgen von Tabelle 4. Der wesentliche Schritt ist, die Wahrscheinlichkeiten aus Tabelle 4, welche von der $l-$adischen Bewertung der Matrix $\gamma \in G$ abhängen, so umzuformen, daß sie nur noch von der abgeschnittenen $l-$adischen Bewertung von $\lambda \in G_r$ abhängen. Um die in Tabelle 4 auftretenden Wahrscheinlichkeiten unter der Bedingung $v_l^{(r)}(det(\lambda) - 1) = s$ für $\lambda \in G_r$ zu formulieren, benötigen wir eine zusätzliche Form von Mengen.

Definition 7.1 *Seien $l \in \mathbb{P}$, $\gamma \in G$ und s, $r \in \mathbb{N}$ gegeben. Wir definieren die Mengen*

$$X_s = \{\gamma \in G \mid v_l(det(\gamma) - 1) = s\}.$$

sowie

$$X_s^{(r)} = \{\gamma \in G_r \mid v_l^{(r)}(det(\gamma) - 1) = s\}.$$

Bemerkung 7.2 *Seien s, $n \in \mathbb{N}$ mit $n > s$ gegeben. Dann gilt:*

$$\nu(X_s) = \frac{|X_s^{(n)}|}{|G_n|}.$$

Beweis: n ist so groß gewählt, daß die Bedingung aus der Definition der Mengen X_s durch Kongruenzen modulo l^n beschrieben werden kann. □

Bemerkung 7.3 *Seien $s = 0$ und $r > 0$, dann gilt:*

$$\nu(X_s) = \frac{|X_s^{(r)}|}{|G_r|} = \frac{l-2}{l-1}.$$

Im Fall $(r > s > 0)$ gilt:

$$\nu(X_s) = \frac{|X_s^{(r)}|}{|G_r|} = l^{-s}.$$

Im Fall $(r > 0)$ gilt:

$$\sum_{s=r}^{\infty} \nu(X_s) = \frac{l}{l-1} \cdot l^{-r}.$$

Beweis: Im Fall $(s = 0, r > 0)$ und $\gamma \in G_r$ gibt es $(l-1)$ verschiedene Möglichkeiten für die Werte von $det(\gamma)$ modulo l, und genau $(l-2)$ davon haben die Eigenschaft

$$det(\gamma) - 1 \not\equiv 0 \bmod l \Leftrightarrow v_l^{(1)}(det(\gamma) - 1) = 0.$$

Im Fall $(s > 0)$ gilt mit Korollar(4.5) für $(r = s + 1)$:

$$|X_s^{(r)}| = l(l^2 - 1) \cdot l^{3(s-1)} \cdot l^3(l-1) = |G_1| \cdot l^{3s}.$$

Daraus folgt mit Bemerkung(7.2) die Behauptung. Im Fall $(r > 0)$ gilt:

$$\sum_{s=r}^{\infty} \nu(X_s) = \sum_{s=r}^{\infty} l^{-s} = \frac{l}{l-1} \cdot l^{-r}.$$

□

Die Umrechnung der Wahrscheinlichkeiten erfolgt in zwei Schritten für jeden Tabelleneintrag von Tabelle 4: Der erste Schritt ist die Summation über alle $s \geq r$ für diejenigen Einträge in Tabelle 4, bei denen ein Exponent s vorkommt. Der zweite Schritt ist die Division durch $\nu(X_s)$ im Fall $(s < r)$ bzw. durch $\sum_{s=r}^{\infty} \nu(X_s)$ im Fall $(s \geq r)$.

Der folgende Satz formalisiert die Herleitung von Tabelle 3 aus Tabelle 4.

Satz 7.4 *Seien $l \in \mathbb{P}$, r, s, α, $\beta \in \mathbb{N}$, $\lambda \in G_r$ mit $\alpha \leq \beta$, $\alpha \leq s$ gegeben. Sei $v_l^{(r)}(det(\lambda) - 1) = s$. Dann gilt im Fall $(s < r)$:*

$$\nu(X_r^{\lambda}(\alpha, \beta) \mid v_l^{(r)}(det(\lambda) - 1) = s) = \frac{\nu(X_{r,s}^{\lambda}(\alpha, \beta))}{\nu(X_s)},$$

und im Fall $(s = r)$:

$$\nu(X_r^{\lambda}(\alpha, \beta) \mid v_l^{(r)}(det(\lambda) - 1) = r) = \frac{\sum_{t \geq r} \nu(X_{r,t}^{\lambda}(\alpha, \beta))}{\sum_{t \geq r} \nu(X_t)}.$$

Beweis: Seien für $n > max(\beta, r, s)$ eine Matrix $\gamma \in G$ und $\lambda \in G_r$ mit $v_l^{(r)}(det(\lambda) - 1) = s$ gegeben. Seien A, B, C die drei Ereignisse

$$A = \{\gamma \in G \mid cok(\gamma - 1) \cong H_{\alpha,\beta}\}, \quad B = \{\gamma \in G \mid v_l^{(r)}(det(\gamma) - 1) = s\},$$

$$C = \{\gamma \in G \mid \gamma \equiv \lambda \bmod l^r\}.$$

Wir wollen unter der Bedingung B Wahrscheinlichkeiten für das Ereignis $A \cap C$ angeben. Mit der Definition der bedingten Wahrscheinlichkeit gilt:

$$\nu(A \cap C \mid B) = \frac{\nu(A \cap B \cap C)}{\nu(B)}.$$

Unter der Bedingung $\lambda \equiv \gamma \bmod l^r$ des Ereignisses C gelten die Äquivalenzen

$$v_l^{(r)}(det(\lambda) - 1) = s \Longleftrightarrow v_l(det(\gamma) - 1) = s$$

im Fall $(s < r)$ und

$$v_l^{(r)}(det(\lambda) - 1) = r \Longleftrightarrow v_l(det(\gamma) - 1) \geq r$$

im Fall $(s = r)$. Daher ergibt ein Vergleich mit der Definition der Mengen $X_{r,s}^{\lambda}(\alpha, \beta)$ und X_s bzw. der abgeleiteten endlichen Mengen

$$\nu(X_r^{\lambda}(\alpha, \beta)) = \nu(A \cap B \cap C) = \nu(X_{r,s}^{\lambda}(\alpha, \beta))$$

im Fall $(s < r)$ und

$$\nu(X_r^{\lambda}(\alpha, \beta)) = \nu(A \cap B \cap C) = \sum_{t=r}^{\infty} \nu(X_{r,t}^{\lambda}(\alpha, \beta))$$

im Fall $(s = r)$. Dies macht zusammen mit der Tatsache $\nu(X_s) = \nu(B)$ im Fall $(s < r)$ und $\sum_{t=r}^{\infty} \nu(X_t) = \nu(B)$ im Fall $(s = r)$ die Behauptung des Satzes offensichtlich. □

Tabelle 3 folgt nun sofort durch die Durchführung der Rechnungen aus Satz(7.4) für jeden Eintrag von Tabelle 4 für alle Konstellationen von $\alpha \leq \beta$ und $r \geq \alpha$ mit r, α, $\beta \in \mathbb{N}$. Die Wichtigkeit von Tabelle 3 für den folgenden Abschnitt besteht in der Erkenntnis, daß wir die Wahrscheinlichkeiten der Mengen $X_r^{\lambda}(\alpha, \beta)$ in allen auftretenden Fällen für $\alpha \leq \beta$ unter der Bedingung $v_l^{(r)}(det(\lambda) - 1) = s$ angeben können, oder anders formuliert, daß die einzigen Unterschiede in den Formeln bei festgehaltenen $\alpha \leq \beta$ durch die Bedingung $v_l^{(r)}(det(\lambda) - 1) = s$ zustande kommen. Wir werden im nächsten Abschnitt die Kongruenzbedingung abschwächen, indem wir nicht mehr $\gamma \equiv \lambda \bmod l^r$ fordern, sondern für ein $z \in \mathbb{Z}_l / l^r \mathbb{Z}_l$ die Bedingung

$$det(\gamma) \equiv z \bmod l^r$$

aufstellen. Wir werden sehen, daß die daraus resultierenden bedingten Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ in Abhängigkeit von $v_l^{(r)}(z - 1) = s$ angegeben werden können.

