Masterarbeit

Wahrscheinlichkeitsverteilung endlicher Moduln über Polynomringen

30. März 2011

Autorin: Sarah Katharina Detzler
Betreuer: Professor Dr. Ernst-Ulrich Gekeler

Wintersemester 2010/2011

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Arbeit selbst angefertigt und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

Saarbrücken, den 30.03.2011

Inhaltsverzeichnis

Kapitel 1

Einleitung

Die vorliegende Arbeit, die den Titel „Wahrscheinlichkeitsverteilung endlicher Moduln über Polynomringen“ trägt, wurde im Zeitraum vom 1. Oktober 2010 bis zum 31. März 2011 zum Erlangen des Masterabschlusses in Mathematik (mathematische Grundlagenforschung) unter Betreuung von Professor Dr. Ernst-Ulrich Gekeler an der Universität des Saarlandes verfasst.
Dieser Arbeit liegen die Doktorarbeit von Johannes Lengler [Len09], die sich mit der Wahrscheinlichkeitsverteilung endlicher abelscher Gruppen befasst, sowie [CL84] und [Ful97] zugrunde.
Wir beschäftigen uns mit folgender Problemstellung: Erzeugt man zufällig einen endlichen Modul über einem Polynomring, so ist es interessant zu wissen, mit welcher Wahrscheinlichkeit dieser Modul gewisse Eigenschaften aufweist, bzw. mit welcher Wahrscheinlichkeit er isomorph zu einem gegebenen Modul ist. Die Idee zur Definition eines solchen Wahrscheinlichkeitsmaßes kam erstmals 1984 im Paper [CL84] von Cohen und Lenstra auf. Sie postulierten, dass das Gewicht der Klassengruppe eines Zahlkörpers umgekehrt proportional zur Größe ihrer Automorphismengruppe ist. Dies soll auf die hier betrachtete Problemstellung übertragen werden, indem man dieses Maß durch Normierung zu einem Wahrscheinlichkeitsmaß macht. Beschränkt man sich auf die lokale Situation, in der für ein fixiertes Primideal $\mathfrak{p}$ nur endliche $\mathfrak{p}$-primäre Moduln über einem Polynomring in einer Variablen über einem endlichen Körper betrachtet werden, so erhält man wie gewünscht ein Wahrscheinlichkeitsmaß. Dann kann man eine natürliche Bijektion zwischen der Menge der Partitionen und diesen Moduln finden. Zudem werden wir eine gruppentheoretische Interpretation mittels der Konjugationsklassen der allgemeinen linearen Gruppe über einem endlichen Körper angeben.
In der allgemeinen Situation hingegen ist die Definition eines Wahrscheinlichkeitsmaßes nicht mehr möglich, wie wir in Kapitel 6 sehen werden. Ersetzt man jedoch die σ-Additivität durch endliche Additivität, so erhält man einen Inhaltsraum und kann Inhalte statt Wahrscheinlichkeiten betrachten. Eine wichtige Rolle bei der Berechnung dieser Inhalte spielt dabei die Zeta-Funktion.

Im zweiten Kapitel werden die Grundlagen, die zum Verständnis dieser Arbeit erforderlich sind, kurz zusammengetragen. Dies umfasst algebraische Grundlagen, Grundlagen über Partitionen sowie eine Einführung in q-Reihen und elementare Definitionen der Statistik.
In Kapitel 3 betrachten wir nur endliche $\mathfrak{p}$-primäre Moduln über Polynomringen in einer Variablen über endlichen Körpern, da wir für diese einen Wahrscheinlichkeitsraum erhalten. Als Erstes wird das Prinzip der Cohen-Lenstra-Heuristik erläutert und es werden Aussagen über die Struktur von endlichen $\mathfrak{p}$-primären Moduln gesammelt. Ebenso wird die Größe der Automorphismengruppe berechnet und damit das Cohen-Lenstra-Wahrscheinlichkeitsmaß definiert. Danach wird ein natürlicher stochastischer Prozess zum Erzeugen von endlichen $\mathfrak{p}$-primären Moduln angegeben, dessen Ergebnis empirisch überprüft werden kann. Zum Abschluss verwenden wir dieses Wissen, um Beispiele zu berechnen.
Dann wird im vierten Kapitel die Cohen-Lenstra-Abbildung definiert. Zur Berechnung dieser Abbildung wird ein Algorithmus, der mit Young-Diagrammen arbeitet, sowie ein numerischer Algorithmus angegeben. Zum Ende des Kapitels benutzen wir diese Theorie zur Berechnung eines Beispiels.
In Kapitel 5 wird der Zusammenhang des Cohen-Lenstra-Wahrscheinlichkeitsmaßes mit den Konjugationsklassen der allgemeinen linearen Gruppe hergestellt. Dazu werden wir zwei Algorithmen, einen mittels Young-Tableaus und einen mittels Young-Gittern, angeben. Anschließend werden Resultate, die aus dieser Theorie hergeleitet werden, zusammengetragen.
Die globale Theorie wird in Kapitel 6 behandelt, indem wir zunächst einige Grundlagen über Zeta-Funktionen sammeln. Da es nicht möglich ist, ein Wahrscheinlichkeitsmaß zu definieren, werden Inhalte und Erwartungswerte behandelt. Die Definition dieser Inhalte ist zunächst nicht zur Berechnung von Beispielen geeignet. Deshalb wird eine bessere Methode entwickelt, diese Inhalte zu berechnen, wobei sich die Theorie der Zeta-Funktionen und die Tauber-Theorie als hilfreich erweisen. Schließlich werden die so gewonnenen Sätze zur Berechnung von Beispielen herangezogen.

An dieser Stelle möchte ich mich noch bei all denen bedanken, die mich bei der Anfertigung dieser Arbeit unterstützt haben. Mein ganz besonderer Dank gilt Professor Dr. Ernst-Ulrich Gekeler für die sehr gute Betreuung diese Arbeit. Außerdem bedanke ich mich ganz herzlich bei Anne Wald, Simon Krämer, Johannes Lengler sowie meinen Eltern Heidi und Karl-Heinz Detzler und meiner Schwester Jana Detzler.

Kapitel 2

Grundlagen

Diese Arbeit richtet sich an Leser, die bereits einige Grundlagen im Bereich der Algebra besitzen. Die wichtigsten Aussagen werden in diesem Kapitel nochmal aufgeführt. Dazu gehören algebraische Grundlagen, Partitionen, q-Reihen und elementare Statistik. Leser, denen diese Theorien wohlbekannt sind, können problemlos zu Kapitel 3 übergehen.

2.1 Algebraische und maßtheoretische Grundlagen

2.1.1 Satz (Elementarteilersatz):
Sei R ein Hauptidealring und M ein endlich erzeugter freier R-Modul. Weiter sei $N \subset M$ ein Untermodul. Dann existieren Elemente $x_1, \ldots, x_r \in M$, die Teil einer Basis von M sind, sowie Koeffizienten $\alpha_1, \ldots, \alpha_r \in R - \{0\}$, so dass gilt:

1. *$\alpha_1 x_1, \ldots, \alpha_r x_r$ bilden eine Basis von N.*
2. *$\alpha_i | \alpha_{i+1}$ für $1 \leq i \leq r$.*

Dabei sind $\alpha_1, \ldots, \alpha_r$ bis auf Assoziiertheit eindeutig bestimmt durch N, unabhängig von der Wahl von $x_1, \ldots, x_r$. Man nennt $\alpha_1, \ldots, \alpha_r$ die Elementarteiler von $N \subset M$. Insbesondere ist deren Anzahl r eindeutig bestimmt (siehe [Bos06], Seite 210, Theorem 4).

2.1.2 Satz (Lemma von Nakayama):
Es sei R ein kommutativer Ring mit 1, M ein endlich erzeugter nichttrivialer R-Modul und $\mathfrak{a}$ ein Ideal, das im Jacobson-Radikal $J(R)$ liegt. Dann ist $\mathfrak{a}M \neq M$.

Die folgenden drei Aussagen sind Korollare bzw. Umformulierungen des Lemmas von Nakayama.

2.1.3 Korollar:

1. *Ist M ein endlich erzeugter R-Modul, N ein Untermodul und $\mathfrak{a} \subset J(R)$ ein Ideal, so gilt:*

$$M = \mathfrak{a}M + N \;\Rightarrow\; M = N.$$

2. *Es seien R ein lokaler Ring, $\mathfrak{m}$ sein maximales Ideal und $K := R/\mathfrak{m}$ der Restklassenkörper.*
   Sind dann $x_1, \ldots, x_n$ Urbilder der Elemente einer Basis des K-Vektorraums $M/\mathfrak{m}M$, so erzeugen die x_i den Modul M.
   Diese Folgerung kann man zum Heben von Basen verwenden.

3. *Es seien R ein lokaler Ring, $\mathfrak{m}$ sein maximales Ideal und M, N endlich erzeugte R-Moduln. Dann gilt: $\varphi : M \to N$ ist genau dann bijektiv, wenn $\bar{\varphi} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ bijektiv ist.*

2.1.4 Definition:
Sei Ω eine beliebige nichtleere Menge. Eine Familie $\mathcal{A}$ von Teilmengen von Ω heißt σ-Algebra, wenn gilt:

1. *Ω liegt in $\mathcal{A}$.*

2. *Ist eine Menge $A \subset \Omega$ in $\mathcal{A}$ enthalten, so auch ihr Komplement.*

3. *Sind $A_1, A_2 \ldots$ aus $\mathcal{A}$, so liegt auch $\bigcup_{i=1}^{\infty} A_i$ in $\mathcal{A}$.*

2.1.5 Definition:
Für einen gegebenen topologischen Raum X ist die Borelsche σ-Algebra definiert als die kleinste σ-Algebra, die die offenen Mengen von X enthält. Die Elemente dieser σ-Algebra heißen Borel-Mengen (siehe [Lan69], Seite 128, Definition 10.1).

2.1.6 Definition:
Sei $\mathcal{A}$ eine σ-Algebra, die die Borelsche σ-Algebra enthält.
Ein Maß $\mu : \mathcal{A} \to [0, \infty]$ heißt σ-regulär, falls für jedes $A \in \mathcal{A}$ gilt:

1. $\mu(A) = \sup\{\mu(K) : K \subset A,\ K \text{ kompakt}\}$.

2. *Ist K kompakt, so ist $\mu(K)$ endlich.*

3. $\mu(A) = \inf\{\mu(U) : A \subset U,\ U \text{ offen}\}$.

2.1.7 Definition:
Das (linke) Haarsche Maß einer lokalkompakten Gruppe G ist das bis auf einen Faktor eindeutig bestimmte linksinvariante, σ-reguläre Maß auf den Borel-Mengen, das auf nichtleeren offenen Teilmengen positiv ist. Ein Maß μ heißt dabei linksinvariant, wenn für jede Borel-Menge A und jedes Gruppenelement g

$$\mu(gA) = \mu(A)$$

oder in Integralschreibweise

$$\int_G f(gx)\,\mathrm{d}\mu(x) = \int_G f(x)\,\mathrm{d}\mu(x)$$

für stetige Funktionen f und Gruppenelemente g gilt (Siehe [Lan69], Seite 351-352).

2.1.8 Definition:
Eine Folge

$$A' \longrightarrow A \longrightarrow A''$$

von Objekten und Morphismen in einer geeigneten Kategorie heißt exakt an der Stelle A, wenn

$$\mathrm{im}(A' \to A) = \ker(A \to A'')$$

gilt. Eine längere Folge

$$A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow A_4 \longrightarrow A_5$$

heißt exakt, wenn sie exakt an den Stellen A_2, A_3 und A_4 ist.
Eine kurze exakte Folge ist eine exakte Folge der Form

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0.$$

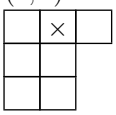
2.2 Partitionen

2.2.1 Definition:
Eine Partition ist ein Tupel nicht wachsender positiver ganzer Zahlen $\underline{n}_1 \geq \underline{n}_2 \geq \ldots \geq \underline{n}_k$. Wir nennen $n := \sum_{i=1}^{k} \underline{n}_i$ die Länge von $\underline{n}$ und sagen: $\underline{n}$ ist eine Partition von n. Die leere Partiton besitzt Länge Null und wird mit $\underline{0}$ bezeichnet. Wir nennen k den Rang von $\underline{n}$.
Mit $\mathcal{P}$ bezeichnen wir die Menge aller Partitionen.

2.2.2 Bemerkung:
In der Literatur ist es üblich, noch eine andere Definition für den Rang einer Partition zu verwenden. Wir wollen uns in dieser Arbeit aber auf die eben eingeführte Definition beschränken.

2.2.3 Definition:
Sei $\underline{n} = (\underline{n}_1, \underline{n}_2, \ldots, \underline{n}_k) \in \mathcal{P}$. Das zugehörige Young-Diagramm ist eine endliche Sammlung von Boxen, angeordnet in linksbündigen Zeilen, wobei die i-te Zeile (von oben gezählt) n_i Boxen enthält.
Wir nummerieren die Boxen in Paaren (i, j), wobei i die Zeilenzahl (von oben gezählt) und j die Spaltenzahl (von links gezählt) der Box ist.

2.2.4 Beispiel:
Das untere Diagramm zeigt das Young-Diagramm der Partition $(3, 2, 2)$; die $(1, 2)$-Box ist markiert:



2.2.5 Definition:
Für jedes $\underline{n} \in \mathcal{P}$ ist die zugehörige konjugierte Partition diejenige Partition, deren Young-Diagramm durch Reflektion des Young-Diagramms von $\underline{n}$ an der Hauptdiagonalen hervorgeht.
Äquivalent dazu kann man im Originaldiagramm die Zeilen anstatt der Spalten lesen.

2.2.6 Beispiel:
Die konjugierte Partition zum obigen Beispiel $(3, 2, 2)$ ist $(3, 3, 1)$.

2.2.7 Definition:
Wir versehen $\mathcal{P}$ mit einer partiellen Ordnungsrelation. Wir schreiben $\underline{n} < \underline{m}$, wenn das Young-Diagramm von $\underline{n}$ im Young-Diagramm von $\underline{m}$ enthalten ist. Äquivalent dazu gilt $\underline{n} < \underline{m}$ genau dann, wenn $\underline{n}_i \leq \underline{m}_i$ für alle $i \geq 1$, wobei unbestimmte Einträge auf 0 gesetzt werden.

2.3 q-Reihen

Wir werden uns im Folgenden mit q-Reihen beschäftigen. Diese Bezeichnung ist in der Literatur üblich und wurde deshalb übernommen. Da die hier angegebenen Identitäten in späteren Kapiteln ausschließlich auf Potenzreihen in der

Substitutionsvariablen q_0 angewendet werden, wird diese bereits hier verwendet.
Wir wollen uns mit der Funktion $a(n) := |\{\text{Partitionen von } n\}|$ beschäftigen. Ein elementares Werkzeug ist folgende Funktion, die im kombinatorischen Kontext als erzeugende Funktion

$$F(q_0) = \sum_{n=0}^{\infty} a(n) q_0^n$$

auftritt. Die Reihen, die in diesem Teil behandelt werden, haben alle positiven Konvergenzradius, sodass alle erzeugenden Funktionen wohldefiniert als holomorphe Funktionen auf einem geeigneten Gebiet sind.
Zunächst gilt die Produktformel:

$$F(q_0) = \prod_{i=1}^{\infty} (1 - q_0^i)^{-1}.$$

Diese kann direkt überprüft werden, indem man die geometrische Reihenentwicklung $(1 - q_0^i)^{-1} = 1 + q_0^i + q_0^{2i} + \dots$ benutzt und ausmultipliziert.
Des Weiteren gilt die Identität

$$F(q_0) = \prod_{i=1}^{\infty} (1 - q_0^i)^{-1} = \sum_{s=0}^{\infty} q_0^s \prod_{i=1}^{s} (1 - q_0^i)^{-1}. \tag{2.1}$$

Das Produkt $\prod_{i=1}^{s} (1 - q_0^i)^{-1} = \sum_{n=0}^{\infty} a_k(n) q_0^n$ stellt die erzeugende Funktion der Partitionen mit Gliedern kleiner oder gleich s dar. Weiter ist das Produkt $q_0^s \prod_{i=1}^{s} (1 - q_0^i)^{-1}$ die erzeugende Funktion der Partitionen mit höchstem Glied s. Dies zeigt die gewünschte Identität. Durch Konjugation ergibt sich auch: $a_s(n)$ ist gleich der Anzahl der Partitionen von n in höchstens s vielen ganzen Zahlen.

2.3.1 Satz:
Sei $a_{k,b}(n)$ die Anzahl der Partitionen von n in höchstens k ganze Zahlen von einer Größe von höchstens b. Dann ist die erzeugende Funktion durch

$$\psi_{k,b}(q_0) = \sum_{n=0}^{\infty} a_{k,b}(n) q_0^n = \frac{\prod_{i=1}^{k+b} (1 - q_0^i)}{\prod_{i=1}^{k} (1 - q_0^i) \prod_{i=1}^{b} (1 - q_0^i)}$$

gegeben.