Die Volumina der Mengen $X_r^{\lambda}(\alpha, \beta)$ sind sehr regelmäßig, wenn wir keine Bedingung an $\lambda \in G_r$ im Vorhinein stellen. Mit der Notation vom Beweis von Satz(7.4) gilt für $\lambda \in G_r$:

$$(A \cap B \cap C) = X_r^{\lambda}(\alpha, \beta),$$

und wir haben das folgende

Korollar 7.5 *Seien α, β, s, $r \in \mathbb{N}$ mit $\alpha \leq \beta$, $s \leq r$ und sei $\lambda \in G_r$ so gegeben, daß $X_r^{\lambda}(\alpha, \beta) \neq \emptyset$ ist. Es sei $s = v_l^{(r)}(det(\lambda) - 1)$. Dann sind die Volumina bzgl. des Haar'schen Maßes ν der Mengen $X_r^{\lambda}(\alpha, \beta)$ durch die folgende Tabelle gegeben.*

	$0 < r \leq \alpha$	$\alpha < r \leq \beta$	$r > \beta$
$s < r$	$-$	$\frac{l^2}{l^2-1} \cdot l^{-3r-\beta}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r}$
$s = r$	$\nu(X(\alpha, \beta))$	$\frac{l^2}{l^2-1} \cdot l^{-3r-\beta}$	$\frac{l^3}{(l^2-1)(l-1)} \cdot l^{-4r}$

Tabelle der Volumina $\nu(X_r^{\lambda}(\alpha, \beta))$

8 Die Gleichverteilungsaussage

Im ganzen Abschnitt sei stets $p \neq l$ vorausgesetzt.

8.1 Die Volumina der Mengen $X^z_{r,s}(\alpha, \beta)$

Definition 8.1 *Seien $l \in \mathbb{P}$ und α, β, r, s, $n \in \mathbb{N}$ mit den Bedingungen $\alpha \leq \beta$, $n > \max(\beta, r, s)$ und $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ gegeben. Wir definieren die Mengen*

$$X^z_{r,s}(\alpha,\beta) = \{\gamma \in G \mid cok(\gamma - 1) \cong H_{\alpha,\beta} \quad \wedge \quad det(\gamma) \equiv z \bmod l^r$$
$$\wedge \quad v_l(\det(\gamma) - 1) = s\}.$$

Wir definieren die entsprechenden endlichen Mengen

$$X^{z,(n)}_{r,s}(\alpha,\beta) = \{\gamma \in G_n \mid \gamma \in X^{(n)}(\alpha,\beta) \quad \wedge \quad det(\gamma) \equiv z \bmod l^r$$
$$\wedge \quad v_l(\det(\gamma) - 1) = s\}.$$

Definition 8.2 *Seien $l \in \mathbb{P}$ und α, β, r, $n \in \mathbb{N}$ mit den Bedingungen $\alpha \leq \beta$, $n > \max(\beta, r)$ und $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ gegeben. Wir definieren die Mengen*

$$X^z_r(\alpha,\beta) = \{\gamma \in G \mid cok(\gamma - 1) \cong H_{\alpha,\beta} \quad \wedge \quad det(\gamma) \equiv z \bmod l^r\}.$$

Wir definieren die entsprechenden endlichen Mengen

$$X^{z,(n)}_r(\alpha,\beta) = \{\gamma \in G_n \mid \gamma \in X^{(n)}(\alpha,\beta) \quad \wedge \quad det(\gamma) \equiv z \bmod l^r\}.$$

Bemerkung 8.3 *Seien $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$, α, β, r, s, $n \in \mathbb{N}$ mit $\alpha \leq \beta$ und $s \geq \alpha$. Dann gilt für $n > max(\beta, s, r)$:*

$$\nu(X^z_{r,s}(\alpha,\beta)) = \frac{|X^{z,(n)}_{r,s}(\alpha,\beta)|}{|G_n|},$$

$$\nu(X^z_r(\alpha,\beta)) = \frac{|X^{z,(n)}_r(\alpha,\beta)|}{|G_n|}.$$

Sei $v^{(r)}_l(z-1) = s$. Dann gilt im Fall $(s < r)$:

$$\nu(X^z_r(\alpha,\beta) \mid v^{(r)}_l(z-1) = s) = \frac{\nu(X^z_{r,s}(\alpha,\beta))}{\nu(X_s)},$$

sowie für $(s = r)$:

$$\nu(X^z_r(\alpha,\beta) \mid v^{(r)}_l(z-1) = r) = \frac{\sum_{t \geq r} \nu(X^z_{r,t}(\alpha,\beta))}{\sum_{t \geq r} \nu(X_t)}.$$

Beweis: Nach Voraussetzung ist $n > \max(s, r, \beta)$, daher sind die Wahrscheinlichkeiten $\nu(X^z_{r,s}(\alpha,\beta))$ und $\nu(X^z_r(\alpha,\beta))$ wohldefiniert. Für den Nachweis der Identität für $\nu(X^z_r(\alpha,\beta) \mid v^{(r)}_l(z-1) = s)$ können wir die Argumentation aus dem Beweis von Satz(7.4) wortwörtlich übernehmen, wenn wir $det(\lambda)$ durch z ersetzen sowie die Bedingung C durch die Bedingung

$$C' = \{\gamma \in G \mid det(\gamma) \equiv z \bmod l^r\}.$$

□

Proposition 8.4 *Seien $l \in \mathbb{P}$, r, $s \in \mathbb{N}$, $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ gegeben. Dann gilt mit der Definition der Mengen $X^z_{r,s}(\alpha,\beta)$*
im Fall $(r = 0)$:

$$X^z_{r,s}(\alpha,\beta) = X_s(\alpha,\beta),$$

im Fall $(0 \leq \alpha \leq s < r)$:

$$X^z_{r,s}(\alpha,\beta) \neq \emptyset \Leftrightarrow v_l^{(r)}(z-1) = s,$$

und in den Fällen $(0 < r \leq \alpha \leq s)$ und $(0 \leq \alpha < r \leq s)$:

$$X^z_{r,s}(\alpha,\beta) \neq \emptyset \Leftrightarrow v_l^{(r)}(z-1) = r.$$

In allen anderen Fällen sind die Mengen $X^z_{r,s}(\alpha,\beta)$ leer und die Volumina $\nu(X^z_{r,s}(\alpha,\beta))$ gleich Null.