Beweis: [AE04], Theorem 7.2.

Die vorangegangene Formel für die erzeugende Funktion von $a_k(n)$ kann als Formel für $\psi_{k,\infty}(q_0) = \psi_{\infty,k}(q_0)$ aufgefasst werden.

2.3.2 Satz (Rogers-Ramanujan-Identitäten):
Es gelten die Potenzreihenidentitäten:

1. $1+\sum_{r=1}^{\infty}\frac{{q_0}^{r^2}}{\prod_{s=1}^{r}(1-{q_0}^{s})}=\prod_{s=1}^{\infty}\frac{1}{(1-{q_0}^{5s-1})(1-{q_0}^{5s-4})}$.
2. $1+\sum_{r=1}^{\infty}\frac{{q_0}^{r(r+1)}}{\prod_{s=1}^{r}(1-{q_0}^{s})}=\prod_{s=1}^{\infty}\frac{1}{(1-{q_0}^{5s-2})(1-{q_0}^{5s-3})}$.

Beweis: [And98], Korollar 7.9 und Korollar 7.10.

2.4 Statistik

2.4.1 Definition:
Ein messbarer Raum ist ein Paar $(\Omega,\mathcal{A})$ bestehend aus einer nichtleeren Menge Ω und einer σ-Algebra $\mathcal{A}$ von Teilmengen von Ω. Ein Wahrscheinlichkeitsmaß P ist eine auf $\mathcal{A}$ definierte Funktion mit Werten in $[0,1]$, welche den folgenden drei Bedingungen genügt:

1. $P(\Omega)=1$.
2. $P(A)\geq 0$ *für alle* $A\in\mathcal{A}$.
3. P *ist* σ*-additiv, d.h. für paarweise disjunkte* $A_1,A_2,\cdots\in\mathcal{A}$ *ist*

$$P\left(\bigcup_{i=1}^{\infty}A_i\right)=\sum_{i=1}^{\infty}P(A_i).$$

Ein messbarer Raum versehen mit einem Wahrscheinlichkeitsmaß wird dann als Wahrscheinlichkeitsraum bezeichnet.

2.4.2 Definition:
1. *Eine Zufallsvariable auf einem messbaren Raum $(\Omega,\mathcal{A})$ ist eine messbare Funktion*
$$X:\Omega\to\mathbb{R}.$$
2. *Der Erwartungswert einer Zufallsvariablen X ist definiert als*
$$E(X)=\int_{\Omega}X\,dP.$$

2.4.3 Satz:
Sind X, Y reellwertige Zufallsvariablen auf dem Wahrscheinlichkeitsraum $(\Omega, \mathcal{A})$, für welche die Erwartungswerte $E(X)$, $E(Y)$, $E(X^2)$ und $E(Y^2)$ existieren, so heißt $Var(X) = E((X - E(X))^2)$ die Varianz von X und $Cov(X, Y) = E((X - E(X))(Y - E(Y)))$ die Kovarianz von X und Y. Es gilt:

1. $Var(X) = E(X^2) - E(X)^2$.

2. $Cov(X, Y) = E(XY) - E(X)E(Y)$.

(Siehe [Kre05], Seite 52-53).

Kapitel 3

Die lokale Cohen-Lenstra-Heuristik

Notation

Im Folgenden bezeichnen:

- $\mathbb{N} := \{0, 1, 2 \ldots\}$,
- $\mathbb{N}^+ := \{1, 2 \ldots\}$,
- $|M|$ oder auch $ord(M)$ die Kardinalität einer Menge M,
- q eine Primzahlpotenz,
- $\mathbb{F}_q$ den Körper mit q Elementen,
- $A := \mathbb{F}_q[X]$ den Polynomring über dem Körper mit q Elementen,
- $\mathfrak{p}$ ein Primideal in A, erzeugt von einem normierten irreduziblen Polynom p vom Grad n,
- $N\mathfrak{p}$ die Norm q^n von $\mathfrak{p}$,
- $deg(f)$ den Grad eines Polynoms $f \in A$,
- $A_\mathfrak{p} = \varprojlim_{n \in \mathbb{N}} A/\mathfrak{p}^n$ die Komplettierung von A nach $\mathfrak{p}$,
- $\mathcal{M}$ die Menge aller (Isomorphieklassen von) endlichen A-Moduln,
- $\mathcal{M}_\mathfrak{p}$ die Menge aller endlichen $\mathfrak{p}$-primären A-Moduln,
- $\underline{\lambda}$ eine Partition,

- Länge($\underline{\lambda}$) die Länge einer Partition $\underline{\lambda}$,
- $\mathcal{P}$ die Menge aller Partitionen,
- $rk(M)$ den Rang des Moduls M,
- $exp_{\mathfrak{p}}$ den $\mathfrak{p}$-adischen Exponenten des Moduls M,
- $Aut(M)$ die Automorphismengruppe von M,
- $w(M)$ das Cohen-Lenstra-Maß des Moduls M,
- $P(M)$ das Cohen-Lenstra-Wahrscheinlichkeitsmaß des Moduls M,
- $GL(m, A_{\mathfrak{p}})$ die allgemeine lineare Gruppe über $A_{\mathfrak{p}}$.

3.1 Generelles Prinzip

Zu Beginn werden wir das Prinzip der Cohen-Lenstra-Heuristik erläutern. Sei $\mathfrak{p}$ ein Primideal. Angenommen, wir haben einen natürlichen stochastischen Prozess zum Erzeugen endlicher $\mathfrak{p}$-primärer A-Moduln, dessen Ergebnis empirisch überprüft werden kann. Fixieren wir einen solchen $\mathfrak{p}$-Modul, so ist die Wahrscheinlichkeit dafür, dass der mit dem Prozess erzeugte zufällige endliche $\mathfrak{p}$-primäre A-Modul isomorph zu M ist, umgekehrt proportional zur Ordnung der Automorphismengruppe $Aut(M)$.
Dies ist kein bewiesenes Theorem, sondern ein heuristisches Prinzip. Cohen und Lenstra gaben in ihrem Paper [CL84] plausible Gründe an.

Zunächst betrachten wir nur endliche $\mathfrak{p}$-primäre A-Moduln, da wir für diese einen Wahrscheinlichkeitsraum erhalten. Später werden wir sehen, dass dies für allgemeine endliche A-Moduln nicht der Fall ist. Als Erstes befassen wir uns mit der Struktur von endlichen $\mathfrak{p}$-primären A-Moduln sowie der Größe der Automorphismengruppe. Anschließend definieren wir das Cohen-Lenstra-Wahrscheinlichkeitsmaß und geben einen natürlichen stochastischen Prozess zum Erzeugen von endlichen $\mathfrak{p}$-primären A-Moduln an. Zuletzt verwenden wir dieses Wissen, um Beispiele zu berechnen.

3.2 Endliche A-Moduln und endliche $\mathfrak{p}$-primäre A-Moduln

Zunächst gehen wir auf die verwendete Notation ein und tragen einige Fakten über endliche Moduln über dem Polynomring in einer Variablen zusammen. Es wird vorausgesetzt, dass der Leser mit der grundlegenden Modultheorie vertraut ist; falls nicht, findet man eine Einführung in [Bos06], Kapitel 6.
In der ganzen Arbeit werden wir uns ausschließlich mit endlichen A-Moduln

befassen. Zudem betrachten wir diese nur bis auf Isomorphie. Jedes Mal, wenn wir von Moduln sprechen, sind automatisch endliche A-Moduln gemeint und falls in Formeln über alle Moduln summiert wird, so bedeutet dies, dass wir über alle Isomorphieklassen von endlichen A-Moduln summieren. Im Folgenden fixieren wir ein Primideal $\mathfrak{p}$, das von einem normierten irreduziblen Polynom p mit Grad n erzeugt wird.

3.2.1 Definition:
Wir definieren die Norm $N\mathfrak{p}$ eines Ideals $\mathfrak{p}$ als $|A/\mathfrak{p}|$. Für ein normiertes irreduzibles Polynom $\mathfrak{p}$ vom Grad n gilt: $N\mathfrak{p} = q^n$.

3.2.2 Definition:
Ist M ein endlicher A-Modul, dann bezeichnet $ord(M)$ die Anzahl der Elemente in M. Der Rang $rk(M)$ von M ist die minimale Anzahl von Elementen, die M erzeugen. Wir bezeichnen mit $\mathcal{M}$ die Menge aller endlichen A-Moduln.

3.2.3 Definition:
Ein endlicher A-Modul wird $\mathfrak{p}$-primär genannt, wenn für jedes Element ein Exponent $e \in \mathbb{N}$ existiert, so dass $\mathfrak{p}^e$ dieses Element annulliert. Wir definieren $\mathcal{M}_\mathfrak{p}$ als die Menge aller endlichen $\mathfrak{p}$-primären A-Moduln oder äquivalent als die Menge aller endlichen $A_\mathfrak{p}$-Moduln. Diese Moduln wollen wir im Folgenden verkürzt als $\mathfrak{p}$-Moduln bezeichnen.

3.2.4 Definition:
Sei M ein endlicher $\mathfrak{p}$-primärer A-Modul. Wir definieren seinen $\mathfrak{p}$-adischen Exponenten $exp(M) = exp_\mathfrak{p}(M)$ als kleinstes $e \in \mathbb{N}$, so dass $\mathfrak{p}^e$ alle Elemente von M annulliert.

Die folgenden Sätze sind Korollare bzw. Abwandlungen des Elementarteilersatzes.

3.2.5 Satz:
Jeder endliche A-Modul ist ein direktes Produkt von zyklischen A-Moduln.

3.2.6 Satz:
Jeder endliche A-Modul M ist ein Torsionsmodul über A, d.h. für jedes $m \in M$ existiert ein $a \in A \setminus \{0\}$ mit $am = 0$.
Insbesondere ist M das Produkt von $\mathfrak{p}$-primären A-Moduln: $M = \prod_{\mathfrak{p} \in \mathbb{P}} M_\mathfrak{p}$. Die endlichen A-Moduln $M_\mathfrak{p}$ sind eindeutig durch M bestimmt und werden als $\mathfrak{p}$-Anteil oder $\mathfrak{p}$-primärer Anteil von M bezeichnet. Wir schreiben $r_\mathfrak{p}(M)$ für den Rang des $\mathfrak{p}$-primären Anteils von M.

3.2.7 Satz:
Ein endlicher $\mathfrak{p}$-primärer A-Modul M kann (bis auf Isomorphie) eindeutig in der Form

$$\prod_{i=1}^{k}(A/\mathfrak{p}^{e_i})^{r_i}$$

geschrieben werden. Hierbei ist $k \in \mathbb{N}$, $e_i, r_i \in \mathbb{N}^+$ und $e_1 > e_2 > \ldots > e_k$. Dies ist die Standarddarstellung eines $\mathfrak{p}$-Moduls.

3.2.8 Bemerkung:
Wir können diese Standarddarstellung auch als eine Partition mit r_i Summanden der Größe e_i als Einträge auffassen.

3.3 Die Ordnung der Automorphismengruppe

Für die Cohen-Lenstra-Heuristik benötigen wir die Größe der Automorphismengruppe $Aut(M)$ von M. Im Folgenden wollen wir uns mit einer elementaren Berechnung dieser Größe befassen.
Sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ teilerfremde Ideale von A, so ist

$$Hom(A/\mathfrak{a}_1, A/\mathfrak{a}_2) = 0$$

und

$$Aut(A/\mathfrak{a}_1 \times A/\mathfrak{a}_2) \cong Aut(A/\mathfrak{a}_1) \times Aut(A/\mathfrak{a}_2).$$

Dies zeigt, dass wir $|Aut(M)|$ nur für $\mathfrak{p}$-Moduln berechnen müssen. Die allgemeinere Situation, mit der wir uns in Kapitel 6 beschäftigen werden, kann mittels dieser Bijektion zusammengesetzt werden. Somit ist es völlig legitim und hilfreich, sich zunächst der lokalen Situation für ein fixiertes $\mathfrak{p}$ zuzuwenden.

Zunächst werden diese Automorphismen in bestimmte Matrizen übersetzt.
Anschließend können die Automorphismen leicht abgezählt werden.
Sei $M = \prod_{1 \le i \le k} M_i$ mit $M_i \cong (A/\mathfrak{p}^{e_i})^{r_i}$, wobei $k \ge 0$, $e_1 > e_2 > \ldots > e_k > 0$, $r_i > 0$.
Dann ist die Endomorphismengruppe $End(M) = \bigoplus_{1 \le i,j \le k} Hom(M_j, M_i)$, mit $Hom(M_j, M_i) = Hom((A/\mathfrak{p}^{e_j})^{r_j}, (A/\mathfrak{p}^{e_i})^{r_i})$.
Diese wird durch eine $r_i \times r_j$-Matrix mit Einträgen in $Hom((A/\mathfrak{p}^{e_j}), (A/\mathfrak{p}^{e_i}))$ beschrieben.

3.3.1 Lemma:
$Hom((A/\mathfrak{p}^{e}), (A/\mathfrak{p}^{e'}))$ ist kanonisch isomorph zu $A/\mathfrak{p}^{e'}$ für $e' \le e$ und zu $\mathfrak{p}^{e'-e}A/\mathfrak{p}^{e'}$ für $e' \ge e$.

Beweis: Ein Homomorphismus von $A/\mathfrak{p}^{e}$ nach $A/\mathfrak{p}^{e'}$ ist eindeutig durch das Bild der Eins bestimmt. Für $e' \le e$ gibt es keine Einschränkung; für $e' \ge e$ muss das Bild der Eins in $\mathfrak{p}^{e'-e}A/\mathfrak{p}^{e'}$ liegen. □

Die Endomorphismen von M werden dann durch folgende Matrizen beschrieben:

$$\begin{pmatrix} \boxed{A_1} & B_{1,2} & B_{1,3} & \cdots & B_{1,k} \\ C_{2,1} & \boxed{A_2} & B_{1,3} & \cdots & B_{2,k} \\ C_{3,1} & C_{3,2} & \boxed{A_3} & \cdots & B_{2,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{k,1} & C_{k,2} & C_{k,3} & \cdots & \boxed{A_k} \end{pmatrix} \begin{matrix} \}r_1 \\ \}r_2 \\ \}r_3 \\ \vdots \\ \}r_k, \end{matrix}$$

wobei A_i eine $r_i \times r_i$-Matrix, $B_{i,j}$ eine $r_i \times r_j$-Matrix und $C_{i,j}$ eine $r_i \times r_j$-Matrix ist.
Es gilt nun, die Einträge der einzelnen Teilmatrizen zu bestimmen.
Betrachten wir zunächst A_i. Sie beschreibt eine Abbildung von $(A/\mathfrak{p}^{e_i})^{r_i}$ in sich selbst mit Einträgen in $A/\mathfrak{p}^{e_i}$.
Die Teilmatrix $B_{i,j}$, $i < j$, bildet $(A/\mathfrak{p}^{e_j})^{r_j}$ nach $(A/\mathfrak{p}^{e_i})^{r_i}$ ab. Da e_j kleiner ist als e_i, müssen die Einträge von $B_{i,j}$ in $\mathfrak{p}^{e_i-e_j}A/\mathfrak{p}^{e_i}$ liegen, welcher als Modul isomorph ist zu $A/\mathfrak{p}^{e_j}$.
Die Teilmatrix $C_{i,j}$, $i > j$, bildet $(A/\mathfrak{p}^{e_j})^{r_j}$ nach $(A/\mathfrak{p}^{e_i})^{r_i}$ ab. Da e_i kleiner ist als e_j, müssen die Einträge von $C_{i,j}$ in $A/\mathfrak{p}^{e_i}$ liegen.
Somit haben wir alle Endomorphismen von M beschrieben, wir interessieren uns aber nur für die Automorphismen, d.h. Endomorphismen, die bijektiv sind. Das folgende Lemma zeigt, dass dies genau dann der Fall ist, wenn die diagonalen Blöcke invertierbar sind.

3.3.2 Lemma:
Sei wie oben eine Matrix gegeben, die einen Homomorphismus $\Phi : M \to M$ beschreibt. Dann sind folgende Aussagen äquivalent:

1. *Φ ist bijektiv.*
2. *A_i ist invertierbar für alle $i = 1, \ldots, k$.*
3. *Die reduzierte Matrix $\bar{A}_i$ von A_i mod $\mathfrak{p}$ ist invertierbar für alle $i = 1, \ldots, k$.*

Beweis: „2. $\Leftrightarrow$ 3.“ Eine Matrix ist genau dann invertierbar, wenn ihre Determinante invertierbar ist. Dies bedeutet in beiden Fällen, dass die Determinante nicht in $\mathfrak{p}$ liegt.
„1. $\Leftrightarrow$ 3.“ M ist ein Modul über dem lokalen Ring $A_\mathfrak{p}$ mit maximalem Ideal $\mathfrak{p}A_\mathfrak{p}$. Dann wird der reduzierte Endomorphismus $\bar{\phi}$ von $\bar{M} := M/\mathfrak{p}M$ durch eine Matrix von der Form

$$\begin{pmatrix} \boxed{\bar{A}_1} & 0 & 0 & \cdots & 0 \\ * & \boxed{\bar{A}_2} & 0 & \cdots & 0 \\ * & * & \boxed{\bar{A}_3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & \boxed{\bar{A}_k} \end{pmatrix}$$

dargestellt. Wir sehen, dass $\bar{\phi}$ genau dann bijektiv ist, wenn alle $\bar{A}_i$ invertierbar sind. Andererseits folgt nach dem Lemma von Nakayama (Satz 2.1.2), dass $\bar{\phi}$ genau dann bijektiv ist, wenn ϕ bijektiv ist. □

Zur weiteren Vereinfachung beweisen wir zunächst einen nützlichen Spezialfall, bevor wir die allgemeine Automorphismengruppe abzählen.

3.3.3 Lemma:
Sei $H := Aut((A/\mathfrak{p}^e)^r)$, dann ist

$$|H| = (q^n)^{r^2 e} \prod_{i=1}^{r} (1 - (q^n)^{-i}).$$

Beweis: Betrachten wir zunächst den Fall $e = 1$. Wir zählen die invertierbaren $r \times r$-Matrizen mit Einträgen in $A/\mathfrak{p}$. Die erste Zeile darf jeden von Null verschiedenen Vektor enthalten, dafür gibt es $(q^n)^r - 1$ viele Möglichkeiten.
Die zweite Zeile darf alle Vektoren enthalten, die nicht im Spann des Vektors in der ersten Zeile liegen. Dies schließt q^n Vektoren aus. Es bleiben also $(q^n)^r - q^n$ Möglichkeiten für die zweite Spalte.
In derselben Weise erhalten wir, dass die i-te Zeile alle Vektoren enthalten darf, die nicht im Spann der ersten $i-1$ Zeilenvektoren liegen. Dies gibt uns $(q^n)^r - (q^n)^{i-1}$ Möglichkeiten für die i-te Zeile. Insgesamt erhalten wir

$$\begin{aligned} \prod_{i=1}^{r} ((q^n) - (q^n)^{i-1}) &= (q^n)^{r^2} \prod_{i=1}^{r} (1 - (q^n)^{i-1-r}) \\ &= (q^n)^{r^2} \prod_{i=1}^{r} (1 - (q^n)^{-i}) \end{aligned}$$

viele irreduzible Matrizen. Für den Fall $e > 1$ benutzen wir die exakte Folge

$$0 \to H_1 \hookrightarrow H \to Aut((A/\mathfrak{p})^r) \to 1,$$

wobei $H_1 = \{Mat \in H \mid Mat \equiv Id \bmod \mathfrak{p}\}$ und die zweite Abbildung die Reduktion modulo $\mathfrak{p}$ ist. Da offensichtlich $|H_1| = (q^n)^{r^2(e-1)}$ gilt, ergibt sich für $|H| = |H_1| \cdot |Aut((A/\mathfrak{p})^r)|$ die behauptete Formel. □

Mit Hilfe dieses Lemmas können wir nun $|Aut(M)|$ berechnen.

3.3.4 Satz:
Sei $M = \prod_{i=1}^{k}(A/\mathfrak{p}^{e_i})^{r_i}$ ein endlicher $\mathfrak{p}$-primärer Modul in Standarddarstellung, d.h. $k \geq 0$, $e_1 > e_2 > \ldots > e_k > 0$, $r_i > 0$. Die Kardinalität der Automorphismengruppe von M ist

$$|Aut(M)| = \left(\prod_{i=1}^{k}\left(\prod_{j=1}^{r_i}(1-(q^n)^{-j})\right)\right)\left(\prod_{1\leq i,j\leq k}(q^n)^{min(e_i,e_j)r_ir_j}\right).$$

Beweis: Wir müssen alle Matrizen Mat der Form

$$\begin{pmatrix} \boxed{A_1} & B_{1,2} & B_{1,3} & \cdots & B_{1,k} \\ C_{2,1} & \boxed{A_2} & B_{1,3} & \cdots & B_{2,k} \\ C_{3,1} & C_{3,2} & \boxed{A_3} & \cdots & B_{2,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{k,1} & C_{k,2} & C_{k,3} & \cdots & \boxed{A_k} \end{pmatrix} \begin{matrix} \}r_1 \\ \}r_2 \\ \}r_3 \\ \vdots \\ \}r_k \end{matrix}$$

abzählen, für die gilt, dass A_i eine invertierbare $r_i \times r_i$-Matrix mit Einträgen in $A/\mathfrak{p}^{e_i}$, $B_{i,j}$ eine $r_i \times r_j$-Matrix mit Einträge in $A/\mathfrak{p}^{e_j}$ und $C_{i,j}$ eine $r_i \times r_j$-Matrix mit Einträgen in $A/\mathfrak{p}^{e_i}$ ist.
Nach dem vorangegangenen Lemma gibt es $(q^n)^{r^2e}\prod_{i=1}^{r}(1-(q^n)^{-i})$ Möglichkeiten für A_i.
Für $B_{i,j}$ haben wir $(q^n)^{e_jr_ir_j}$ Möglichkeiten und für $C_{i,j}$ haben wir $(q^n)^{e_ir_ir_j}$ Möglichkeiten. Man beachte, dass im ersten Fall immer $i < j$ ($\Leftrightarrow e_i > e_j$) und im zweiten Fall immer $i > j$ ($\Leftrightarrow e_i < e_j$) gilt. Für alle Paare (i,j) mit $i \neq j$ haben wir somit $(q^n)^{min(e_i,e_j)r_ir_j}$ Möglichkeiten. Zusammengefasst erhalten wir

$$\begin{aligned} |Aut(M)| &= \prod_{i=1}^{k}\left((q^n)^{(r_i)^2e_i}\prod_{j=1}^{r_i}(1-(q^n)^{-j})\right)\left(\prod_{1\leq i,j\leq k, i\neq j}(q^n)^{min(e_i,e_j)r_ir_j}\right) \\ &= \left(\prod_{i=1}^{k}\left(\prod_{j=1}^{r_i}(1-(q^n)^{-j})\right)\right)\left(\prod_{1\leq i,j\leq k}(q^n)^{min(e_i,e_j)r_ir_j}\right). \end{aligned}$$

□

3.4 Das lokale Cohen-Lenstra-Wahrscheinlichkeitsmaß

3.4.1 Definition:
Das lokale Cohen-Lenstra-Maß ist das Maß auf der abzählbaren Menge $\mathcal{M}_\mathfrak{p}$ aller $\mathfrak{p}$-Moduln, das für alle einelementigen Teilmengen $\{M\} \subset \mathcal{M}_\mathfrak{p}$ wie folgt definiert wird:

$$w(\{M\}) = \frac{1}{|Aut(M)|}.$$

Das (lokale) Cohen-Lenstra-Wahrscheinlichkeitsmaß P ist das Wahrscheinlichkeitsmaß auf $\mathcal{M}_\mathfrak{p}$, das wir durch Skalierung von w erhalten:

$$P(N) := \frac{w(N)}{w(\mathcal{M}_\mathfrak{p})}$$

für Teilmengen N von $\mathcal{M}_\mathfrak{p}$. Dafür benutzen wir, dass $w(\mathcal{M}_\mathfrak{p}) = \sum_{M \in \mathcal{M}_\mathfrak{p}} w(\{M\})$ endlich ist. Dies wird durch den folgenden Satz garantiert.

3.4.2 Satz:
Das Cohen-Lenstra-Maß aller $\mathfrak{p}$-Moduln ist

$$w(\mathcal{M}_\mathfrak{p}) = \prod_{i=1}^{\infty}(1-(q^n)^{-i})^{-1}.$$

Beweis: (Vgl. [Hal38]) Sei $M \cong \underline{\lambda} = (\underline{\lambda}_1, \ldots, \underline{\lambda}_l) \in \mathcal{M}_\mathfrak{p}$ und sei $\underline{\mu} = (\underline{\mu}_1, \ldots, \underline{\mu}_m)$ die zugehörige konjugierte Partition. Dann ist der Faktor $A/\mathfrak{p}^i$ genau $(\underline{\mu}_i - \underline{\mu}_{i+1})$-mal in M enthalten. Nach Satz 3.3.4 erhalten wir

$$\begin{aligned} |Aut(M)| &= \left(\prod_{i=1}^{m}\left(\prod_{j=1}^{\underline{\mu}_i-\underline{\mu}_{i+1}}(1-(q^n)^{-j})\right)\right) \\ &\quad \cdot \left(\prod_{1\le i,j\le m}(q^n)^{min(i,j)(\underline{\mu}_i-\underline{\mu}_{i+1})(\underline{\mu}_j-\underline{\mu}_{j+1})}\right) \\ &= \left(\prod_{i=1}^{m}\left(\prod_{j=1}^{\underline{\mu}_i-\underline{\mu}_{i+1}}(1-(q^n)^{-j})\right)\right)\left(\prod_{1\le i,j\le m}(q^n)^{\underline{\mu}_i^2}\right). \end{aligned}$$

Zwischenbehauptung: $\sum_{1\le i\le m}\underline{\mu}_i^2 = \sum_{1\le i,j\le m} min(i,j)(\underline{\mu}_i - \underline{\mu}_{i+1})$.
Diese Gleichheit bekommen wir durch Zählen der Anzahl der Terme $\underline{\mu}_i\underline{\mu}_i$ für jedes Paar (i,j). Es ist leicht einzusehen, dass die Anzahl der auftretenden Summen sich für $i \neq j$ zu 0 und sonst zu 1 aufsummiert.
Durchläuft $\underline{\lambda}$ alle Elemente von $\mathcal{M}_\mathfrak{p}$, so gilt dies auch für $\underline{\mu}$.

Sei $a(s)$ die Anzahl der Partitionen der Länge s und $M_{\underline{\mu}}$ der zu $\underline{\mu}$ assoziierte Modul. Da die Gleichheit $\sum_{s=0}^{\infty} a(s)(q^n)^{-s} = \prod_{i\geq 1}(1-(q^n)-i)^{-1}$ nach (2.1) erfüllt ist, müssen wir also zeigen, dass folgende Gleichheit gilt:

$$\sum_{s=0}^{\infty} a(s)(q^n)^{-s} = \sum_{s=0}^{\infty} \sum_{\substack{\underline{\mu}\in\mathcal{M}_{\mathfrak{p}},\\ \text{Länge}(\underline{\mu})=s}} Aut(M_{\underline{\mu}})^{-1}.$$

Zur Vereinfachung verwenden wir die Substitution $q_o = (q^n)^{-1}$ und für die linke Seite der Gleichung benutzen wir die Identität für Potenzreihen (2.1)

$$\sum_{s=0}^{\infty} a(s){q_o}^s = \sum_{s=0}^{\infty} {q_o}^s \prod_{i=1}^{s}(1-{q_o}^i)^{-1}.$$

Wir müssen nur zeigen, dass für jedes $m \geq 0$ die folgende q-Reihen-Identität gilt:

$$ {q_o}^m \prod_{i=1}^{m}(1-{q_o}^i)^{-1} = \sum_{\substack{\underline{\mu}\in\mathcal{M}_{\mathfrak{p}},\\ \text{Länge}(\underline{\mu})=m}} \left(\prod_{i=1}^{m}\left(\prod_{j=1}^{\underline{\mu}_i-\underline{\mu}_{i+1}}(1-{q_o}^{-j})\right)\right)\left(\prod_{1\leq i,j\leq m} {q_o}^{{\underline{\mu}_i}^2}\right). \tag{3.1}$$

Das Ergebnis folgt durch Ersetzen von q_o durch $(q^n)^{-1}$ und Summation über alle m. Wir beweisen diese Gleichheit, indem wir beide Seiten als erzeugende Funktionen von Partitionen einer bestimmten Art interpretieren. Für die linke Seite gilt: Der Koeffizient von ${q_o}^{N+m}$ ist die Anzahl der Partitionen von N, deren größter Teil höchstens m ist. Zu einer solchen Partition $\underline{\nu}$ definieren wir eine Partition der Form $\underline{\mu}$ der rechten Seite wie folgt:
Betrachte das Young-Diagramm D von $\underline{\nu}$. Sei $\underline{\mu}_1$ die größte ganze Zahl, sodass der Punkt $(\underline{\mu}_1, \underline{\mu}_1)$ zu D gehört. Wir betrachten ihn als den unteren rechten Eckpunkt des größten Quadrates, das in D eingezeichnet werden kann. Nun definieren wir rekursiv $\underline{\mu}_i$ als größte ganze Zahl, sodass $(\underline{\mu}_1 + \underline{\mu}_2 + \ldots + \underline{\mu}_i, \underline{\mu}_i)$ zu D gehört. Somit ist $\underline{\mu}_i$ die Größe des größten Quadrates, das unter die vorangegangenen Quadrate in D passt. Sei $L := N - \underline{\mu}_1^2 - \underline{\mu}_2^2 + \ldots$, dann existieren genau L Blöcke von D außerhalb der erwähnten Quadrate. Wir unterteilen diese Blöcke wie folgt: Definiere L_i als die Anzahl der Blöcke von D zur Rechten des i-ten Quadrates, d.h. die Anzahl der Blöcke $(x, y) \in D$, für die gilt

$$\underline{\mu}_1 + \underline{\mu}_2 + \ldots + \underline{\mu}_{i-1} < x \leq \underline{\mu}_1 + \underline{\mu}_2 + \ldots + \underline{\mu}_i$$

und

$$\underline{\mu}_i < y.$$

Dann gilt offensichtlich $L = L_1 + \ldots + L_m$. Des Weiteren bildet der Block L_i eine Partition der Höhe kleiner oder gleich $\underline{\mu}_i$ und Breite von höchstens $\underline{\mu}_{i-1} - \underline{\mu}_i$ (wäre diese Breite größer, so könnte $\underline{\mu}_{i-1}$ größer gewählt werden).
Andererseits ist es klar, dass wir unsere Konstruktion umkehren können: Sei ein

Term ${q_o}^N$ auf der rechten Seite gegeben, spezifiziert durch die Wahl von $\underline{\mu}$ und der Zahlen L_i. Diese werden so gewählt, dass $L_1 + \ldots + L_m = N - \underline{\mu}_1^2 - \ldots - \underline{\mu}_m^2$ gilt und die Partitionen von L_i der Höhe kleiner oder gleich $\underline{\mu}_i$ sind und eine Breite von höchstens $\underline{\mu}_{i-1} - \underline{\mu}_i$ haben. Dann können wir das Young-Diagramm D und somit die Partition $\underline{\nu}$ rekonstruieren.
Wir bezeichnen mit $\psi_{k,b}(q_o)$ die erzeugende Funktion für Partitionen mit höchstens k Termen, die alle kleiner gleich b sind. Wir haben gezeigt, dass

$$ {q_o}^m \prod_{i=1}^{m} (1 - {q_o}^i)^{-1} = \sum_{\substack{\underline{\mu} \in \mathcal{M}_{\mathfrak{p}}, \\ \text{Länge}(\underline{\mu}) = m}} \left(\prod_{i=1}^{m} \psi_{\underline{\mu}_{i+1}, \underline{\mu}_i - \underline{\mu}_{i+1}}(q_o) \right) \left(\prod_{1 \le i,j \le m} (q_o{}^n)^{{\underline{\mu}_i}^2} \right), $$

wobei wir $\underline{\mu}_0 = \infty$ und $\underline{\mu}_{m+1} := 0$ setzen. Wie wir bereits in Satz 2.3.1 gesehen haben, ist für endliche k und b

$$ \psi_{k,b}(q_0) = \frac{\prod_{i=1}^{k+b}(1 - {q_o}^i)}{\prod_{i=1}^{k}(1 - {q_o}^i) \prod_{i=1}^{b}(1 - {q_o}^i)} $$

und

$$ \psi_{\infty,b}(q_0) = \frac{1}{\prod_{i=1}^{b}(1 - {q_o}^i)}. $$

Durch Einsetzen dieser Formeln erhalten wir (3.1), dies beendet den Beweis. □

3.4.3 Bemerkung:

1. Die Menge $\mathcal{M}_{\mathfrak{p}}$ wird mit diesem Wahrscheinlichkeitsmaß P zu einem Wahrscheinlichkeitsraum.

2. Als Maß sind P und w σ-additiv. Wie wir später sehen werden, ist dies in der globalen Situation nicht mehr der Fall.

3.5 Beschreibung eines zufälligen $\mathfrak{p}$-Moduls durch Erzeugende und Relationen

Eine Relation in einem Modul ist eine Gleichung der Form $a_1 e_1 + \ldots + a_r e_r = 0$, wobei e_i die Erzeugenden sind und die Koeffizienten a_i in $A_{\mathfrak{p}}$ liegen. Die von uns betrachteten $\mathfrak{p}$-Moduln können auch als endliche $A_{\mathfrak{p}}$-Moduln aufgefasst werden, sodass wir hier nur Moduln über $A_{\mathfrak{p}}$ betrachten müssen. Da wir r Relationen brauchen, benötigen wir eine $r \times r$-Matrix Mat mit Elementen in $A_{\mathfrak{p}}$. Der erzeugte Modul M ist dann $coker(Mat) := A_{\mathfrak{p}}^r / im(Mat)$. Um einen $\mathfrak{p}$-Modul zu erhalten, muss Mat vollen Rang haben. Als eine kompakte Gruppe kann $A_{\mathfrak{p}}$ mit einem Haar-Maß versehen werden. Dieses kann normiert werden, sodass wir ein zugehöriges Wahrscheinlichkeitsmaß erhalten. Folglich erhält auch $A_{\mathfrak{p}}^{r \times r}$ ein Haar-Wahrscheinlichkeitsmaß, welches im Folgenden mit Pr bezeichnet wird,

und wir können eine zufällige Matrix mit Berücksichtigung dieses Wahrscheinlichkeitsmaßes wählen.
Zunächst werden wir ein paar Fakten über Modulhomomorphismen zusammentragen.