Beweis: Im Fall $(r = 0)$ ist die Kongruenzbedingung $\det(\gamma) \equiv z \bmod l^r$ gleich der leeren Bedingung und die übrigen Bedingungen aus der Definition der Mengen $X^z_{r,s}(\alpha,\beta)$ sind genau die Bedingungen aus der Definition der Mengen $X_s(\alpha,\beta)$.
Im Fall $(0 \leq \alpha \leq s < r)$ gilt unter der Voraussetzung $\det(\gamma) \equiv z \bmod l^r$ die Äquivalenz

$$v_l(det(\gamma) - 1) = s \Leftrightarrow v_l^{(r)}(z-1) = s.$$

Daher ist die Bedingung $v_l^{(r)}(z-1) = s$ im Fall $(0 \leq \alpha \leq s < r)$ notwendig. Hinreichend ist die Bedingung $v_l^{(r)}(z-1) = s$ im Fall $(0 \leq \alpha \leq s < r)$ mittels der Korollare(4.5,4.7,4.11) und Lemma(4.3).
In den beiden anderen Fällen ist immer $det(\gamma) - 1 \equiv 0 \bmod l^r$, da $s \geq r$ nach Voraussetzung. Das bedeutet aber, daß $v_l^{(r)}(z-1) = r$ sein muß, damit $X^z_{r,s}(\alpha,\beta) \neq \emptyset$ ist. Ist umgekehrt $v_l^{(r)}(z-1) = r$, dann folgt $det(\gamma) - 1 \equiv 0 \bmod l^r$, was wegen $s \geq r$ immer erfüllt ist. □

Satz 8.5 (Gleichverteilungsaussage) *Sei $l \in \mathbb{P}$ gegeben, α, β, r, $s \in \mathbb{N}$ mit $\alpha \leq \min(\beta, s)$.*
Sei $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ so gewählt, daß die Menge $X^z_{r,s}(\alpha,\beta) \neq \emptyset$ ist. Dann gilt im Fall $(\alpha = s = 0 < r)$ für $l \neq 2$:

$$\nu(X^z_{r,s}(\alpha,\beta)) = \nu(X_s(\alpha,\beta)) \cdot (l-2)^{-1} l^{-(r-1)}.$$

Ist $(\alpha = s = 0 < r)$ und $l = 2$, so sind die Mengen der Form $X^z_{r,s}(\alpha,\beta)$ leer und die Volumina $\nu(X^z_{r,s}(\alpha,\beta))$ gleich Null.
In den Fällen $(0 < s = \alpha < r)$ und $(\alpha < s < r)$ gilt die Identität

$$\nu(X^z_{r,s}(\alpha,\beta)) = \nu(X_s(\alpha,\beta)) \cdot (l-1)^{-1} l^{s-(r-1)},$$

und in den Fällen $(r = 0)$, $(0 < r \leq \alpha)$ und $(\alpha < r \leq s)$ gilt:

$$\nu(X^z_{r,s}(\alpha,\beta)) = \nu(X_s(\alpha,\beta)).$$

Beweis: Im Fall $(r = 0)$ ist die Kongruenzbedingung $\det(\gamma) \equiv z \bmod l^r$ aus der Definition der Mengen $X^z_{r,s}(\alpha, \beta)$ leer und die Behauptung ist offensichtlich.
Im Fall $(0 < r \leq \alpha)$ gilt unter der Voraussetzung, daß wir $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ so gewählt haben, daß $X^z_{r,s}(\alpha, \beta) \neq \emptyset$ ist, die Mengengleichheit

$$X^z_{r,s}(\alpha, \beta) = X_s(\alpha, \beta).$$

Im Fall $(\alpha < r \leq s)$ gilt für $\lambda \in G_r$ mit der Herleitung von Tabelle 4:

$$\nu(X^z_{r,s}(\alpha, \beta)) = \nu(X^\lambda_{r,s}(\alpha, \beta)) \cdot |\lambda| = \nu(X_s(\alpha, \beta)).$$

Der Fall $(\alpha < s < r)$ folgt ebenfalls mit den Ergebnissen der Tabelle 4, wobei sich der Faktor $(l-1)^{-1} \cdot l^{s-(r-1)}$ wie folgt erklärt: Auf der Stufe(s) gibt es je nachdem, welche andere Bedingung zusätzlich zu

$$det(\delta) + tr(\delta) \equiv 0 \bmod l^s \quad \wedge \quad det(\delta) + tr(\delta) \not\equiv 0 \bmod l^{s+1} \tag{1}$$

durch die Bedingungen der Mengen $X_s(\alpha, \beta)$ gegeben ist, entweder $(l-1)^2l^2$, $(l-1)l^3$ oder $(l-1)l^2$ Möglichkeiten zur Bestimmung der Koeffizienten der Matrix $\delta = \gamma - 1$. Ersetzen wir nun die Bedingung(1) für $k \in \mathbb{N}_l - \{0\}$ durch die stärkere Kongruenzbedingung

$$det(\delta) + tr(\delta) \equiv 0 \bmod l^s \quad \wedge \quad det(\delta) + tr(\delta) \equiv k \cdot l^s \bmod l^{s+1}, \tag{2}$$

aus der Definition der Mengen $X^z_{r,s}(\alpha, \beta)$ für $(\alpha < s < r)$, so werden die oben aufgezählten Anzahlen von Möglichkeiten für die Wahl der Koeffizienten auf der Stufe s jeweils reduziert zu $(l-1)l^2$, l^3 bzw. l^2, also alle drei in derselben Weise durch den Faktor $(l-1)^{-1}$. Dies erklärt den Faktor $(l-1)^{-1}$ für den Fall $(\alpha < s < r)$. Für $m \in \mathbb{N}$ werden auf den Stufen $(s < m < r)$ durch die Bedingung

$$det(\delta) + tr(\delta) \equiv 0 \bmod l^s \quad \wedge \quad det(\delta) + tr(\delta) \equiv z \cdot l^s \bmod l^r \tag{3}$$

für $z = \sum_{i=0}^{r-s-1} k_i \cdot l^i$, $k_i \in \mathbb{N}_l$ für alle $(0 \leq i < r-s)$, $k_0 \neq 0$, auf jeder Stufe (m) die Möglichkeiten zur Bestimmung der Koeffizienten um den Faktor l reduziert (vgl. die Korollare(4.5,4.7)). Das erklärt den Faktor $l^{s-(r-1)}$.

Noch zu beweisen ist die Gleichverteilungsaussage in den Fällen $(\alpha = s < r)$. Gehen wir der Reihe nach vor.
(a) Der Fall $\alpha = \beta = s = 0$:
Sei eine Matrix $\gamma \in G_1$ gegeben und sei $\gamma - 1 = \delta \in G_1$ mit $\delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Seien x und y die beiden Eigenwerte modulo l der Matrix δ und sei $k \in \{1, 2, \ldots, (l-2)\}$. Dann entnehmen wir der Definition der Mengen $X^z_{1,0}(\alpha, \beta)$ die Bedingungen

$$ad - bc \equiv xy \not\equiv 0 \bmod l \quad \wedge \quad a + d \equiv x + y \bmod l \quad \wedge$$

$$ad - bc + a + d \equiv xy + x + y \equiv k \bmod l \tag{4}$$

Wir erhalten sofort die Einschränkungen $x \not\equiv -1 \bmod l \ \wedge \ x \not\equiv 0 \bmod l$ für x und entsprechend $y \not\equiv -1 \bmod l \ \wedge \ y \not\equiv 0 \bmod l$ für y. Demnach haben wir $l-2$ Möglichkeiten, unter der Bedingung

$$xy + x + y \equiv k \bmod l$$

die Variable x zu wählen. Dadurch wir die Variable y eindeutig bestimmt, da $k \in \{1, 2, \ldots, (l-2)\}$ fest vorgegeben ist nach Voraussetzung. Haben wir eine der beiden Variablen x und y mit $(l-2)$ Möglichkeiten gewählt, so sind sowohl die Summe $x+y$ als auch das Produkt xy eindeutig bestimmt. Nun bestimmen wir die Variablen a, b, c, d derart, daß sie für festes x und y den Bedingungen(4) genügen. Die Fälle $ad = xy$ und $ad \neq xy$ unterscheidend erhalten wir nacheinander $(2(2l-1))$ und $(l-1)(l-2)$ Möglichkeiten zur Bestimmung von a,b,c,d. Mit Bemerkung(8.3) folgt dann

$$\nu(X^z_{1,0}(0,0)) = \nu(X^k_{1,0}(0,0)) = \frac{(l-2)(2(2l-1)+(l-1)(l-2))}{|G_1|} = \frac{l-2}{(l-1)^2}.$$

(b) Der Fall $\alpha = \beta = s > 0$:
Seien $\gamma \in G_{\alpha+1}$ und $\delta \in M_{\alpha+1}$ mit $\gamma - 1 = \delta$ und δ mit den Einträgen a,b,c,d angeordnet wie im Fall(a). Sei $k \in \{1, 2, \ldots, (l-1)\}$ gegeben. Wir entnehmen der Definition der Mengen $X^z_{\alpha+1,\alpha}(\alpha, \alpha)$ die Bedingungen

$$a_\alpha + d_\alpha \equiv k \bmod l \quad \wedge \quad a_\alpha d_\alpha - b_\alpha c_\alpha \not\equiv 0 \bmod l.$$

In den Fällen $a_\alpha = 0$ und $a_\alpha = k$ haben wir jeweils $(l-1)^2$ Möglichkeiten der Wahl für $b_\alpha c_\alpha$, und d_α ist eindeutig bestimmt. Für alle anderen $(l-2)$ Wahlen für a_α ($a_\alpha \neq k$ und $a_\alpha \neq 0$) ist d_α ebenfalls eindeutig bestimmt und wir haben $(2l-1+(l-1)(l-2))$ Möglichkeiten zur Bestimmung von $b_\alpha c_\alpha$. Zusammengenommen berechnen wir mit Bemerkung(8.3) und $z = k \cdot l^\alpha$

$$\nu(X^z_{\alpha+1,\alpha}(\alpha,\alpha)) = \frac{(l-2)((2l-1)+(l-1)(l-2))+(l-1)^2}{|G_{\alpha+1}|}$$

$$= \frac{(l^2-l-1)}{(l+1)(l-1)^2} \cdot l^{-4\alpha}.$$

(c) Der Fall $0 \leq s = \alpha < \beta$:
Seien n, $r \in \mathbb{N}$ gegeben mit $r > \alpha$ und $n > \max(\beta, r)$. Seien $\delta \in M_n$, $\gamma \in G_n$ mit $\delta = \gamma - 1$ und δ mit den Einträgen a,b,c,d angeordnet wie in Fall(a). Wir entnehmen aus der Definition der Mengen $X^z_{\alpha+1,\alpha}(\alpha, \beta)$ für ein $k \in \{1, 2, \ldots, (l-2)\}$ im Fall $(\beta > \alpha = s = 0)$ (bzw. $k \in \{1, 2, \ldots, (l-1)\}$ im Fall $(\beta > \alpha = s > 0)$) die Bedingungen

$$\delta \equiv 0 \bmod l^\alpha \quad \wedge \quad ad - bc \equiv 0 \bmod l^{\alpha+1} \quad \wedge \quad a + d \equiv k \cdot l^\alpha \bmod l^{\alpha+1},$$

und daraus schließen wir für die Stufe (α) der Matrix δ

$$a_\alpha + d_\alpha \equiv k \bmod l \quad \wedge \quad a_\alpha d_\alpha - b_\alpha c_\alpha \equiv 0 \bmod l.$$

Wir unterscheiden die drei Fälle $(a_\alpha = 0)$, $(a_\alpha = k)$, $(0 \neq a_\alpha \neq k)$ und erhalten nacheinander $(2l-1)$, $(2l-1)$, $(l-2)(l-1)$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe (α) unter den Bedingungen der Definition der Mengen $X^z_{\alpha+1,\alpha}(\alpha, \beta)$. Zusammengenommen ergeben sich so $l(l+1)$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe (α). Da die Bedingungen der Definition

der Mengen $X^z_{\alpha+1,\alpha}(\alpha,\beta)$ für alle Stufen ungleich α die gleichen sind wie im Falle der Mengen $X_\alpha(\alpha,\beta)$, berechnen wir mit Bemerkung(8.3) das Volumen

$$\nu(X^z_{\alpha+1,\alpha}(\alpha,\beta)) = \frac{(l^2+l)(l-1)}{l(l+1)(l-1)^2}\cdot l^{-3\alpha-\beta} = \frac{1}{l-1}\cdot l^{-3\alpha-\beta}.$$

In allen Fällen $(0<\alpha=s<r)$ erklärt sich der Faktor $l^{s-(r-1)}$ durch die oben im Zusammenhang mit der Bedingung(3) für den Fall $(\alpha<s<r)$ angeführten Aussagen. Im Fall $(\alpha=0=s<r)$ erklärt sich der Faktor $l^{(-r+1)}$ durch Korollar(4.11). □

Korollar 8.6 (Tabellenform der Gleichverteilungsaussage) *(a) Seien $l\in\mathbb{P}$ und α, β, r, $s\in\mathbb{N}$ mit $\alpha\le min(\beta,s)$ gegeben. Sei $z\in\mathbb{Z}_l/l^r\mathbb{Z}_l$ so gewählt, daß $X^z_{r,s}(\alpha,\beta)\neq\emptyset$ ist und sei $r>\alpha$. Dann sind die Volumina der Mengen $X^z_{r,s}(\alpha,\beta)$ bzgl. des normierten Haar'schen Maßes ν gegeben durch die folgende Tabelle.*

	$(\alpha=s<r)$	$(\alpha<s<r)$	$(\alpha<r\le s)$
$0=\alpha=\beta$	$\frac{l(l-2)}{(l-1)^2}\cdot l^{-r}$ *	$\frac{(l^2-l-1)l}{(l^2-1)(l-1)}\cdot l^{-r}$	$\frac{l^2-l-1}{l^2-1}\cdot l^{-s}$
$0<\alpha=\beta$	$\frac{(l^2-l-1)l}{(l^2-1)(l-1)}\cdot l^{-3\alpha-r}$	$\frac{l^2}{l^2-1}\cdot l^{-3\alpha-r}$	$\frac{l}{l+1}\cdot l^{-3\alpha-s}$
$0=\alpha<\beta$	$\frac{l}{l-1}\cdot l^{-\beta-r}$ *	$l^{-\beta-r}$	$\frac{l-1}{l}\cdot l^{-\beta-s}$
$0<\alpha<\beta$	$\frac{l}{l-1}\cdot l^{-2\alpha-\beta-r}$	$l^{-2\alpha-\beta-r}$	$\frac{l-1}{l}\cdot l^{-2\alpha-\beta-s}$

Tabelle 5: $\nu(X^z_{r,s}(\alpha,\beta))$

*Die mit einem * versehenen Wahrscheinlichkeiten sind für $l=2$ nicht definiert. (b) Im Fall $(0\le r\le\alpha)$ gilt entweder $\nu(X^z_{r,s}(\alpha,\beta))=0$, falls $v_l^{(r)}(z-1)<r$ ist, oder*

$$\nu(X^z_{r,s}(\alpha,\beta)) = \nu(X_s(\alpha,\beta)),$$

falls $v_l^{(r)}(z-1)=r$ ist.

Mit Bemerkung(8.3) folgen aus der Tabellenform der Gleichverteilungsaussage die Wahrscheinlichkeiten der Mengen $X^z_r(\alpha,\beta)$.