3.5.1 Lemma:
Seien $e' > e \geq 0$. Die Anzahl der $r \times r$-Matrizen Mat über $A/\mathfrak{p}^{e'}$, für die gilt $\left(\mathfrak{p}^e\left(A/\mathfrak{p}^{e'}\right)\right)^r \not\subseteq im(Mat)$, ist kleiner oder gleich

$$(q^n)^{r^2e'+r^2-re}\prod_{s=1}^{r}(1-(q^n)^{-s}).$$

Beweis: Eine solche Matrix sei gegeben. Dann müssen wir den Homomorphismus bilden, der durch Mat verknüpft mit einem Automorphismus φ von $A/\mathfrak{p}^e$ definiert ist und eingeschränkt auf $A/\mathfrak{p}^{e-1}$ die Identität ergibt. Damit erreichen wir, dass $(0,0,\ldots,0,p^e) \not\subseteq im(\varphi \circ Mat)$. Präziser ausgedrückt nehmen wir einen Automorphismus φ mod $\mathfrak{p}^e$ und erweitern ihn zu einen Automorphismus mod $\mathfrak{p}^{e'}$. Dann ist

$$(im(\varphi \circ Mat)) \subseteq \underbrace{A/\mathfrak{p}^{e'} \times A/\mathfrak{p}^{e'} \times A/\mathfrak{p}^{e'} \times \ldots \times A/\mathfrak{p}^{e'}}_{r-1} \times p^{e+1}A/\mathfrak{p}^{e'}.$$

Wir haben $(q^n)^{r(re'-e)}$ Möglichkeiten für $\varphi \circ Mat$. Bleibt noch die Frage zu beantworten, wie viele Möglichkeiten wir für φ haben. Offensichtlich können wir statt φ einen Automorphismus von $(A/\mathfrak{p})^r$ wählen. Nach Lemma 3.3.4 erhalten wir

$$(q^n)^{r^2}\prod_{i=1}^{r}(1-(q^n)^{-i})$$

Möglichkeiten für φ. Die Wahl von φ muss nicht eindeutig sein, aber in jedem Fall haben wir höchstens

$$(q^n)^{r(re'-e)}(q^n)^{r^2}\prod_{i=1}^{r}(1-(q^n)^{-i}) = (q^n)^{r^2e'+r^2-re}\prod_{s=1}^{r}(1-(q^n)^{-s})$$

viele Matrizen mit $\left(\mathfrak{p}^eA/\mathfrak{p}^{e'}\right)^r \not\subseteq im(Mat)$. □

3.5.2 Lemma:
Sei M ein endlicher $\mathfrak{p}$-primärer A-Modul mit $N := ord(M)$ und $r := rk(M)$. Sei $m \geq r$, dann gilt:

$$|\left\{\Gamma \subseteq A_{\mathfrak{p}}^m | A_{\mathfrak{p}}^m/\Gamma \cong M\right\}| = \frac{N^m}{|Aut(M)|}\left(\prod_{i=m-r+1}^{m}(1-(q^n)^{-i})\right).$$

Hierbei durchläuft Γ alle Untermoduln von $A_{\mathfrak{p}}^m$.

Beweis: [CL84], Theorem 3.1 □

3.5.3 Satz (Friedman-Washington):
Für eine zufällig gewählte Matrix $Mat \in A_{\mathfrak{p}}^{m\times m}$ gilt:

1. *$Pr(Mat$ hat vollen Rang$) = 1$ für alle $m > 0$.*
2. *Für einen endlichen $\mathfrak{p}$-primären A-Modul M ist*

$$Pr(coker(Mat) \cong M) \to P(M) \text{ für } m \to \infty,$$

wobei P das Cohen-Lenstra-Wahrscheinlichkeitsmaß ist. Man beachte, dass die Wahrscheinlichkeit auf der linken Seite implizit von m abhängt.

Beweis: 1. Eine Matrix Mat hat genau dann vollen Rang, wenn ein e existiert, so dass gilt: $(\mathfrak{p}^e A_{\mathfrak{p}})^m \subseteq im(Mat)$. Für jedes $e' > e$ ist dies äquivalent zu der Aussage, dass für die Reduktion von Mat modulo $\mathfrak{p}^{e'}$ gilt: $(\mathfrak{p}^e A/\mathfrak{p}^{e'})^m \subseteq im(Mat \bmod \mathfrak{p}^{e'})$. In anderen Worten erhalten wir für alle $e \geq 0$ und alle $e' > e$:

$$\begin{aligned} Pr\left(Mat \text{ hat vollen Rang }\right) &\geq Pr\left((\mathfrak{p}^e A_{\mathfrak{p}})^m \subseteq im(Mat)\right) \\ &= Pr\left((\mathfrak{p}^e A/\mathfrak{p}^{e'})^m \subseteq im(Mat \bmod \mathfrak{p}^{e'})\right). \end{aligned}$$

Da die Reduktion modulo $\mathfrak{p}^{e'}$ mit dem Haar-Maß kompatibel ist, können wir die letzte Wahrscheinlichkeit durch Matrizenzählen berechnen. Nach Lemma 3.5.1 ist die Anzahl der Matrizen mod $\mathfrak{p}^{e'}$, die die Bedingung $(\mathfrak{p}^e A/\mathfrak{p}^{e'})^m \subseteq im(Mat \bmod \mathfrak{p}^{e'})$ nicht erfüllen,

$$(q^n)^{m^2+m^2e'-me} \prod_{s=1}^{m} (1-(q^n)^{-s}).$$

Indem wir diese Anzahl durch die Anzahl $(q^n)^{m^2e'}$ aller Matrizen in $(A/\mathfrak{p}^{e'})^{m\times m}$ dividieren, erhalten wir die Wahrscheinlichkeit dafür, dass eine Matrix in $(A/\mathfrak{p}^{e'})^{m\times m}$ diese Eigenschaft hat:

$$Pr\left(\begin{array}{c} Mat \in (A/\mathfrak{p}^{e'})^{m\times m} \text{ erfüllt} \\ (\mathfrak{p}^e A/\mathfrak{p}^{e'})^m \not\subseteq im(Mat) \end{array}\right) \leq (q^n)^{m^2-me} \prod_{s=1}^{m} (1-(q^n)^{-s}).$$

Insgesamt erhalten wir für alle $e' > e \geq 0$:

$$\begin{aligned} Pr\left(\begin{array}{c} Mat \in (A/\mathfrak{p})^{m\times m} \\ \text{hat vollen Rang} \end{array}\right) &\geq Pr\left(\begin{array}{c} Mat \in (A/\mathfrak{p})^{m\times m} \\ \text{mit } (\mathfrak{p}^e A_{\mathfrak{p}})^m \subseteq im(Mat) \end{array}\right) \\ &\geq 1-(q^n)^{m^2-me} \prod_{s=1}^{m} (1-(q^m)^{-s}) \\ &\overset{e\to\infty}{\to} 1. \end{aligned}$$

2. Wir zeigen, dass für $r := rk(M) \leq m$ gilt:

$$\begin{aligned} Pr(coker(Mat) \cong M) &= \frac{1}{|Aut(M)|}\left(\prod_{i=1}^{m}(1-(q^n)^{-i})\right) \\ &\quad \cdot \left(\prod_{i=m-r+1}^{m}(1-(q^n)^{-i})\right). \end{aligned}$$

Die Behauptung folgt dann mit 3.4.2 durch Bilden des Grenzwertes $m \to \infty$.
Sei Γ ein Untermodul von $A_{\mathfrak{p}}^m$, sodass $A_{\mathfrak{p}}^m/\Gamma \cong M$ gilt. Wir berechnen die Wahrscheinlichkeit für das Ereignis $im(Mat) \cong \Gamma$.
Sei Mat_0 eine Matrix mit $im(Mat_0) = \Gamma$. Dann haben wir die Identifikation $\{Mat \,|\, im(Mat) = \Gamma\} = Mat_0 \cdot GL(m, A_{\mathfrak{p}})$. Nach den Eigenschaften des Haar-Maßes folgt:

$$\begin{aligned} Pr(im(Mat) = \Gamma) &= |det(Mat_0)|^{-m} \cdot Pr(Mat \in GL(m, A_{\mathfrak{p}})) \\ &= \frac{Pr(Mat \text{ ist invertierbar })}{ord(M)^m}. \end{aligned}$$

Da eine Matrix genau dann invertierbar ist, wenn ihre Reduktion modulo $\mathfrak{p}$ invertierbar ist, erhalten wir

$$\begin{aligned} Pr(Mat \text{ ist invertierbar }) &= \frac{|GL(m, A/\mathfrak{p})|}{|(A/\mathfrak{p})^{m\times m}|} \\ &\overset{3.3.4}{=} \frac{(q^n)^{m^2}\prod_{i=1}^{m}(1-(q^n)^{-i})}{(q^n)^{m^2}} \\ &= \prod_{i=1}^{m}(1-(q^n)^{-i}). \end{aligned}$$

Insbesondere ist diese Wahrscheinlichkeit unabhängig von Γ. Deshalb gilt:

$$\begin{aligned} Pr(coker(Mat) \cong M) &= |\{\Gamma \subseteq A^m | A_{\mathfrak{p}}/\Gamma = M\}| \cdot Pr(im(Mat) = \Gamma) \\ &\overset{3.5.2}{=} \frac{(ord(M))^m}{|Aut(M)|}\left(\prod_{i=m-r+1}^{m}(1-(q^n)^{-i})\right) \\ &\quad \cdot \left(\frac{\prod_{i=1}^{m}(1-(q^n)^{-i})}{(ord(M))^m}\right) \\ &= \frac{1}{|Aut(M)|}\left(\prod_{i=1}^{m}(1-(q^n)^{-i})\right) \\ &\quad \cdot \left(\prod_{i=m-r+1}^{m}(1-(q^n)^{-i})\right). \end{aligned}$$

□

3.6 Einige Beispiele

3.6.1 Beispiel:
Wir berechnen die Wahrscheinlichkeit dafür, dass ein $\mathfrak{p}$-Modul der triviale Modul ist. Da $w(0) = 1$, erhalten wir:

$$P(0) = \prod_{i=1}^{\infty}(1 - (q^n)^{-i}) = 1 - (q^n)^{-1} - (q^n)^{-2} + (q^n)^{-5} - (q^n)^{-7} - (q^n)^{-12} \ldots .$$

Unter Benutzung von q-Reihen erhalten wir weitere Wahrscheinlichkeiten. Zur Vereinfachung verwenden wir die Substitution $q_o = (q^n)^{-1}$.

3.6.2 Beispiel:
Die Wahrscheinlichkeit, dass ein zufällig gewählter $\mathfrak{p}$-primärer A-Modul zyklisch ist, ist

$$\begin{aligned}
P(M \text{ zyklisch}) &= \frac{1}{w(\mathcal{M}_{\mathfrak{p}})} \sum_{M \text{ zyklisch}} w(M) \\
&= \left(\prod_{i=1}^{\infty}(1 - {q_o}^i)\right)\left(\sum_{e=1}^{\infty}\frac{{q_o}^e}{1-q_o} + 1\right) \\
&= \left(\prod_{i=1}^{\infty}(1 - {q_o}^i)\right)\frac{1}{(1-q_o)}\left(\sum_{e=0}^{\infty}\frac{{q_o}^e}{1-q_o} - q_o\right) \\
&= \left(\prod_{i=1}^{\infty}(1 - {q_o}^i)\right)\frac{1}{(1-q_o)^2}\left(1 - q_o + {q_o}^2\right) \\
&= \frac{\left(1 - q_o + {q_o}^2\right)}{(1-q_o)}\left(\prod_{i=2}^{\infty}(1 - {q_o}^i)\right). \\
&= 1 - {q_o}^4 - {q_o}^5 - 2{q_o}^6 - {q_o}^7 - {q_o}^8 + {q_o}^{10} + 2{q_o}^{11} \ldots
\end{aligned}$$

Mit den Mitteln der Statistik können wir weitere interessante Eigenschaften berechnen, wie zum Beispiel die Varianz $Var(X)$. Hierbei ist E der Erwartungswert und X diejenige Zufallsvariable, für die gilt:

$$X(M) = \begin{cases} 1, M \text{ zyklisch} \\ 0 \text{ sonst.} \end{cases}$$

Wir berechnen:

$$\begin{aligned}
Var(X) &= E(X^2) - (E(X))^2 \\
&= \frac{\left(1 - q_o + {q_o}^2\right)}{(1-q_o)} \left(\prod_{i=2}^{\infty}(1-{q_o}^i)\right) + \left(\frac{\left(1 - q_o + {q_o}^2\right)}{(1-q_o)} \left(\prod_{i=2}^{\infty}(1-{q_o}^i)\right)\right)^2 \\
&= \frac{\left(1 - q_o + {q_o}^2\right)}{(1-q_o)} \left(\prod_{i=2}^{\infty}(1-{q_o}^i)\right) + \frac{\left(1 - q_o + {q_o}^2\right)^2}{(1-q_o)^2} \left(\prod_{i=2}^{\infty}(1-{q_o}^i)^2\right) \\
&= (1 - {q_o}^4 - {q_o}^5 - 2{q_o}^6 - {q_o}^7 - {q_o}^8 + {q_o}^{10} + 2{q_o}^{11} \ldots) \\
&\quad -(1 - 2{q_o}^4 - 2{q_o}^5 - 2{q_o}^6 - 2{q_o}^7 - {q_o}^8 + 2{q_o}^9 + 7{q_o}^{10} + 10{q_o}^{11} \ldots) \\
&= {q_o}^4 + {q_o}^5 + {q_o}^7 - 2{q_o}^9 - 6{q_o}^{10} - 8{q_o}^{11} \ldots .
\end{aligned}$$

3.6.3 Beispiel:
Für die Wahrscheinlichkeit, dass ein zufällig gewählter $\mathfrak{p}$-primärer A-Modul M elementar ist (d.h., dass M direkte Summe von r Kopien $A/\mathfrak{p}$ mit $r \in \mathbb{N}$ ist), erhalten wir mit Hilfe der Rogers-Ramanujan-Identität 2.3.2:

$$\begin{aligned}
P(M \text{ elementar}) &= \frac{1}{w(\mathcal{M}_{\mathfrak{p}})} \sum_{M \text{ elementar}} w(M) \\
&= \left(\prod_{i=1}^{\infty}\left(1-{q_o}^i\right)\right) \sum_{r=0}^{\infty} \frac{{q_o}^{r^2}}{\prod_{s=1}^{r}(1-{q_o}^s)} \\
&\overset{(2.3.2)}{=} \left(\prod_{i=1}^{\infty}\left(1-{q_o}^i\right)\right) \left(\prod_{s=1}^{\infty} \frac{1}{(1-{q_o}^{5s-4})(1-{q_o}^{5s-1})}\right) \\
&= 1 - {q_o}^2 - {q_o}^3 + {q_o}^9 + {q_o}^{11} \ldots
\end{aligned}$$