Korollar 8.7 *Seien $l\in\mathbb{P}$ und α, β, r, $s\in\mathbb{N}$ mit $\alpha\le\min(\beta,s)$. Sei $z\in\mathbb{Z}_l/l^r\mathbb{Z}_l$. Dann sind die Volumina der Mengen $X^z_r(\alpha,\beta)$ bzgl. des normierten Haar'schen Maßes ν unter der Bedingung $v_l^{(r)}(z-1)=s$ durch die folgende Tabelle gegeben.*

	$(\alpha=s<r)$	$(\alpha<s<r)$	$(\alpha<r=s)$
$0=\alpha=\beta$	$\frac{l}{l-1}\cdot l^{-r}$ *	$\frac{(l^2-l-1)l}{(l^2-1)(l-1)}\cdot l^{s-r}$	$\frac{l^2-l-1}{l^2-1}$
$0<\alpha=\beta$	$\frac{(l^2-l-1)l}{(l^2-1)(l-1)}\cdot l^{-2\alpha-r}$	$\frac{l^2}{l^2-1}\cdot l^{-3\alpha+s-r}$	$\frac{l}{l+1}\cdot l^{-3\alpha}$
$0=\alpha<\beta$	$\frac{l}{l-2}\cdot l^{-\beta-r}$ *	$l^{-\beta+s-r}$	$\frac{l-1}{l}\cdot l^{-\beta}$
$0<\alpha<\beta$	$\frac{l}{l-1}\cdot l^{-\alpha-\beta-r}$	$l^{-2\alpha-\beta+s-r}$	$\frac{l-1}{l}\cdot l^{-2\alpha-\beta}$

Tabelle 6: $\nu(X^z_r(\alpha,\beta)\mid v_l^{(r)}(z-1)=s)$

*Die mit einem * versehenen Wahrscheinlichkeiten sind für $l = 2$ nicht definiert. Im Fall $(r = 0 \leq \alpha)$ gilt:*

$$\nu(X_r^z(\alpha,\beta) \mid v_l^{(r)}(z-1) = s) = \nu(X(\alpha,\beta)),$$

sowie im Fall $(0 < r \leq \alpha)$:

$$\nu(X_r^z(\alpha,\beta) \mid v_l^{(r)}(z-1) = r) = \nu(X(\alpha,\beta)) \cdot \frac{l-1}{l} \cdot l^r.$$

Die Angabe der Wahrscheinlichkeiten $\nu(X_r^z(\alpha,\beta))$ in Abhängigkeit von der abgeschnittenen $l-$adischen Bewertung $v_l^{(r)}(z-1)$ durch Tabelle 6 allein löst das Problem aus der Motivierung der Problemstellung noch nicht, da die Bedingung $v_l^{(r)}(z-1) = s$ nicht die gewünschte Bedingung ist. Deshalb lösen wir die Problemstellung auf die folgende Art und Weise auf.

8.2 Die bedingten Wahrscheinlichkeiten $P_r^z(\alpha,\beta)$

Definition 8.8 *Wir definieren für n, $r \in \mathbb{N}$ und $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ die Mengen*

$$X_r^z = \{\gamma \in G \mid det(\gamma) \equiv z \bmod l^r\}.$$

Die von X_r^z abgeleiteten endlichen Mengen sind für $n \geq r$ definiert durch

$$X_r^{z,(n)} = \{\gamma \in G_n \mid det(\gamma) \equiv z \bmod l^r\}.$$

Proposition 8.9 *Für die Mengen X_r^z gilt im Fall $r = 0$*

$$X_0^z = G,$$

und für $r > 0$ gilt

$$X_r^z \neq \emptyset \Longleftrightarrow z \in \mathbb{Z}_l^*.$$

Beweis: Klar im Fall $r = 0$. Im Fall $r > 0$ gilt $\det(\gamma) \in \mathbb{Z}_l^*$ für alle $\gamma \in G$. □

Bemerkung 8.10 *Sei $z \in \mathbb{Z}_l^*$. Dann gilt für die Volumina $\nu(X_r^z)$ der Mengen X_r^z im Fall $(r > 0)$*

$$\nu(X_r^z) = \frac{l}{l-1} \cdot l^{-r}.$$

Im Fall $(r = 0)$ gilt $\nu(X_0^z) = 1$ unabhängig von z.

Beweis: Der Fall $(r = 0)$ ist klar. Sei nun $(n \geq r > 0)$ und $z \in \mathbb{Z}_l^*$ zusammen mit $\gamma \in G_1$ gegeben. Dann gibt es genau $l(l^2-1)$ Möglichkeiten zur Bestimmung der Koeffizienten der Stufe 0 der Matrix γ, so daß die Bedingung $det(\gamma) \equiv z \bmod l$ erfüllt ist. Dann gibt es nach Korollar(4.11) genau $l^{3(r-1)}$ viele Fortsetzungen $\overline{\gamma}$ von γ auf die Stufe $(r-1)$, so daß für $n = r$ gilt:

$$\nu(X_r^z) = \frac{|X_r^{z,(r)}|}{|G_r|} = \frac{l(l^2-1)l^{3(r-1)}}{|G_r|} = \frac{1}{l-1} \cdot l^{-(r-1)}.$$

□

Wir wollen nun die bedingten Wahrscheinlichkeiten dafür berechnen, daß der $l-$Torsionsanteil $E(\mathbb{F}_p)[l^\infty]$ einer elliptischen Kurve $E/\mathbb{F}_p$ isomorph zu einer Gruppe der Form $H_{\alpha,\beta}$ ist, falls wir $p \equiv z \bmod l^r$ für $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ gewählt haben.

Definition 8.11 *Sei $l \in \mathbb{P}$ gegeben. Seien α, β, $r \in \mathbb{N}$ gegeben mit $\alpha \leq \beta$. Sei $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ gegeben. Wir definieren die bedingten Wahrscheinlichkeiten*

$$P_r^z(\alpha,\beta) := \frac{P(\mathcal{F}, E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta} \wedge p \equiv z \bmod l^r)}{P(\mathcal{F}, p \equiv z \bmod l^r)}$$

Unter Annahme der Gültigkeit der Hypothese (H) haben wir die folgende

Proposition 8.12 *Sei $l \in \mathbb{P}$ gegeben. Seien α, β, s, $r \in \mathbb{N}$ gegeben mit $\alpha \leq \beta$. Sei $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ gegeben und sei $v_l^{(r)}(z-1) = s$.*
Dann gilt im Fall $(r > s \geq \alpha)$:

$$P_r^z(\alpha,\beta) = \frac{\nu(X_{r,s}^z(\alpha,\beta))}{\nu(X_r^z)}.$$

Im Fall $(r = s > \alpha)$ gilt:

$$P_r^z(\alpha,\beta) = \sum_{t=r}^{\infty} \frac{\nu(X_{r,t}^z(\alpha,\beta))}{\nu(X_r^z)}.$$

Im Fall $(0 < r = s \leq \alpha)$ gilt:

$$P_r^z(\alpha,\beta) = \nu(X(\alpha,\beta)) \cdot \frac{l-1}{l} \cdot l^r.$$

Im Fall $(r = 0)$ gilt:

$$P_r^z(\alpha,\beta) = \nu(X(\alpha,\beta)).$$

In allen anderen Fällen gilt $P_r^z(\alpha,\beta) = 0$.

Beweis: In allen Fällen wollen wir die Gültigkeit der Hypothese (H) annehmen.
Im Fall $(r = 0)$ bleibt von allen Bedingungen aus der Definition der Wahrscheinlichkeiten $P_r^z(\alpha,\beta)$ einzig die Bedingung im Zähler $E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta}$ übrig. Alle anderen Bedingungen sind gleich der leeren Bedingung, woraus mittels (H) die Behauptung folgt.
Im Fall $(0 < r = s \leq \alpha)$ gilt wegen $p \equiv 1 \bmod l^\alpha$ von der Bedingung $E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta}$ unter der Voraussetzung $v_l^{(r)}(z-1) = r$ die Gleichheit

$$P(\mathcal{F}, E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta} \wedge p \equiv z \bmod l^r) = P(\mathcal{F}, E(\mathbb{F}_p)[l^\infty] \cong H_{\alpha,\beta}),$$

und mittels (H) folgt die Behauptung.
Im Fall $(\alpha \leq s < r)$ gilt unter der Voraussetzung $p \equiv z \bmod l^r$ die Äquivalenz

$$v_l(p-1) = s \Longleftrightarrow v_l^{(r)}(z-1) = s,$$

woraus mittels (H) die Behauptung folgt.
Im Fall $(s = r > \alpha)$ gilt unter der Voraussetzung $p \equiv z \bmod l^r$ die Äquivalenz

$$v_l(p-1) \geq r \Longleftrightarrow v_l^{(r)}(z-1) = r.$$

Daher folgt mittels (H)

$$P_r^z(\alpha,\beta) = \sum_{t=r}^{\infty} \frac{\nu(X_{r,t}^z(\alpha,\beta))}{\nu(X_r^z)}$$

□

Korollar 8.13 (Auflösung der Problemstellung) *Seien $l \in \mathbb{P}$, $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ und α, β, r, $s \in \mathbb{N}$ mit $\alpha \leq \min(\beta, s)$ gegeben. Sei $r > \alpha$ und sei $v_l^{(r)}(z-1) = s$. Dann sind die bedingten Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ durch die folgende Tabelle gegeben.*

	$(\alpha = s < r)$	$(\alpha < s \leq r)$
$0 = \alpha = \beta$	$\frac{l-2}{l-1}$ *	$\frac{l^2-l-1}{l^2-1}$
$0 < \alpha = \beta$	$\frac{l^2-l-1}{l^2-1} \cdot l^{-3\alpha}$	$\frac{l}{l+1} \cdot l^{-3\alpha}$
$0 = \alpha < \beta$	$l^{-\beta}$ *	$\frac{l-1}{l} \cdot l^{-\beta}$
$0 < \alpha < \beta$	$l^{-2\alpha-\beta}$	$\frac{l-1}{l} \cdot l^{-2\alpha-\beta}$

Tabelle 7: $P_r^z(\alpha, \beta)$

*Die mit einem * versehenen Wahrscheinlichkeiten sind für $l = 2$ nicht definiert. Insbesondere geht die Größe z nur über $s = v_l^{(r)}(z-1)$ in die Beschreibung von $P_r^z(\alpha, \beta)$ ein.*

Beweis: Die Aussage folgt aus Korollar(8.5) durch Aufsummieren der geometrischen Reihe (vgl. Proposition(8.12). □
Durch Proposition(8.12) ist die eingangs formulierte Problemstellung dieser Arbeit umfassend beantwortet. Letztlich hängen die resultierenden Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ für $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$, $r \in \mathbb{N}$ und $(r > \alpha)$ für fest vorgegebene α, β nur von $v_l^{(r)}(z-1) \geq \alpha$ ab.

Beispiel 8.14 *Sei $l = 5$, $\alpha = 0$, $\beta = 2$ und $r = 1$. Es ist $s = 0$ für $z = 2, 3, 4$ und $s = 1$ für $z = 1$. Deshalb gilt*

$$P_1^z(0, 2) = \frac{5}{125}$$

für $z = 2, 3, 4$, und

$$P_1^z(0, 2) = \frac{4}{125}$$

für $z = 1$. Mit anderen Worten: $E(\mathbb{F}_p)[5^\infty] \cong \mathbb{Z}/25\mathbb{Z}$ ist für Primzahlen $p \equiv 2, 3, 4 \bmod 5$ etwas wahrscheinlicher als für $p \equiv 1 \bmod 5$.

Beispiel 8.15 *Sei $l = 11$, $\alpha = 1$, $\beta = 3$ und $r = 2$. Es ist $s = 1$ für $z = 12, 23, \ldots, 100$ und $s = 2$ für $z = 1$. Deshalb gilt*

$$P_2^z(1, 3) = \frac{11}{121} \cdot 11^{-4}$$

für $z = 12, 23, \ldots, 100$, und

$$P_2^z(1, 3) = \frac{10}{121} \cdot 11^{-4}$$

für $z = 1$.

Die Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ nehmen beim Übergang von $(\alpha = s)$ nach $(\alpha < s)$ im Fall $(\alpha < \beta)$ ab.

Beispiel 8.16 *Sei* $l = 7$, $\alpha = 0$, $\beta = 0$ *und* $r = 1$. *Es ist* $s = 0$ *für* $z = 2, 3, \ldots, 6$ *und* $s = 1$ *für* $z = 1$. *Deshalb gilt*

$$P_1^z(0,0) = \frac{40}{48}$$

für $z = 2, 3, \ldots 6$, *und*

$$P_1^z(0,0) = \frac{41}{48}$$

für $z = 1$.

Beispiel 8.17 *Sei* $l = 3$, $\alpha = 1$, $\beta = 1$ *und* $r = 2$. *Es ist* $s = 1$ *für* $z = 4$ *und* $z = 7$ *und* $s = 2$ *für* $z = 1$. *Deshalb gilt*

$$P_2^z(1,1) = \frac{5}{8} \cdot 3^{-3}$$

für $z = 4$ *und* $z = 7$, *und*

$$P_2^z(1,1) = \frac{6}{8} \cdot 3^{-3}$$

für $z = 1$.

Die Wahrscheinlichkeiten $P_r^z(\alpha, \beta)$ nehmen beim Übergang von $(\alpha = s)$ nach $(\alpha < s)$ im Fall $(\alpha = \beta)$ zu.

A Appendix

A.1 Definition eines Topologischen Raumes und einleitende Eigenschaften

Definition A.1 *Ein topologischer Raum $(X, \mathfrak{D})$ ist eine Menge X versehen mit einem System $\mathfrak{D}$ von Teilmengen von X, so daß folgende Axiome erfüllt sind:*

1. *Jede Vereinigung von Mengen aus $\mathfrak{D}$ gehört zu $\mathfrak{D}$, $\emptyset \in \mathfrak{D}$.*
2. *Jeder endliche Durchschnitt von Mengen aus $\mathfrak{D}$ gehört zu $\mathfrak{D}$, $X \in \mathfrak{D}$.*

Die Elemente $x \in X$ heißen Punkte, die Elemente von $\mathfrak{D}$ heißen die offenen Mengen von X, und $\mathfrak{D}$ heißt die Topologie von X. Sei a ein Element aus X und V eine Teilmenge von X. V heißt eine Umgebung von a, wenn es ein $U \in \mathfrak{D}$ gibt mit der Eigenschaft $a \in U \subset V$. X heißt separiert oder ein Hausdorff-Raum, wenn zu allen $a, b \in X$ mit der Eigenschaft $a \neq b$ Umgebungen U von a, V von b existieren mit der Eigenschaft $U \cap V = \emptyset$.

Korollar A.2 *Die Menge $A^c = X \setminus A$ heißt die zu A komplementäre Menge in X. Eine Menge $A \subset X$ heißt abgeschlossen, wenn die zu A komplementäre Menge A^c in X offen ist. Jeder Durchschnitt abgeschlossener Mengen ist abgeschlossen. Jede endliche Vereinigung abgeschlossener Mengen ist abgeschlossen. X und $\emptyset$ sind abgeschlossene Mengen.*

Definition A.3 *Ist $Y \subset X$, so ist $\mathfrak{D}|Y := \{U \cap V \mid U \in \mathfrak{D}\}$ eine Topologie auf Y, die Spurtopologie oder Relativtopologie von $\mathfrak{D}$ auf Y. Jedes Paar der Form $(Y, \mathfrak{D}|Y)$ heißt Teilraum von $(X, \mathfrak{D})$.*

Definition A.4 *Sind X, Y topologische Räume und $f : X \to Y$ eine Abbildung, so heißt f stetig in $a \in X$, falls zu jeder Umgebung V von $f(a)$ eine Umgebung U von a existiert, so daß die Bedingung $f(U) \subset V$ erfüllt ist. Eine Abbildung $f : X \to Y$ heißt stetig, wenn sie in jedem Punkt $a \in X$ stetig ist.*