Auch hier können wir wieder die Varianz berechnen. Es sei Y diejenige Zufallsvariable mit

$$Y(M) = \begin{cases} 1, M \text{ elementar} \\ 0 \text{ sonst.} \end{cases}$$

Es gilt:

$$\begin{aligned}
Var(Y) &= E(Y^2) - (E(Y))^2 \\
&= \left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)\left(\prod_{s=1}^{\infty}\frac{1}{(1-{q_o}^{5s-4})(1-{q_o}^{5s-1})}\right) \\
&\quad -\left(\left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)\left(\prod_{s=1}^{\infty}\frac{1}{(1-{q_o}^{5s-4})(1-{q_o}^{5s-1})}\right)\right)^2 \\
&= \left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)\left(\prod_{s=1}^{\infty}\frac{1}{(1-{q_o}^{5s-4})(1-{q_o}^{5s-1})}\right) \\
&\quad -\left(\prod_{i=1}^{\infty}(1-{q_o}^i)^2\right)\left(\prod_{s=1}^{\infty}\frac{1}{(1-{q_o}^{5s-4})^2(1-{q_o}^{5s-1})^2}\right) \\
&= (1-{q_o}^2-{q_o}^3+{q_o}^9\ldots) \\
&\quad -(1-2{q_o}^2-2{q_o}^3+{q_o}^4+2{q_o}^5+{q_o}^6+2{q_o}^9\ldots) \\
&= {q_o}^2+{q_o}^3-{q_o}^4-2{q_o}^5-{q_o}^6-{q_o}^9\ldots
\end{aligned}$$

3.6.4 Beispiel:
Man erhält für die Wahrscheinlichkeit, dass eine Gruppe zyklisch und elementar ist:

$$\begin{aligned}
P(M \text{ elementar und zyklisch}) &= \left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)\left(1+\frac{q_o}{1-q_o}\right) \\
&= \left(\prod_{i=2}^{\infty}(1-{q_o}^i)\right) \\
&= 1-{q_o}^2-{q_o}^3-{q_o}^4+{q_o}^7+{q_o}^8+{q_o}^9\ldots
\end{aligned}$$

Mit Hilfe der oben berechneten Formeln können wir nun auch die Kovarianz der

beiden Ereignisse „elementar“ und „zyklisch“ berechnen:

$$\begin{aligned}
Cov(X,Y) &= E(XY) - E(X)E(Y) \\
&= \left(\prod_{i=2}^{\infty}\left(1-{q_o}^i\right)\right) - \frac{\left(1-q_o+{q_o}^2\right)}{(1-q_o)}\left(\prod_{i=2}^{\infty}(1-{q_o}^i)\right) \\
&\quad \cdot \left(\prod_{i=1}^{\infty}\left(1-{q_o}^i\right)\right)\left(\prod_{s=1}^{\infty}\frac{1}{(1-{q_o}^{5s-4})(1-{q_o}^{5s-1})}\right) \\
&= \left(1+\frac{q_o}{1-q_o}\right)\left(\prod_{i=2}^{\infty}\left(1-{q_o}^i\right)\right) - \left(1-q_o+{q_o}^2\right) \\
&\quad \cdot \left(\prod_{i=2}^{\infty}\left(1-{q_o}^i\right)\right)^2\left(\prod_{s=1}^{\infty}\frac{1}{(1-{q_o}^{5s-4})(1-{q_o}^{5s-1})}\right) \\
&= (1-{q_o}^2-{q_o}^3-{q_o}^4+{q_o}^7+{q_o}^8+{q_o}^9\ldots) \\
&\quad -(1-{q_o}^4-{q_o}^5-2{q_o}^6-{q_o}^7-{q_o}^8\ldots)(1-{q_o}^2-{q_o}^3+{q_o}^9\ldots) \\
&= {q_o}^5+{q_o}^6-{q_o}^8-3{q_o}^9\ldots
\end{aligned}$$

3.6.5 Bemerkung:
Das Ausschlaggebende dieser Rechnung ist das Vorzeichen des ersten Terms, in unserem Term haben wir ein positives Ergebnis. Dies gibt an, dass die beiden Ereignisse positiv korreliert sind. Somit tendieren zyklische Moduln dazu, auch elementar zu sein und elementare Moduln tendieren dazu, zyklisch zu sein.

3.6.6 Beispiel:
Ein weiterer interessanter Fakt ist der folgende: Wenn wir einen Modul M vorgegeben haben, können wir die Wahrscheinlichkeit berechnen, mit der ein zufälliges Element x den Modul M erzeugt.
Dazu definieren wir uns die Funktion $f : \mathcal{M}_{\mathfrak{p}} \to [0,1]$ mit

$$f(M) = \frac{\text{Anzahl der Elemente, die } M \text{ erzeugen}}{|M|}.$$

Für den Fall, dass M zyklisch ist, erhält man

$$f(M) = \begin{cases} 1 \text{ falls } M = \{0\} \\ 1-q_0 \text{ falls } \{0\} \neq M \text{ zyklisch} \\ 0, \text{ sonst} \end{cases}.$$

Somit erhalten wir für die Wahrscheinlichkeit, dass ein zufällig gewähltes Ele-

ment x den zufälligen Modul M erzeugt:

$$\begin{aligned} P(x \text{ erzeugt } M) &= \left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)\left(1+\sum_{e=1}^{\infty}\frac{(1-q_0)\,{q_o}^e}{1-q_o}\right) \\ &= \left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)\sum_{e=0}^{\infty}{q_o}^e \\ &= \left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right)(1-q_0)^{-1} \\ &= \left(\prod_{i=2}^{\infty}(1-{q_o}^i)\right) \\ &= 1-{q_o}^2-{q_o}^3-{q_o}^4+{q_o}^7+{q_o}^8\ldots. \end{aligned}$$

3.6.7 Bemerkung:
Diese Wahrscheinlichkeit stimmt mit der Wahrscheinlichkeit überein, dass ein Modul zyklisch und elementar ist.

3.6.8 Beispiel:
Wir berechnen die Wahrscheinlichkeit, dass ein Modul Rang 2 hat. Bei dieser Fragestellung müssen wir zwei verschiedene Fälle betrachten, entsprechend der möglichen Modulstrukturen $M=(A/\mathfrak{p}^e)^2$ und $M=A/\mathfrak{p}^{e_1}\times A/\mathfrak{p}^{e_2}$.

$$\begin{aligned} P(rk(M)=2) &= \frac{1}{w(\mathcal{M}_{\mathfrak{p}})}\sum_{M \text{ hat } rk(M)=2} w(M) \\ &= \left(\sum_{e=1}^{\infty}\frac{{q_o}^{4e}}{(1-q_o)(1-{q_o}^2)}+\sum_{e_1=1}^{\infty}\sum_{e_2=e_2+1}^{\infty}\frac{{q_o}^{e_1+3e_2}}{(1-{q_o}^2)}\right) \\ &\quad\cdot\left(\prod_{i=1}^{\infty}\left(1-{q_o}^i\right)\right) \\ &= \left(\frac{{q_o}^4}{(1-q_o)(1-{q_o}^2)(1-{q_o}^4)}+\frac{1}{(1-q_o)^2}\sum_{e_2=1}^{\infty}{q_o}^{3e_2}{q_o}^{e_2+1}\frac{1}{(1-q_o)}\right) \\ &\quad\cdot\left(\prod_{i=1}^{\infty}\left(1-{q_o}^i\right)\right) \\ &= \left(\frac{{q_o}^4}{(1-q_o)(1-{q_o}^2)(1-{q_o}^4)}+\frac{{q_o}^5}{(1-q_o)^3(1-{q_o}^4)}\right) \\ &\quad\cdot\left(\prod_{i=1}^{\infty}\left(1-{q_o}^i\right)\right) \end{aligned}$$

$$\begin{aligned} P(rk(M)=2) &= \left(\frac{{q_o}^4-{q_o}^5+{q_o}^5+{q_o}^6}{(1-q_o)^2(1-{q_o}^2)(1-{q_o}^4)}\right)\left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right) \\ &= \left(\frac{{q_o}^4}{(1-q_o)^2(1-{q_o}^2)^2}\right)\left(\prod_{i=1}^{\infty}(1-{q_o}^i)\right) \\ &= {q_o}^4+{q_o}^5+2{q_o}^6+{q_o}^7+{q_o}^8-{q_o}^9-2{q_o}^{10}-4{q_o}^{11}\ldots. \end{aligned}$$

Auch in diesem Fall kann man der Frage nachgehen, mit welcher Wahrscheinlichkeit zwei zufällig gewählte Elemente den Modul erzeugen.

Wir stellen fest, dass die Rechnungen schnell aufwendiger werden, wenn die Moduln kompliziertere Strukturen annehmen. Es ist möglich, auf diese Weise generelle Ergebnisse über Ordnung und Rang eines zufälligen endlichen $\mathfrak{p}$-primären A-Moduls zu erhalten, allerdings erfordert dies einen geschickten Umgang mit q-Reihen. Wie wir später sehen werden, kann man dies aber eleganter berechnen.

Kapitel 4

Zusammenhang der Cohen-Lenstra-Heuristik mit Partitionen

Notation

Im Folgenden bezeichnen:

- $|M|$ oder auch $ord(M)$ die Kardinalität einer Menge M,
- q eine Primzahlpotenz,
- $\mathbb{F}_q$ den Körper mit q Elementen,
- $A := \mathbb{F}_q[X]$ den Polynomring über dem Körper mit q Elementen,
- $\mathfrak{p}$ ein Primideal in A, erzeugt von einem normierten irreduziblen Polynom p mit Grad n,
- $\mathcal{M}_\mathfrak{p}$ die Menge aller endlichen $\mathfrak{p}$-primären A-Moduln,
- $\underline{\lambda}$ bzw. $\underline{n}$ eine Partition,
- Länge($\underline{\lambda}$) die Länge einer Partition $\underline{\lambda}$,
- $\bar{n}$ eine Derivation,
- $\mathcal{P}$ die Menge aller Partitionen,
- $w(M)$ das Cohen-Lenstra-Maß des Moduls M,
- $P(M)$ das Cohen-Lenstra-Wahrscheinlichkeitsmaß des Moduls M,

- Λ die Cohen-Lenstra-Abbildung.

Wir verwenden wieder die Substitution $q_o = (q^n)^{-1}$.
Wir haben in 3.4.2 gesehen, dass für das Maß aller $\mathfrak{p}$-Moduln gilt:

$$\sum_{\text{M ist } \mathfrak{p}\text{-Modul}} w(M) = \prod_{i=1}^{\infty} \left(1 - (q_0)^i\right)^{-1}.$$

Die Gleichung kann über die erzeugende Funktion der Partitionen erweitert werden:

$$\sum_{\text{M ist } \mathfrak{p}\text{-Modul}} w(M) = \prod_{i=1}^{\infty} \left(1 - (q_0)^i\right)^{-1} = \sum_{n \in \mathbb{N}} \sum_{\substack{\underline{n} \text{ ist eine} \\ \text{Partition von } n}} q_0^n.$$

Wir haben bereits gesehen, dass wir $\mathfrak{p}$-Moduln mit Partitionen identifizieren können, indem wir die Standarddarstellung $M = \prod_{i=1}^{k} (A/\mathfrak{p}^{e_i})^{r_i}$ als eine Partition mit r_i Summanden der Größe e_i als Einträge auffassen.
Diese Gleichheit deutet jedoch an, dass es, zusätzlich zur bisher behandelten offensichtlichen, eine tiefere Verbindung zwischen dem Cohen-Lenstra-Maß und Partitionen gibt. Als Potenzreihe in q_0 betrachtet, hat $w(M)$ nichtnegative ganze Koeffizienten. Gibt es auf der rechten Seite genauso viele Terme wie auf der linken, so könnte dies auf eine natürliche Bijektion zwischen den Termen hindeuten. Für jede Partition sollte es also einen zugehörigen $\mathfrak{p}$-Modul geben.
Wir brauchen somit eine Abbildung der Menge aller Partitionen in die Menge aller $\mathfrak{p}$-Moduln, die uns sagt, zu welcher Potenzreihe $w(M)$ der ${q_0}^n$-Term der Partition gehört.

4.1 Die Cohen-Lenstra-Abbildung

4.1.1 Definition:
Eine Abbildung $\Lambda : \mathcal{P} \to \mathcal{M}_{\mathfrak{p}}$ ist eine Cohen-Lenstra Abbildung, wenn für jeden $\mathfrak{p}$-Modul M gilt

$$w(M) = \sum_{n \geq 0} a_M(n) q_0^n,$$

wobei $a_M(n) = \left|\left\{\Lambda^{-1}(M)\right\} \cap \{\underline{n} \in \mathcal{P} | \textit{Länge}(\underline{n}) = n\}\right|$ die Anzahl der Partitionen von n ist, die auf M abgebildet werden.

Es gilt noch festzulegen, wann eine Abbildung natürlich ist. In unserem Fall gilt dies, wenn sie ordnungserhaltend ist.

4.1.2 Definition:
Sei $M = \prod_{i=1}^{k} (A/\mathfrak{p}^{e_i})^{r_i}$ ein $\mathfrak{p}$-Modul. Wir definieren die Indexmenge I_M von M als

$$I_M := \{(t_{i,s}) : 1 \leq i \leq k, 1 \leq s \leq r_i \,|\, t_{i,s} \in \mathbb{N}\}.$$

Für jeden Vektor $t \in I_M$ definieren wir den Exponenten:

$$expon(t) := \sum_{1 \le i,j \le k} min(e_i, e_j) r_i r_j + \left(\sum_{i=1}^{k} \sum_{s=1}^{r_i} st_{i,s} \right).$$

4.1.3 Bemerkung:
Das Cohen-Lenstra-Maß eines $\mathfrak{p}$-Moduls $M = \prod_{i=1}^{k} (A/\mathfrak{p}^{e_i})^{r_i}$ ist gegeben durch die Formel

$$\begin{aligned} w(M) &= \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} (1 - (q_0)^j)^{-1} \right) \right) \left(\prod_{1 \le i,j \le k} (q_0)^{min(e_i,e_j) r_i r_j} \right) \\ &= \left(\prod_{i=1}^{k} \left(\prod_{s=1}^{r_i} \sum_{t=0}^{\infty} (q_0)^{ts} \right) \right) \left(\prod_{1 \le i,j \le k} (q_0)^{min(e_i,e_j) r_i r_j} \right). \end{aligned}$$

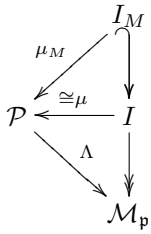
Multiplizieren wir aus, so erhalten wir ein Monom für jedes Tupel $(t_{i,s})_{1 \le i \le k, 1 \le s \le r_i}$. Damit können wir das Cohen-Lenstra-Maß von M schreiben als

$$w(M) = \sum_{t \in I_M} q_0^{expon(t)}.$$

4.1.4 Definition:
Die Menge I_M besitzt eine natürliche partielle Ordnung „$<$“: $(t_{i,s})_{1 \le i \le k, 1 \le s \le r_i} \in I_M$ ist kleiner oder gleich $(\tilde{t}_{i,s})_{1 \le i \le k, 1 \le s \le r_i} \in I_M$, wenn für alle $1 \le i \le k$ gilt: Die Sequenz $(t_{i,r_i}, t_{i,r_{i-1}} \dots t_{i,1})$ ist bezüglich der Produktordnung kleiner oder gleich $(\tilde{t}_{i,r_i}, \tilde{t}_{i,r_{i-1}} \dots \tilde{t}_{i,1})$.

4.1.5 Bemerkung:
Seien $t, \tilde{t} \in I_M$ mit $t < \tilde{t}$. Dann gilt: $expon(t) \le expon(\tilde{t})$.

4.1.6 Definition:
Wir können I_M kanonisch einbetten in die Vereinigung $I := \dot{\bigcup}_{M \in \mathcal{M}_\mathfrak{p}} I_M$ und I kanonisch in die Menge $M_\mathfrak{p}$ projizieren, indem wir die Projektion auf den Index betrachten. Im Folgenden bezeichnet μ eine bijektive Abbildung von I nach $\mathcal{P}$ und μ_M die Einschränkung von μ auf M. Dabei heißt μ_M monoton, falls für $t, t' \in I_M$ mit $t < t'$ gilt $\mu_M(t) < \mu_M(t')$ für alle $\mathfrak{p}$-Moduln M. Eine Cohen-Lenstra Abbildung $\Lambda : \mathcal{P} \to \mathcal{M}_\mathfrak{p}$ heißt ordnungserhaltend, wenn eine bijektive Abbildung $\mu : I \to \mathcal{P}$ existiert mit Länge$(\mu(t)) = expon(t)$, so dass das Diagramm



kommutiert und für alle $M \in \mathcal{M}_\mathfrak{p}$ μ_M monoton ist.

Johannes Lengler zeigt in seiner Dissertation [Len09] in Kapitel 3 die Existenz und Eindeutigkeit einer solchen ordnungserhaltenden Cohen-Lenstra-Abbildung. Er gibt dabei zwei Algorithmen an, die beide Λ definieren. Der erste Algorithmus benutzt Young-Diagramme, der zweite ist numerischer Natur. Beide erzeugen dieselbe Abbildung Λ. Wir geben im weiteren Verlauf dieses Kapitels seine Definitionen und Algorithmen wieder.

4.2 Definition mittels Young-Diagrammen

Sei $(i,j) \in \mathbb{Z}\times\mathbb{Z}$ und sei $\lambda \in \mathbb{Z}$. Der λ-Nachfolger $s_\lambda(i,j)$ von (i,j) ist der Punkt $(i+2, j-\lambda) \in \mathbb{Z}\times\mathbb{Z}$. Für jedes $N \in \mathbb{Z}\times\mathbb{Z}$ sei $s_\lambda(M)$ das Bild von M unter s_λ.

4.2.1 Algorithmus:
Sei $\underline{n} \in \mathcal{P}$.

1. Sei $N_1 \in \mathbb{N}^+ \times \mathbb{N}^+$ das Young-Diagramm von $\underline{n}$. Setze $k := 1$.
2. Sei $Q_k := \{(i,j) \in \mathbb{Z}\times\mathbb{Z} \,|\, j \geq 1\,,\, 1 \geq 2k-1\}$. Finde $\lambda_k \in \mathbb{Z}$ minimal, so dass $s_{\lambda_k}(N_k) \cap Q_k \subset N_k$.
3. Finde das maximale $i_k \in \mathbb{Z}$, so dass ein $j \in \mathbb{Z}$ existiert mit $(i_k, j) \in M_k$ und $s_{\lambda_k - 1}(i_k, j) \in Q_k \setminus N_k$.
4. Sei $C_k := \{(i,j) \in \mathbb{N}^+ \times \mathbb{N}^+ \,|\, i \leq i_k\} \setminus N_k$.
   Setze $N_{k+1} := (M_k \setminus s_{\lambda_k}(C_k)) \cap Q_{k+1}$. Erhöhe k um 1.
5. Wiederhole Schritt $2-4$, bis $N_k \cap Q_k$ leer ist.

Wenn der Algorithmus nach k Durchläufen abbricht, gibt er $\lambda_1, \ldots, \lambda_n$ aus. Setze $\Lambda(\underline{n}) := (\lambda_1, \ldots, \lambda_n) \in \mathcal{M}_\mathfrak{p}$.

4.2.2 Bemerkung:
1. Der Algorithmus bricht immer ab, sodass Λ wohldefiniert ist.
2. Die λ_i sind sortiert, $\lambda_1 \geq \ldots \geq \lambda_k > 0$, sodass das Ergebnis des Algorithmus eine Partition ist.

4.3 Numerische Definition

Bevor wir den numerischen Algorithmus betrachten können, müssen wir zunächst Derivationen definieren.

4.3.1 Definition:
Sei $\underline{n} = (\underline{n}_1, \underline{n}_2, \ldots, \underline{n}_k) \in \mathcal{P}$. Die Derivation von $\underline{n}$ ist das Tupel $\bar{n} = (\bar{n}_0, \bar{n_1}, \ldots, \bar{n}_k)$ definiert durch:

$$\bar{n}_i := \begin{cases} \underline{n}_1 - \underline{n}_2, \text{ für } i = 0 \\ \underline{n}_i - \underline{n}_{i+2}, \text{ für } 1 \leq i \leq k-2 \\ \underline{n}_i, \text{ für } i = k-1, k \end{cases} .$$

4.3.2 Lemma:
Sei $\underline{n} = (\underline{n}_1, \underline{n}_2, \ldots, \underline{n}_k) \in \mathcal{P}$ und sei $\bar{n} = (\bar{n}_0, \bar{n}_1, \ldots, \bar{n}_k)$ die zugehörige Derivation. Dann ist es möglich, $\underline{n}$ aus $\bar{n}$ mittels folgender Formel zu erhalten:

$$\underline{n}_i = \sum_{\substack{1 \leq i \leq j \leq k \\ i \equiv j \bmod 2}} \bar{n}_j .$$

Beweis: Für $i = k$ und $i = k-1$ ist die Formel offensichtlich. Für $i \leq k-2$ erhalten wir

$$\sum_{\substack{1 \leq i \leq j \leq k \\ i \equiv j \bmod 2}} \bar{n}_j = \left(\sum_{\substack{1 \leq i \leq j \leq k-2 \\ i \equiv j \bmod 2}} \underline{n}_j - \underline{n}_{j+2} \right) + \begin{cases} \underline{n}_k, \text{ für } i \equiv k \bmod 2 \\ \underline{n}_{k-1}, \text{ sonst} \end{cases} = \underline{n}_i .$$

Wir haben $\bar{n}_0$ nicht benötigt, um $\underline{n}$ zu berechnen. □

4.3.3 Lemma:
Eine Sequenz $\bar{n} = (\bar{n}_0, \bar{n}_1, \ldots, \bar{n}_k)$ ist genau dann eine Derivation, wenn folgende Bedingungen gelten:

1. $\bar{n}_{k-1} \geq \bar{n}_k > 0$.
2. $\bar{n}_i \geq 0$ *für alle* $i \geq 1$.
3. $\sum_{j=i_1}^{i_2} (-1)^{j-i_1} \bar{n}_j \geq 0$ *für alle* $1 \leq i_1 < i_2 \leq k$, $i_1 \equiv i_2 \bmod 2$ *(falls* $i_2 = k$, *entfällt die Bedingung* $i_1 \equiv i_2 \bmod 2$*).*
4. $\sum_{j=0}^{k} (-1)^j \bar{n}_j = 0$.

Beweis: Sei $\bar{n}$ die Derivation einer Partition $\underline{n} \in \mathcal{P}$. Die Aussagen 1. und 2. sind offensichtlich richtig. Des Weiteren haben wir nach Lemma 4.3.2

$$\bar{n}_0 = \underline{n}_1 - \underline{n}_2 = \left(\sum_{\substack{1 \le j \le k \\ i \equiv 1 \bmod 2}} \bar{n}_j \right) - \left(\sum_{\substack{2 \le j \le k \\ i \equiv 0 \bmod 2}} \bar{n}_j \right);$$

dies impliziert 4.
Um 3. zu beweisen, nehmen wir zur Vereinfachung $i_2 < k$ an. Der Fall $i_2 = k$ folgt analog. In der folgenden Rechnung wird ein Term $\underline{n}_j$ durch 0 ersetzt, falls er, da $j > k$ gilt, nicht existiert. Es gilt:

$$\begin{aligned}
\sum_{j=i_1}^{i_2} (-1)^{j-i_1} \bar{n}_j &= \left(\sum_{\substack{i_1 \le j \le i_2 \\ j \equiv i_1 \bmod 2}} \bar{n}_j \right) - \left(\sum_{\substack{i_1 \le j \le i_2 \\ j \not\equiv i_1 \bmod 2}} \bar{n}_j \right) \\
&= \underline{n}_{i_1} - \underline{n}_{i_2+2} - (\underline{n}_{i_1+1} - \underline{n}_{i_2+1}) \\
&= \underbrace{\underline{n}_{i_1} - \underline{n}_{i_1+1}}_{\ge 0} + \underbrace{\underline{n}_{i_2+1} - \underline{n}_{i_2+2}}_{\ge 0}. \\
&\ge 0
\end{aligned}$$

Nun zeigen wir, dass jedes Tupel mit den Eigenschaften 1.-4. eine Derivation ist. Wir definieren $\underline{n}$ wie in Lemma 4.3.2. Dann erhalten wir

$$\bar{n}_0 = \left(\sum_{\substack{1 \le j \le k \\ i \equiv 1 \bmod 2}} \bar{n}_j \right) - \left(\sum_{\substack{2 \le j \le k \\ i \equiv 0 \bmod 2}} \bar{n}_j \right) = \underline{n}_1 - \underline{n}_2.$$

Ist $\underline{n}$ eine Partition, dann ist nach Lemma 4.3.2 klar, dass $\bar{n}$ die zugehörige Derivation ist. Nach den Bedingungen 1. und 2. ist $\underline{n}_i \ge 0$ für $1 \le i \le k$. Wir müssen also lediglich noch zeigen, dass $\underline{n}_i \ge \underline{n}_{i+1}$ für $1 \le i \le k-1$. Für diese i erhalten wir:

$$\begin{aligned}
\underline{n}_i - \underline{n}_{i+1} &= \left(\sum_{\substack{i \le j \le k \\ j \equiv i \bmod 2}} \bar{n}_j \right) - \left(\sum_{\substack{i+1 \le j \le k \\ j \not\equiv i \bmod 2}} \bar{n}_j \right) \\
&= \sum_{j=i_1}^{i_2} (-1)^{j-i_1} \bar{n}_j \\
&\overset{3.}{\ge} 0.
\end{aligned}$$

□

4.3.4 Bemerkung:
Wir benutzen 3. insbesondere mit $i_2 = i_1 + 2$. In diesem Fall ist die Aussage:

$$\bar{n}_{i_1} + \bar{n}_{i_1+2} \geq \bar{n}_{i_1+1}.$$

4.3.5 Algorithmus:
Sei $\underline{n} = (\underline{n}_1, \ldots, \underline{n}_m) \in \mathcal{P}$.

1. Sei $\bar{n}^1 = \bar{n}$ die Derivation von $\underline{n}$. Sei k:=1.
2. Sei $\lambda_k := max_l \left\{\bar{n}_l^k\right\}$ und sei $i_k := max \left\{l | \bar{n}_l^k = \lambda_k\right\}$.
3. Entferne die Einträge $i_k - 1, i_k$ und $i_k + 1$ von $\bar{n}^k$ und ersetze sie durch den neuen Eintrag $\bar{n}^k_{i_k-1} + \bar{n}^k_{i_k+1} - \bar{n}^k_{i_k}$ und man erhält $\bar{n}^{k+1}$. Erhöhe k um 1.
4. Wiederhole Schritt 2 und 3, bis $\bar{n}^k$ nur noch aus Nullen besteht.

Das Ergebnis des Algorithmus ist $(\lambda_1, \ldots, \lambda_k) \in \mathcal{M}_{\mathfrak{p}}$.

4.3.6 Bemerkung:
1. Für jedes k ist $\bar{n}^k$ eine Derivation (bis auf eventuelle Nulleinträge am Schluss).
2. In der k-ten Schleife sind alle Werte $\bar{n}^k$ ganze Zahlen zwischen 0 und λ_{k-1}, so dass die λ_k monoton abfallen. Der Algorithmus liefert in der Tat eine Partition.

4.3.7 Satz:
Sei $e \geq 0$ fest gewählt. Dann erhalten wir

$$\sum_{\substack{M \text{ ist } \mathfrak{p}\text{-Modul} \\ \text{mit Exponenten} \leq e}} w(M) = \prod_{j \not\equiv 0, \pm(e+1) mod(2e+3)} (1 - {q_0}^j)^{-1}.$$

Beweis: Ist Λ eine Cohen-Lenstra-Abbildung, so gilt:

$$w(M) = \sum_{n \geq 0} a_M(n) q_0^n,$$

wobei $a_M(n) = \left|\left\{\Lambda^{-1}(M)\right\} \cap \{\underline{n} \in \mathcal{P} \,|\, \underline{n} \text{ ist eine Partition von } \}\right|$ mit $n \in \mathbb{N}$.
In unserem Fall gilt:

$$\sum_{\substack{M \text{ ist } \mathfrak{p}\text{-Modul} \\ \text{mit Exponenten} \leq e}} w(M) = \sum_{n \geq 0} \left| \left\{ \underline{n} \in \mathcal{P} \;\middle|\; \begin{array}{c} \underline{n} \text{ ist eine Partition von } n \text{ und} \\ \Lambda(\underline{n}) \text{ hat Exponenten } \leq e \end{array} \right\} \right| q_0^n.$$

Aber wenn M als eine Partition in $\mathcal{M}_{\mathfrak{p}}$ interpretiert wird, so ist der Exponent lediglich der größte Teil. Bei einer gegebenen Partition $\underline{n} = (\underline{n}_1, \underline{n}_2, \ldots, \underline{n}_m) \in \mathcal{P}$

ist der größte Teil von $\Lambda(\underline{n})$ genau λ_1, da die λ_i sortiert sind. Andererseits ist $\lambda_1 = max_i(\underline{n}_{i-2} - \underline{n}_i)$, wobei wir $\underline{n}_0 := \underline{n}_{-1} := 0$ setzen. Somit wissen wir:

$$\sum_{\substack{M \text{ ist } \mathfrak{p}\text{-Modul} \\ \text{mit Exponenten} \leq e}} w(M) = \sum_{n \geq 0} \left| \left\{ \underline{n} \in \mathcal{P} \;\middle|\; \begin{array}{c} \underline{n} \text{ ist eine Partition von } n \text{ und} \\ \underline{n}_{i-2} - \underline{n}_i \leq e \text{ für alle } i \end{array} \right\} \right| q_0^n.$$

Die rechte Seite ist wohlbekannt (siehe z.B. [And98], Theorem 7.5, $k := i := e+1$; dort wird die konjugierte Bedingung bewiesen) und hat den Wert

$$\prod_{j \not\equiv 0, \pm(e+1) mod(2e+3)} (1 - {q_0}^j)^{-1}.$$

□

4.3.8 Korollar:
Die Cohen-Lenstra-Wahrscheinlichkeit, dass ein $\mathfrak{p}$-Modul Exponenten $\leq e$ hat, ist

$$\prod_{j \equiv 0, \pm(e+1) mod(2e+3)} (1 - (q^n)^{-j}).$$

Beweis: Die Cohen-Lenstra-Heuristik besagt, dass die Wahrscheinlichkeit einer einelementigen Menge $\{M\}$ durch $\frac{w(M)}{w(\mathcal{M}_\mathfrak{p})}$ gegeben ist. Somit ergibt sich für die Wahrscheinlichkeit, dass ein $\mathfrak{p}$-Modul einen Exponenten $\leq e$ hat:

$$\begin{aligned} \frac{1}{w(\mathcal{M}_\mathfrak{p})} \left(\sum_{\substack{M \text{ ist } \mathfrak{p}\text{-Modul} \\ \text{mit Exponenten} \leq e}} w(M) \right) &= \left(\prod_{j \geq 1} (1 - {q_0}^j) \right) \\ &\quad \cdot \left(\prod_{j \not\equiv 0, \pm(e+1) mod(2e+3)} (1 - {q_0}^j)^{-1} \right) \\ &= \prod_{j \equiv 0, \pm(e+1) mod(2e+3)} (1 - {q_0}^j). \end{aligned}$$

□

Kapitel 5

Interpretation der Cohen-Lenstra-Heuristik mittels Konjugationsklassen

Notation

Im Folgenden bezeichnen:

- $|M|$ oder auch $ord(M)$ die Kardinalität einer Menge M,
- q eine Primzahlpotenz,
- $\mathbb{F}_q$ den Körper mit q Elementen,
- $A := \mathbb{F}_q[X]$ den Polynomring über dem Körper mit q Elementen,
- $\mathfrak{p}$ ein Primideal in A, erzeugt von einem normierten irreduziblen Polynom p mit Grad n,
- $deg(f)$ den Grad eines Polynoms $f \in A$,
- $\mathcal{M}_\mathfrak{p}$ die Menge aller endlichen $\mathfrak{p}$-primären A-Moduln,
- $\underline{\lambda}$ eine Partition,
- Länge($\underline{\lambda}$) bezeichnet die Länge einer Partition $\underline{\lambda}$,
- $\underline{\lambda}'$ die zu $\underline{\lambda}$ konjugierte Partition,
- $\mathcal{P}$ die Menge aller Partitionen,
- $rk(M)$ den Rang des Moduls M,

- $exp_{\mathfrak{p}}(M)$ den $\mathfrak{p}$-adischen Exponenten des Moduls M,
- $w(M)$ das Cohen-Lenstra-Maß des Moduls M,
- $P(M)$ das Cohen-Lenstra-Wahrscheinlichkeitsmaß des Moduls M,
- $GL(m, q^n)$ die allgemeine lineare Gruppe über $\mathbb{F}_{q^n}$.

Wir betrachten die Gruppe $Gl(m, q^n)$ aller invertierbaren $m \times m$-Matrizen über $\mathbb{F}_{q^n}$. Jede Konjugationsklasse kann durch eine Matrix in Normalform dargestellt werden. Wir wollen im Folgenden die Normalform einer solchen Matrix bestimmen. Dazu müssen wir zunächst die Begleitmatrix eines Polynoms
$\Phi = X^r + a_{r-1}X^{r-1} + \ldots + a_1X + a_0$ definieren:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{r-1} \end{pmatrix} .$$

Für jedes normierte irreduzible Polynom Φ vom Grad r über $\mathbb{F}_{q^n}$ und jede positive ganze Zahl s sei $J(\Phi, s)$ die Begleitmatrix des Polynoms Φ^s; dieser wird als Jordan-Block der Größe $rs \times rs$ bezeichnet. Die Normalform hat dann die Gestalt:

$$\begin{pmatrix} J_1 & 0 & 0 & \cdots & 0 \\ 0 & J_2 & 0 & \cdots & 0 \\ 0 & 0 & J_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & J_k \end{pmatrix} .$$

Hierbei durchlaufen die J_k alle möglichen $J(\Phi, s)$. Wir setzen lediglich voraus, dass sich die Spaltenzahlen aller Jordan-Blöcke zu m aufaddieren. Um die Normalform anzugeben, müssen wir also für jedes irreduzible Polynom Φ und jedes $s > 0$ angeben, wieviele (Φ, s)-Jordan Blöcke auftreten. Wir suchen also für jedes irreduzible Polynom Φ eine Partition, welche wir mit $\underline{\lambda}_\Phi$ bezeichnen. Da wir nicht davon ausgehen können, dass die Anzahl der einzelnen Jordan-Blöcke absteigend geordnet ist, lassen wir an dieser Stelle auch Partitionen zu, die nicht notwendigerweise absteigend geordnet sind.