Korollar A.5 *Kompositionen stetiger Abbildungen sind stetig.*

Bemerkung A.6 *Eine Abbildung $f : X \to Y$ ist genau dann stetig, wenn $f^{-1}(V)$ offen ist in X für jede offene Menge $V \subset Y$.*

Definition A.7 *Seien durch $\mathfrak{G}$ und $\mathfrak{T}$ zwei Topologien auf der Menge X gegeben. Die Topologie $\mathfrak{G}$ heißt feiner als die Topologie $\mathfrak{T}$ (oder auch $\mathfrak{T}$ gröber als $\mathfrak{G}$), falls die Bedingung $\mathfrak{T} \subset \mathfrak{G}$ erfüllt ist.*

Proposition A.8 *Sind $(X, \mathfrak{G})$, $(Y, \mathfrak{T})$, topologische Räume, so gibt es eine gröbste Topologie $\mathfrak{D}$ auf $X \times Y$, welche die kanonischen Projektionen $pr_X : X \times Y \to X$, $(x, y) \mapsto x$ und $pr_Y : X \times Y \to Y$, $(x, y) \mapsto y$ stetig macht. $\mathfrak{D}$ heißt die Produkttopologie von $\mathfrak{G}$ und $\mathfrak{T}$, und $(X \times Y, \mathfrak{D})$ das topologische Produkt von $(X, \mathfrak{G})$ und $(Y, \mathfrak{T})$.*

Definition A.9 *Ein System $\mathfrak{U}$ offener Teilmengen von X heißt eine offene Überdeckung von $A \subset X$, falls die Bedingung $A \subset \bigcup_{U\in\mathfrak{U}} U$ erfüllt ist. Eine Teilmenge $\mathfrak{T}$ der Überdeckung $\mathfrak{U}$ von A heißt eine Teilüberdeckung, falls $\mathfrak{T}$ eine Überdeckung von A ist. X heißt kompakt, wenn jede offene Überdeckung von X eine endliche Teilüberdeckung hat. Eine Menge $A \subset X$ heißt kompakt, wenn der Teilraum $(A, \mathfrak{D}|A)$ kompakt ist.*

Definition A.10 *Eine Familie $\mathfrak{F}$ von Teilmengen eines topologischen Raumes X hat die endliche Durchschnittseigenschaft, wenn jeder endliche Durchschnitt von Mengen aus $\mathfrak{F}$ nicht leer ist.*

Bemerkung A.11 *Ein topologischer Raum X ist kompakt genau dann, wenn für jede Familie $\mathfrak{F}$ abgeschlossener Teilmengen von X, welche die endliche Durchschnittseigenschaft hat, der Durchschnitt aller Mengen aus $\mathfrak{F}$ nicht leer ist.*

Definition A.12 *Es seien I eine Indexmenge und $((X_i, \mathfrak{D}_i))_{i\in I}$ eine Familie topologischer Räume. Das cartesische Produkt $X := \prod_{i\in I} X_i$ ist definiert als Menge aller Abbildungen $x : I \to \cup_{i\in I} X_i$, so daß $x_i := x(i) \in X_i$ für alle $i \in I$ist. Wir schreiben: $x = (x_i)_{i\in I}$. Sind alle $X_i \neq \emptyset (i \in I)$, so ist $X \neq \emptyset$ (Auswahlaxiom). Das System aller Mengen der Form $\prod_{i\in I} U_i$, zu denen eine endliche Menge $E \subset I$ existiert, so daß $U_i \in \mathfrak{D}_i$ für alle $i \in E$ und $U_i = X_i$ für alle $i \in I \setminus E$, bildet die Basis einer Topologie $\mathfrak{D}$ auf X, der Produkttopologie der $\mathfrak{D}_i (i \in I)$. Dieses ist die gröbste Topologie auf X, die alle Projektionen $pr_\kappa : X \to X_\kappa$, $pr_\kappa((x_i)_{i\in I}) := x_\kappa (\kappa \in I)$ stetig macht. Alle $pr_\kappa (\kappa \in I)$ sind offene Abbildungen.*

Satz A.13 (Satz von Tychonoff) *Sei I eine Indexmenge und $(X_i, \mathfrak{D}_i)$ eine Familie topologischer Räume. Sind für alle $i \in I$ die topologischen Räume $(X_i, \mathfrak{D}_i)$ kompakt, so ist auch das cartesische Produkt $X := \prod_{i\in I} X_i$ versehen mit der Produkttopologie $\mathfrak{D}$ der $\mathfrak{D}_i$ kompakt.*

Zum Beweis dieses Satzes, der zusätzliche Notation erfordert, vgl. etwa im Buch [RI] die Seiten $197 - 199$.

Definition A.14 *Ein topologischer Raum X heißt lokal-kompakt, falls jedes Element $a \in X$ eine kompakte Umgebung hat.*

A.2 Definition einer lokal-kompakten Gruppe

Definition A.15 *Sei G eine multiplikative Gruppe mit Einselement e. G heißt eine topologische Gruppe, wenn G mit einer Topologie ausgestattet ist, so daß die Gruppenmultiplikation $G \times G \to G$, $(x, y) \mapsto xy$ und die Inversenbildung $G \to G$, $x \mapsto x^{-1}$ stetig sind. ($G \times G$ sei hierbei mit der Produkttopologie versehen).*

Definition A.16 *Eine lokal-kompakte Gruppe ist eine topologische Gruppe, deren Topologie lokal-kompakt und Hausdorff'sch ist.*

A.3 Die Existenz und Eindeutigkeit des Haar'schen Maßes für lokal-kompakte Gruppen

Definition A.17 *Sei X eine Menge. Die Menge aller Teilmengen von X, bezeichnet durch $\mathfrak{P}(X)$, heißt die Potenzmenge der Menge X.*

Definition A.18 *Sei X eine Menge und seien A, $B \subset \mathfrak{P}(X)$ gegeben. Die formale Operation*

$$\triangle(A,B) := A \triangle B := A \backslash B \cup B \backslash A$$

heißt symmetrische Differenz der Mengen A und B.

Satz A.19 *Versieht man $\mathfrak{P}(X)$ mit der symmetrischen Differenz $\triangle$ als Addition und der Durchschnittsbildung $\cap$ als Multiplikation, so ist $(\mathcal{P}(X), \triangle, \cap)$ ein kommutativer Ring mit dem Nullelement $\emptyset$ und dem Einselement X.*

Definition A.20 *Eine Menge $\mathfrak{R} \subset \mathfrak{P}(X)$ heißt ein Ring (über X), wenn $\mathfrak{R}$ ein Unterring des Ringes $(\mathfrak{P}(X), \triangle, \cap)$ ist. Ein Ring $\mathfrak{A}$ mit $X \in \mathfrak{A}$ heißt eine Algebra über X oder ein Körper.*

Definition A.21 *Sei X eine Menge. Eine Menge $\mathfrak{R} \subset \mathfrak{P}(X)$ heißt ein $\sigma-$Ring (über X), wenn $\mathfrak{R}$ ein Ring ist und wenn für jede Folge $(A_n)_{n\geq 1}$ von Mengen aus $\mathfrak{R}$ gilt, daß die Vereinigung $\bigcup_{n=1}^{\infty} A_n$ ein Element von $\mathfrak{R}$ ist. Ein $\sigma-$Ring $\mathfrak{A} \subset \mathfrak{P}(X)$ mit der Eigenschaft $X \in \mathfrak{A}$ heißt eine $\sigma-$Algebra (über X).*

Definition A.22 *Eine auf einer $\sigma-$Algebra $\mathfrak{A}$ erklärte Abbildung $\mu : \mathfrak{A} \to \mathbb{R} \cup \{\infty\}$ ist genau dann ein Maß, wenn gilt:*

1. $\mu(\emptyset) = 0$,
2. $\mu \geq 0$,
3. *Für jede Folge $(A_n)_{n\geq 1}$ disjunkter Mengen aus $\mathfrak{A}$ gilt*

$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n).$$

Definition A.23 *Sei X eine Menge, $\mathfrak{A}$ eine $\sigma-$Algebra über X und sei $\mu : \mathfrak{A} \to \mathbb{R} \cup \{\infty\}$ ein Maß.*
(a) Das Tripel $(X, \mathfrak{A}, \mu)$ heißt Maßraum.
(b) Gilt $\mu(X) = 1$, so heißt μ ein Wahrscheinlichkeitsmaß und $(X, \mathfrak{A}, \mu)$ ein Wahrscheinlichkeitsraum.