Die Familien von Partitionen $(\underline{\lambda}_\Phi)_\Phi$, wobei Φ alle irreduziblen Polynome über $\mathbb{F}_{q^n}$ durchläuft, mit den Eigenschaften

1. für das Polynom $\Phi(X) = X$ ist $\underline{\lambda}_X = \underline{0}$;
2. $\sum_{\Phi,s} s \cdot (deg\Phi)\underline{\lambda}_{\Phi,s} = m$;

entsprechen eineindeutig den Konjugationsklasse in $Gl(m, q^n)$ (siehe [Bos06], Seite 231, Theorem 11). Wir schreiben $\underline{\Phi}(Mat)$ für die durch $Mat \in GL(m, q^n)$ und das Polynom $\Phi(X)$ definierte Partition.

5.1 Satz:
Sei Φ ein normiertes Polynom über $\mathbb{F}_{q^n}$ vom Grad 1 mit $\Phi(X) \neq X$, und sei $\underline{\lambda}$ eine Partition. Für $m \to \infty$ konvergiert die Wahrscheinlichkeit, dass $\underline{\lambda}_\Phi(Mat) = \underline{\lambda}$ für eine zufällige Matrix Mat in $Gl(m, q^n)$ gilt, gegen die Cohen-Lenstra-Wahrscheinlichkeit $P(\underline{\lambda})$.

Beweis: [Ful97], Section 3.3, Corollary 5 und Section 2.7, Lemma 6 und Theorem 5 mit $u = 1$, $N \to \infty$ □

5.2 Bemerkung:
Diese Wahrscheinlichkeiten konvergieren nicht gleichmäßig in λ. Fulman beweist diese Konvergenz, indem er den Limes $N \to \infty$ von folgender q-Reihe bildet:

$$P^N(\underline{\lambda}) = \begin{cases} \frac{\left(\prod_{i=1}^{N}\left(1-(q^n)^{-i}\right)\right)^2}{\prod_{i=1}^{N-\underline{\lambda}'_1}(1-(q^n)^{-i})} w(\underline{\lambda}') \text{ falls } \underline{\lambda}'_1 \leq N \\ 0 \text{ falls } \underline{\lambda}'_1 > N. \end{cases}$$

Hierbei ist $\underline{\lambda}'$ die zu $\underline{\lambda}$ konjugierte Partition und $w(\underline{\lambda}')$ das zugehörige Cohen-Lenstra-Maß dieser konjugierten Partition. Für die gleichmäßige Konvergenz betrachtet man den Limes der q-Reihe

$$\left(\frac{\left(\prod_{i=1}^{N}\left(1-(q^n)^{-i}\right)\right)^2}{\prod_{i=1}^{N-\underline{\lambda}'_1}\left(1-(q^n)^{-i}\right)} - \left(\prod_{i=1}^{\infty}\left(1-(q^n)^{-i}\right)\right) \right) w(\underline{\lambda}')$$

entlang der „Diagonalen“, d.h. $N = \underline{\lambda}'_1$. So stellt man fest, dass dieser Ausdruck nicht gegen Null geht und somit auch das Supremum über alle $\underline{\lambda}$ nicht gegen Null geht. Folglich liegt keine gleichmäßige Konvergenz vor.

5.3 Bemerkung:
Dieser Satz besagt, dass die normierten Polynome vom Grad größer als 1 asymptotisch keine Rolle mehr spielen. Die Tatsache, dass die Wahrscheinlichkeit nicht gleichmäßig konvergiert, wirkt zunächst wie eine Einschränkung, allerdings ist die punktweise Konvergenz für unser Zwecke völlig ausreichend.

Fulman gab zwei Interpretationen der Cohen-Lenstra-Wahrscheinlichkeit in seiner Doktorarbeit [Ful97] an, die im Folgenden behandelt werden.

5.1 Interpretation mittels Young-Tableaus

Wir werden im Folgenden die Cohen-Lenstra-Heuristik als Ergebnis eines wahrscheinlichkeitstheoretischen Algorithmus interpretieren.

5.1.1 Algorithmus („Young-Tableau-Algorithmus“):

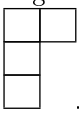
1. Beginne mit einer leeren Partition $\underline{\lambda}$, $N = 1$ und mit einer Sammlung von Münzen indiziert durch die natürlichen Zahlen, so dass Münze i die Wahrscheinlichkeit $(q^n)^{-i}$ auf Kopf und $1 - (q^n)^{-i}$ auf Zahl hat.

2. Wirf Münze N. Ist das Ergebnis Zahl, dann setze $N := N + 1$ und wiederhole Schritt 2. Ist das Ergebnis Kopf, gehe zu Schritt 3.

3. Wähle eine ganze Zahl $S > 0$ nach folgender Auswahlregel: $S := 1$ mit Wahrscheinlichkeit $\frac{(q^n)^{N-\underline{\lambda}_1}-1}{(q^n)^N-1}$. Für $s > 1$, setze $S := s$ mit Wahrscheinlichkeit $\frac{(q^n)^{N-\underline{\lambda}_s}-(q^n)^{N-\underline{\lambda}_{s-1}}}{(q^n)^N-1}$. Erhöhe $\underline{\lambda}_S$ um 1 und gehe zu Schritt 2.

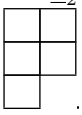
In Schritt 3 benutzen wir, dass alle undefinierten Einträge von $\underline{\lambda}$ Null sind. Der Algorithmus hält nicht an, aber $\underline{\lambda}$ konvergiert mit Wahrscheinlichkeit 1 gegen eine Grenzpartition.

5.1.2 Beispiel:
Angenommen wir befinden uns mit der Partition $\underline{\lambda} = (2, 1, 1)$ in Schritt 2 unseres Algorithmus. Dann betrachten wir das Young-Diagramm



.

Wir nehmen weiter an, dass $N = 3$ ist und dass Münze 3 als Ergebnis Kopf ergibt. Wir gehen also zu Schritt 3 und erhöhen $\underline{\lambda}_1$ mit der Wahrscheinlichkeit $\frac{q^n-1}{(q^n)^3-1}$, $\underline{\lambda}_2$ mit der Wahrscheinlichkeit $\frac{(q^n)^2-q^n}{(q^n)^3-1}$, $\underline{\lambda}_3$ mit der Wahrscheinlichkeit 0 und $\underline{\lambda}_4$ mit der Wahrscheinlichkeit $\frac{(q^n)^3-(q^n)^2}{(q^n)^3-1}$. Wählen wir $S = 2$, so erhöhen wir $\underline{\lambda}_2$ und erhalten $\underline{\lambda} = (2, 2, 1)$ mit zugehörigem Young-Diagramm



.

Anschließend kehren wir zu Schritt 2 zurück, N hat immer noch den Wert 3. Falls Münze 3 erneut Kopf anzeigt, gehen wir zu Schritt 3 und erhöhen $\underline{\lambda}_1$ mit der Wahrscheinlichkeit $\frac{q^n-1}{(q^n)^3-1}$, $\underline{\lambda}_2$ mit der Wahrscheinlichkeit 0, $\underline{\lambda}_3$ mit der Wahrscheinlichkeit $\frac{(q^n)^2-q^n}{(q^n)^3-1}$ und $\underline{\lambda}_4$ mit der Wahrscheinlichkeit $\frac{(q^n)^3-(q^n)^2}{(q^n)^3-1}$.

5.1.3 Bemerkung:
Ein Young-Tableau ist ein Young-Diagramm, dessen Boxen von $1, \ldots, k$ durchnummeriert sind, wobei k die Größe des Young-Diagramms ist. Die Nummerierung muss so gewählt werden, dass für jedes i mit $1 \leq i \leq k$ die Boxen $1, \ldots, i$

erneut ein Young-Diagramm bilden. Man kann ein Young-Tableau also als ein Young-Diagramm versehen mit einer Ordnungsrelation interpretieren, das angibt, wie man das Diagramm ganz von vorne aufbaut. Da der Algorithmus genau dies angibt, erklärt sich der passende Name „Young-Tableau-Algorithmus“.

5.1.4 Satz:
Mit Wahrscheinlichkeit 1 *erzeugt der Algorithmus eine endliche Partition. Für eine gegebene Partition* $\underline{\lambda}$ *ist die Wahrscheinlichkeit, dass der Algorithmus* $\underline{\lambda}$ *erzeugt, die Cohen-Lenstra-Wahrscheinlichkeit* $P(\underline{\lambda})$.

Beweis: [Ful99], Theorem 1. □

5.2 Interpretation im Young-Gitter

Das Young-Gitter ist ein gewichteter und gerichteter Graph mit Knotenmenge $\mathcal{P}$. Es gibt eine gerichtete Kante von $\underline{\lambda}$ nach $\underline{\mu}$ genau dann, wenn das Young-Diagramm von $\underline{\lambda}$ enthalten ist im Young-Diagramm von $\underline{\mu}$ und Länge$(\underline{\lambda})$ = Länge$(\underline{\mu}) - 1$. Die konjugierte Partition $\underline{\lambda}'$ ist der Index des Knotens. Es gibt eine gerichtete Kante von $\underline{\lambda}$ zu $\underline{\nu}$ genau dann, wenn ein Index i_0 existiert, so dass $\underline{\nu}'_{i_0} = \underline{\lambda}'_{i_0} + 1$ und $\underline{\nu}'_i = \underline{\lambda}'_i$ für alle $i = i_0$.

5.2.1 Satz:
Wir legen das Gewicht $m_{\underline{\lambda}',\underline{\mu}'}$ *an die Kanten wie folgt:*

1. $m_{\underline{\lambda}',\underline{\mu}'} = \frac{1}{(q^n)^{\underline{\lambda}'_1}((q^n)^{\underline{\lambda}'_1+1}-1)}$, *falls* $\underline{\mu}'_1 = \underline{\lambda}'_1 + 1$.
2. $m_{\underline{\lambda}',\underline{\mu}'} = \frac{(q^n)^{-\underline{\lambda}'_s} - (q^n)^{-\underline{\lambda}'_{s-1}}}{(q^n)^{\underline{\lambda}'_1}-1}$, *falls* $\underline{\mu}'_s = \underline{\lambda}'_s + 1$ *für* $s > 1$.

Dann gilt folgende Formel für das Cohen-Lenstra-Maß:

$$w(\underline{\lambda}) = \sum_{\gamma'} \prod_{i=0}^{\lambda-1} m_{\gamma'_i,\gamma'_{i+1}},$$

wobei $\gamma' = (\gamma'_1, \ldots, \gamma'_\lambda)$ *alle gerichteten Pfade von der leeren Partition zu* $\underline{\lambda}'$ *im Young-Gitter durchläuft.*

Beweis: [Ful99], Theorem 2. □

5.2.2 Bemerkung:
Wie eine kurze Berechnung zeigt, ist für jede Partition $\underline{\lambda} \in \mathcal{P}$ die Summe aller Gewichte der Kanten weg von $\underline{\lambda}$ gegeben durch $\frac{q^n}{(q^n)^{\underline{\lambda}'_1+1}-1}$, und dies ist kleiner 1. Deshalb kann das Gewicht der Kante $\underline{\lambda}', \underline{\mu}'$ auch als Übergangswahrscheinlichkeit interpretiert werden, während der zu 1 fehlende Rest die Wahrscheinlichkeit angibt, bei $\underline{\lambda}$ stehen zu bleiben

5.3 Beispiele

5.3.1 Satz:
Die Wahrscheinlichkeit, dass ein zufällig gewählter $\mathfrak{p}$*-Modul* M *Rang* r *hat, ist*

$$P(rk(M)=r)=\prod_{i=1}^{\infty}\left(1-(q^n)^{-i}\right)\frac{(q^n)^{r^2}}{\left(\prod_{i=1}^{r}(1-(q^n)^{-i})\right)^2}.$$

Beweis: [Ful97], Theorem 15. □

5.3.2 Satz:
Die Wahrscheinlichkeit, dass ein $\mathfrak{p}$*-Modul* M *Ordnung* e *und Rang* r *hat, ist*

$$P\begin{pmatrix} ord(M)=e \\ rk(M)=r \end{pmatrix}=\prod_{i=1}^{\infty}(1-(q^n)^{-i})\frac{|Gl(r,q^n)|^{-1}\,(q^n)^{e-r}\prod_{i=1}^{e-1}(1-(q^n)^{-i})}{\left(\prod_{i=1}^{r-1}(1-(q^n)^{-i})\right)\left(\prod_{i=1}^{e-r}(1-(q^n)^{-i})\right)}.$$

Beweis: [Ful97], Theorem 16. □

5.3.3 Satz:
Die Wahrscheinlichkeit, dass ein zufällig gewählter $\mathfrak{p}$*-Modul* M *einen Exponenten höchstens* e *hat, ist*

$$P(exp_{\mathfrak{p}}(M)\leq e)\prod_{j\equiv 0,\pm(e+1)mod(2e+3)}(1-(q^n)^{-j}).$$

Beweis: [Ful97], Theorem 21. □

Kapitel 6

Globale Theorie

Notation

Im Folgenden bezeichnen:

- k, u natürliche Zahlen aus $\mathbb{N}$, eventuell $k = \infty$,
- $|M|$ oder auch $ord(M)$ die Kardinalität einer Menge M,
- q eine Primzahlpotenz,
- $\mathbb{F}_q$ den Körper mit q Elementen,
- $A := \mathbb{F}_q[X]$ den Polynomring über dem Körper mit q Elementen,
- $\mathfrak{p}$ ein Primideal in A,
- $\mathfrak{a}$ ein Ideal in A,
- $\mathbb{P}$ die Menge aller Primideale von A,
- $N\mathfrak{p}$ die Norm von $\mathfrak{p}$,
- $deg(f)$ den Grad eines Polynoms $f \in A$,
- $\mathcal{M}$ die Menge aller endlichen A-Moduln,
- $\mathcal{M}_\mathfrak{p}$ die Menge aller endlichen $\mathfrak{p}$-primären A-Moduln,
- $M_{\mathbb{P}_1}$ den $\mathbb{P}_1$-Anteil des Moduls M für eine Teilmenge $\mathbb{P}_1$ von $\mathbb{P}$,
- $rk(M)$ den Rang des Moduls M,
- $r_\mathfrak{p}(M)$ den $\mathfrak{p}$-Rang des Moduls M,
- $Aut(M)$ die Automorphismengruppe von M,

- $w(M) = \frac{1}{|Aut(M)|}$ das Cohen-Lenstra-Maß des Moduls M,
- $\chi_A(M)$ für einen Modul $M = \oplus A/\mathfrak{a}_i$ das wohlbestimmte Ideal $\chi_A(M) = \prod_i \mathfrak{a}_i$,
- $s_k(M)$ die Anzahl der surjektiven A-Homomorphismen von A^k nach M,
- $w_k(M)$ das k-Maß des Moduls M,
- $\zeta_k(s)$ die k-Zeta-Funktion,
- $\zeta_A(s)$ die Dedekindsche Zeta-Funktion,
- κ das Residuum von ζ_A in 1,
- C_k das Residuum von ζ_k in 0,
- $E_{k,u}(f)$ den (k,u)-Erwartungswert von f,
- $I_{k,u}(f)$ den (k,u)-Inhalt von f.