Definition A.24 *Sei $(X, \mathfrak{A}, \mu)$ ein Wahrscheinlichkeitsraum. Jede Teilmenge $A \subset X$ heißt Ereignis. Zwei Ereignisse A, $B \subset X$ heißen unabhängig, falls $\mu(A \cap B) = \mu(A) \cdot \mu(B)$ gilt.*

Definition A.25 *Sei X eine Menge und $\mathfrak{A}$ eine $\sigma-$Algebra von X. Sei durch $\mu : \mathfrak{A} \to \mathbb{R} \cup \{\infty\}$ ein Maß und durch $A \subset X$ eine Teilmenge von X gegeben. A heißt meßbar bzgl. μ (oder $\mu-$meßbar) falls für alle Teilmengen $B \subset X$ gilt:*

$$\mu(B) = \mu(A \cap B) + \mu(A^c \cap B).$$

Hierbei bezeichnet $A^c = X \backslash A$ das Komplement von A in X.

Sei X ab sofort ein Hausdorff Raum. Wir verwenden die Bezeichnungen $\mathfrak{U}(X)$ für das System der offenen Teilmengen von X und $\mathfrak{K}(X)$ für das System der kompakten Teilmengen von X.

Definition A.26 *Sei durch X ein topologischer Raum zusammen mit dem System $\mathfrak{U}$ der offenen Teilmengen von X gegeben. Dann heißt die von $\mathfrak{U}$ erzeugte $\sigma-$Algebra $\sigma(\mathfrak{U})$ die $\sigma-$Algebra der Borelschen Teilmengen von X und wir schreiben $\mathfrak{B}(X) = \sigma(\mathfrak{U})$.*

Definition A.27 *Sei eine Gruppe $G \subset \mathfrak{B}$ gegeben. Ein Maß $\mu : \mathfrak{B}(G) \to [0, \infty]$ heißt linksinvariant, wenn gilt:*

$$\mu(yB) = \mu(B) \qquad \forall(B \in \mathfrak{B}, y \in G).$$

Entsprechend definieren wir die Eigenschaft für ein Maß μ, rechtsinvariant zu sein, wenn gilt:

$$\mu(Bx) = \mu(B) \qquad \forall(B \in \mathfrak{B}, x \in G).$$

Ein Maß μ heißt invariant, wenn es links- und rechtsinvariant ist.

Definition A.28 *Es seien $\mathfrak{B} \supset \mathfrak{A}$ eine σ-Algebra und $\mu : \mathfrak{A} \to [0.\infty]$ ein Maß. μ heißt lokal-endlich, wenn zu jedem $x \in X$ eine offene Umgebung U von x existiert mit $\mu(U) < \infty$. Ein lokal-endliches Maß $\mu : \mathfrak{B} \to [0, \infty]$ heißt ein Borel-Maß.*

Definition A.29 *Sei G eine lokal-kompakte Gruppe und sei μ ein nicht leeres Borel-Maß auf G. Dann wird μ ein linkes Haar'sches Maß (bzw. ein Haar'sches Maß) genannt, wenn es invariant unter Linkstranslation (bzw. translationsinvariant) ist. Entsprechend ist ein rechtes Haar'sches Maß als ein rechtstranslationsinvariantes Maß definiert.*

Satz A.30 *Sei G eine lokal-kompakte Gruppe. Dann existiert ein linkes Haar'sches Maß auf G.*

Satz A.31 *Sei G eine lokal-kompakte Gruppe, und seien μ und ν beides linke Haar'sche Maße auf G. Dann gibt es eine positive reelle Zahl c, so daß $\nu = c\mu$ ist. Es gilt:*

$$\mu(G) < \infty \iff G \text{ ist kompakt.}$$

Beweis: Zum Beweis der Sätze(A.30,A.31) vergleiche im Buch [EL] die Seiten $356 - 366$.

Korollar A.32 *Sei G eine kompakte Gruppe. Dann ist jedes linksinvariante (bzw. rechtsinvariante) Haar'sche Maß auf G invariant.*

Beweis: Zum Beweis vergleiche im Buch [EL] die Seiten 366-367.

B Mengenverzeichnis

$X(\alpha,\beta)$	$= \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta}\},$	Abschnitt(4.2)
$X_s(\alpha,\beta)$	$= \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \wedge v_l(\det(\gamma)-1) = s\},$	Abschnitt(4.4)
$X_r^{\lambda}(\alpha,\beta)$	$= \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \wedge \lambda \equiv \gamma \bmod l^r\},$	Abschnitt(4.5)
$X_{r,s}^{\lambda}(\alpha,\beta)$	$= \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \wedge \lambda \equiv \gamma \bmod l^r \wedge$ $v_l(\det(\gamma)-1) = s\},$	Abschnitt(4.6)
$X_{r,s}^{z}(\alpha,\beta)$	$= \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \wedge z \equiv \det(\gamma) \bmod l^r \wedge$ $v_l(\det(\gamma)-1) = s\},$	Abschnitt(8.1)
$X_r^{z}(\alpha,\beta)$	$= \{\gamma \in G \mid cok(\gamma-1) \cong H_{\alpha,\beta} \wedge \det(\gamma) \equiv z \bmod l^r\},$	Abschnitt(8.1)
X_r^{z}	$= \{\gamma \in G \mid \det(\gamma) \equiv z \bmod l^r\},$	Abschnitt(8.2)
X_s	$= \{\gamma \in G \mid v_l(det(\gamma)-1) = s\},$	Abschnitt(7)

Hierbei ist

- $H_{\alpha,\beta} = \mathbb{Z}/l^{\alpha}\mathbb{Z} \times \mathbb{Z}/l^{\beta}\mathbb{Z}$ für α, $\beta \in \mathbb{N}$ und $\alpha \leq \beta$,
- $\lambda \in G_r$ für $r \in \mathbb{N}$,
- $z \in \mathbb{Z}_l/l^r\mathbb{Z}_l$ für $r \in \mathbb{N}$,
- $v_l(a)$ die l-adische Bewertung einer Zahl $a \in \mathbb{Z}_l$ wie in Definition(4.1),
- $cok(\omega)$ der Kokern einer Abbildung $\omega : \mathbb{Z}_l \times \mathbb{Z}_l \to \mathbb{Z}_l \times \mathbb{Z}_l$ wie in Definition(4.12).

Literatur

[Co-Le] H. Cohen-H.W. Lenstra, Jr.: Heuristics on class groups of number fields.
In: Lecture Notes in Mathematics 1068, 33-62, Springer 1984

[El] Jürgen Elstrodt, Maß- und Integrationstheorie, 3. erweiterte Auflage Springer 2002

[Ge] Ernst-Ulrich Gekeler, The Distribution of Group Structures on Elliptic Curves over Finite Prime Fields, Documenta Mathematica 11 (2006), Seite 119-142

[Ne] Jürgen Neukirch, Algebraische Zahlentheorie, Springer 1.Nachdruck 2002

[Ri] Rinow, Lehrbuch der Topologie, VEB Deutscher Verband der Wissenschaften, Berlin 1975

[Se] Jean-Pierre Serre, A Course in Arithmetic, Springer April 1973

[Sil] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer 1986