Bisher haben wir uns lediglich mit endlichen $\mathfrak{p}$-primären A-Moduln beschäftigt. Nun möchten wir uns mit beliebigen endlichen A-Moduln befassen. Diese Theorie wurde bereits von Cohen und Lenstra in [CL84] entwickelt und wir werden im Folgenden weitestgehend ihre Notation verwenden. Die Techniken, die wir für $\mathfrak{p}$-Moduln haben, können wir leider nicht für den allgemeinen Fall verwenden. Das Cohen-Lenstra-Maß für den Modul M ist proportional zu $|Aut(M)|^{-1}$. Um dies verallgemeinern zu können, müsste $\sum_M |Aut(M)|^{-1} < \infty$ sein. Dies ist aber nicht der Fall, denn

$$\sum_M |Aut(M)|^{-1} \geq \sum_{\mathfrak{p}\in\mathbb{P}} |Aut(A/\mathfrak{p})|^{-1} = \sum_{\mathfrak{p}\in\mathbb{P}} (N\mathfrak{p}-1)^{-1} = \infty.$$

Ein weiteres Problem stellt die σ-Additivität dar. Da ein Wahrscheinlichkeitsmaß P σ-additiv ist, würde gelten:

$$1 = P(\mathcal{M}) = P(\bigcup_{M\in\mathcal{M}} \{M\}) = \sum_{M\in\mathcal{M}} P(\{M\}) = 0.$$

Wir müssen uns also von der Vorstellung trennen, einen Wahrscheinlichkeitsraum konstruieren zu können, der das stochastische Verhalten eines zufälligen endlichen A-Moduls M bescheibt. Wenn wir uns aber auf endliche Additivität beschränken, so erhalten wir einen Inhaltsraum und können Inhalte anstatt Wahrscheinlichkeiten betrachten.

6.1 Definition:
Ein Inhalt auf einer Algebra $\mathcal{A}$ auf der Menge X ist eine Abbildung
$\mu : \mathcal{A} \to \mathbb{R} \cup \{\infty\}$ für die gilt:

1. $\mu(\emptyset) = 0$.
2. $\mu(A) \geq 0$ für alle $A \in \mathcal{A}$.
3. $\mu(A_1 \cup A_2) = \mu(A_1) + \mu(A_2)$ für alle disjunkten Mengen $A_1, A_2 \in \mathcal{A}$.

Zunächst benötigen wir aber noch einige allgemeine Grundlagen zur ζ-Funktion.

6.1 Die Zeta-Funktion

6.1.1 Satz:
Jeden endlichen A-Modul M kann man in der Form

$$M = \oplus A/\mathfrak{a}_i \text{ mit Idealen } \mathfrak{a}_i \text{ von } A$$

schreiben. Obwohl die Komponenten $A/\mathfrak{a}_i$ nicht eindeutig bestimmt sind, ist das Produkt $\prod_i \mathfrak{a}_i$ ein wohlbestimmtes Ideal von A, das nur von der Isomorphieklasse von M abhängt. Es wird mit $\chi_A(M)$ bezeichnet.

6.1.2 Definition:
Sei M ein endlicher A-Modul. Mit $s_k(M)$ bezeichnen wir die Anzahl der surjektiven A-Homomorphismen von A^k nach M.
Das k-Maß von M wird definiert durch

$$w_k(M) = s_k(M)\,|M|^{-k}\,|Aut(M)|^{-1} \text{ und}$$

$$w_\infty(M) := \lim_{k\to\infty} w_k(M).$$

6.1.3 Definition:
Mit $r_\mathfrak{p}(M)$ bezeichnen wir den $\mathfrak{p}$-Rang, d.h. den Rang $dim_{A/\mathfrak{p}}(M/\mathfrak{p}M)$ des $\mathfrak{p}$-primären Anteils $M_\mathfrak{p}$ von M.

6.1.4 Satz:
Sei M ein endlicher A-Modul mit $\chi_A(M) = \mathfrak{a}$. Dann gilt:

$$w_k(M) = \left(\prod_{\mathfrak{p}|\mathfrak{a}} \prod_{i=k-r_\mathfrak{p}+1}^{k} \left(1-(N\mathfrak{p})^{-1}\right)\right) \cdot \frac{1}{|Aut(M)|}$$

und

$$w(M) = \lim_{k\to\infty} w_k(M).$$

Beweis: [CL84], Proposition 3.1 □

6.1.5 Bemerkung:
Zur Vereinfachung wollen wir folgende Abkürzungen verwenden:

$$\sum_{\mathfrak{a}} \text{ steht für } \sum_{\mathfrak{a} \text{ ist Ideal in } A},$$

$$\sum_{M(\mathfrak{a})} \text{ steht für } \sum_{M \text{ bis auf Isomorphie mit } \chi_A(M)=\mathfrak{a}} \text{ und}$$

$$\sum_{M(\mathfrak{a}),\varphi_u} \text{ steht für } \sum_{M \text{ bis auf Isomorphie mit } \chi_A(M)=\mathfrak{a},\ \varphi\in \mathrm{Hom}_A(A^u,M)}.$$

6.1.6 Definition:
Wir definieren das k-Maß eines Ideals $\mathfrak{a}$ *als*

$$w_k(\mathfrak{a}) = \sum_{M(\mathfrak{a})} w_k(M).$$

6.1.7 Definition:
Wir definieren die k-ζ*-Funktion über* $\mathcal{M}$ *als*

$$\zeta_{k,A}(s) := \zeta_k(s) = \sum_{\mathfrak{a}} w_k(\mathfrak{a})(N\mathfrak{a})^{-s}$$

mit $N\mathfrak{a} = |A/\mathfrak{a}|$.
Sei $\mathfrak{p} \in \mathbb{P}$. *Dann ist die k-*$\zeta$*-Funktion eingeschränkt auf die Menge der* $\mathfrak{p}$*-Moduln gegeben durch*

$$\zeta_k^{\mathfrak{p}}(s) := \sum_{\alpha \in \mathbb{N}} w_k(\mathfrak{p}^\alpha)(N\mathfrak{p})^{-\alpha s}.$$

6.1.8 Satz:

1. ζ_k *konvergiert für* $Re(s) > 0$.
2. *Sei* $\mathfrak{p} \in \mathbb{P}$. *Dann gilt für* $Re(s) > -1$*:*

$$\zeta_k^{\mathfrak{p}}(s) = \prod_{1 \le j \le k} \left(1 - (N\mathfrak{p})^{-j-s}\right)^{-1}.$$

3. *Für* $Re(s) > 0$ *ist*

$$\zeta_k(s) = \prod_{1 \le j \le k} \zeta_A(s+j).$$

Hierbei bezeichnet $\zeta_A(s)$ *die Dedekindsche Zeta-Funktion von A, nämlich* $\zeta_A(s) = \frac{1}{1-q^{1-s}} = \prod_{\mathfrak{p} \in \mathbb{P}} (1 - (N\mathfrak{p})^{-s})^{-1}$.

Beweis: [CL84], Korollar 3.7. □

6.1.9 Korollar:
Wenn wir die meromorphe Fortsetzung um $s = 0$ *betrachten, so ergibt sich, dass* ζ_k *in* $s = 0$ *einen einfachen Pol mit Residuum*

$$C_k = \kappa \prod_{2 \le i \le k} \zeta_A(i)$$

hat, wobei $\kappa = \frac{1}{log(q)}$ *das Residuum von* ζ_A *an der Stelle* 1 *ist.*

6.1.10 Bemerkung:
Es gilt die Identität

$$\zeta_{k_1+k_2}(s) = \zeta_{k_1}(s+k_2)\zeta_{k_2}(s).$$

Nun haben wir alle Hilfsmittel, um globale Inhalte und Erwartungswerte zu definieren.

6.2 Inhalte und Erwartungswerte

6.2.1 Definition:
Wir setzen für eine komplexwertige Funktion f, die auf der Menge $\mathcal{M}$ der Isomorphieklassen endlicher A-Moduln definiert ist und $k \in \mathbb{N} \cup \{\infty\}$,

$$w_k(f;\mathfrak{a}) = \sum_{M(\mathfrak{a})} w_k(M) f(M)$$

und

$$\zeta_k(f;s) = \sum_{\mathfrak{a}} w_k(f;\mathfrak{a})(N\mathfrak{a})^{-s}.$$

Wir definieren den (k,u)-Erwartungswert $E_{k,u}(f)$ von f wie folgt:

$$E_{k,u}(f) = \lim_{x\to\infty} \frac{\sum_{N\mathfrak{a}\le x}(N\mathfrak{a})^{-u}\sum_{M(\mathfrak{a}),\varphi_u} f(M/im(\varphi))w_k(M)}{\sum_{N\mathfrak{a}\le x}(N\mathfrak{a})^{-u}\sum_{M(\mathfrak{a}),\varphi_u} w_k(M)}.$$

Ist $k=\infty$, so sprechen wir von u-Mittelwerten von f und schreiben $E_u(f)$ anstatt $E_{\infty,u}(f)$.

6.2.2 Bemerkung:

1. Der (k,u)-Erwartungwert muss nicht notwendigerweise existieren.
2. Der Nenner in $E_{k,u}(f)$ ist gleich $\sum_{N\mathfrak{a}\le x} w_k(\mathfrak{a})$.
3. Falls f die charakteristische Funktion einer Eigenschaft ist, wollen wir von einem (k,u)-Inhalt $I_{k,u}$ oder u-Inhalt I_u von f bezüglich der entsprechenden Eigenschaft sprechen.
4. Für $k=\infty$, $u=0$, sprechen wir vom Erwartungswert bzw. vom Inhalt von f.
5. Wir erhalten nur endliche Additivität.

6.2.3 Bemerkung:
Der u-Inhalt $I_u(M)$ von M ist die „Wahrscheinlichkeit“, dass M bei folgendem zufälligen „Prozess“ erzeugt wird:

1. Wähle einen zufälligen endlichen A-Modul H mit Berücksichtigung der Cohen-Lenstra-Heuristik $|H| \le x$ mit $x >> 0$.
2. Wähle zufällig u Elemente $g_1,\dots,g_u$.
3. Ergebnis: $H/\langle g_1,\dots,g_u\rangle$.

Nun suchen wir einen Weg, $E_{k,u}$ und $I_{k,u}$ einfach zu berechnen. Dazu benötigen wir folgende Definition und anschließend einen Tauber-Satz:

6.2.4 Definition:
Zwei für hinreichend große reelle Argumente definierte Funktionen f und g heißen asymptotisch äquivalent, falls $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, in Zeichen $f(x) \backsim g(x)$.

6.2.5 Lemma:
Konvergiert die Reihe $D(s) = \sum_{\mathfrak{a}} c(\mathfrak{a})(N\mathfrak{a})^{-s}$ mit nicht negativen reellen Koeffizienten $c(\mathfrak{a})$ für $Re(s) > 0$ und ist $D(s) - \frac{C}{s}$ analytisch fortsetzbar für $Re(s) \geq 0$, dann existiert ein $\delta < 1$ mit

$$\sum_{N\mathfrak{a}\leq x} c(\mathfrak{a}) \backsim Clog(x) + O(\frac{log(x)}{log(q)}(x)^{\delta-1}) \text{ für } x \to \infty.$$

Beweis: Wir können $\sum_{\mathfrak{a}} c(\mathfrak{a})(N\mathfrak{a})^{-s}$ wie folgt schreiben:

$$\sum_{\mathfrak{a}} c(\mathfrak{a})(N\mathfrak{a})^{-s} = \sum_{n\geq 1} \left(n \sum_{N\mathfrak{a}=n} c(\mathfrak{a}) \right) (n)^{-s-1}.$$

Da $N\mathfrak{a}$ immer eine Potenz von q ist, können wir [Ros02], Theorem 17.1 auf folgenden Term anwenden:

$$\sum_{N\geq 1} q^N \left(\sum_{N\mathfrak{a}=q^N} c(\mathfrak{a}) \right) (q^N)^{-s-1}.$$

Also gibt es ein $\delta < 1$ mit

$$q^N \left(\sum_{N\mathfrak{a}=q^N} c(\mathfrak{a}) \right) = C \cdot log(q) \cdot q^N + O(q^{\delta N}).$$

Somit ergibt sich

$$\sum_{N\mathfrak{a}=q^N} c(\mathfrak{a}) = C \cdot \sum_{1\leq N} (log(q) + O((q^N)^{\delta-1})) = C \cdot N \cdot log(q) + N \cdot O((q^N)^{\delta-1}).$$

□

6.2.6 Bemerkung:
Genauere Aussagen darüber, wie gut diese Approximation ist, sind nicht möglich, da man δ nicht genau spezifizieren und somit keine Aussagen über die Konstante vor $O(\frac{log(n)}{log(q)}(n)^{\delta-1})$ treffen kann.

6.2.7 Proposition:
Wir schreiben

$$\zeta_k(f;s+u)\zeta_k(s)/\zeta_k(s+u) = \sum_{\mathfrak{a}} a_{k,u}(f;\mathfrak{a})(N\mathfrak{a})^{-s}.$$

Dann ergibt sich

$$E_{k,u}(f) = \lim_{x\to\infty} \frac{\sum_{N\mathfrak{a}\leq x} a_{k,u}(f;\mathfrak{a})}{C_k log(x)}.$$

Beweis: [CL84], Proposition 5.4. □

6.2.8 Korollar:
Sei f eine nicht negativ-wertige reelle Funktion auf einer Teilmenge der Isomorphieklassen von endlichen A-Moduln. Angenommen $\zeta_k(f;s)$ konvergiert für $Re(s) > 0$ und $\zeta_k(f;s) - \frac{C}{s}$ ist analytisch fortsetzbar für $Re(s) \geq 0$. Dann erhalten wir:

$$u \neq 0: \quad E_{k,u} = \zeta_k(f;u)\tfrac{C_u}{C_{u+k}} = \tfrac{\zeta_k(f;u)}{\zeta_k(u)}.$$
$$u = 0: \qquad E_{k,0} = \tfrac{C}{C_k} = \lim_{s\to 0} \tfrac{\zeta_k(f;s)}{\zeta_k(s)}.$$

Beweis: Nach Proposition 6.2.7 ist klar, dass $\sum_{\mathfrak{a}} a_{k,u}(f;\mathfrak{a})(N\mathfrak{a})^{-s}$ für $Re(s) > 0$ konvergiert und asymptotisch äquivalent zu $\left(\frac{\zeta_k(f;u)}{\zeta_k(u)}\right)\frac{C_k}{s}$ für $u > 0$ und zu $\frac{C}{s}$ für $u = 0$ ist. Da $\zeta_k(u) = \frac{C_{u+k}}{C_u}$ gilt, folgt die Behauptung mit Hilfe von Lemma 6.2.5. □

Wir haben also eine angenehme Methode gefunden, $E_{k,u}$ bzw. $I_{k,u}$ zu berechnen. Aber diese Erkenntnis bringt noch weitere Vorteile. Für viele Anwendungen interessiert man sich nur für bestimmte $\mathfrak{p}$-Komponenten eines A-Moduls. Wir nehmen uns eine Teilmenge $\mathbb{P}_1 \subset \mathbb{P}$ und bezeichnen mit $M_{\mathbb{P}_1}$ den $\mathbb{P}_1$-Anteil eines endlichen A-Moduls. Weiter nennen wir einen A-Modul M einen $\mathbb{P}_1$-Modul, falls $M = M_{\mathbb{P}_1} = \bigoplus_{\mathfrak{p}\in\mathbb{P}_1} M_{\mathfrak{p}}$ ist.

6.2.9 Definition:
Die Funktion $f \circ \mathbb{P}_1$ wird definiert als

$$f \circ \mathbb{P}_1(M) = f(M_{\mathbb{P}_1}).$$

Wir erhalten folgende Proposition:

6.2.10 Proposition:
Sei $\mathfrak{a} = \chi_A(M)$ *sowie* $\mathfrak{a}_1$ *das zum* $\mathbb{P}_1$*-Anteil von* M *gehörige Ideal* $\chi_A(M_{\mathbb{P}_1})$ *und* $\mathfrak{a}_2 = \mathfrak{a}\mathfrak{a}_1^{-1}$. *Dann gilt*

$$w_k(f \circ \mathbb{P}_1(M)) = w_k(f; \mathfrak{a}_1) w_k(\mathfrak{a}_2)$$

und demzufolge

$$\zeta_k(f \circ \mathbb{P}_1(M); s) = \left(\sum_{\mathfrak{a}, \mathfrak{p} \mid \mathfrak{a} \Rightarrow \mathfrak{p} \in \mathbb{P}_1} w_k(f; \mathfrak{a}) (N\mathfrak{a})^{-s} \right) \prod_{\mathfrak{p} \notin \mathbb{P}_1} \prod_{1 \leq j \leq k} (1 - (N\mathfrak{p})^{-j-s})^{-1}.$$

Beweis: Setze $\mathbb{P}_2 = \mathbb{P} - \mathbb{P}_1$, $M_1 = M_{\mathbb{P}_1}$, $M_2 = M_{\mathbb{P}_2}$ dann erhalten wir $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ wobei $\mathfrak{a}_1$ der $\mathbb{P}_1$-Anteil von $\mathfrak{a}$ ist und

$$w_k(f \circ \mathbb{P}_1; \mathfrak{a}) = \sum_{M(\mathfrak{a})} w_k(M) f(M_1) = \sum_{M_1(\mathfrak{a}_1)} w_k(M_1) f(M_1) \sum_{M_2(\mathfrak{a}_2)} w_k(M_2).$$

Dies zeigt die erste Gleichung; die zweite ist eine formale Konsequenz der Definition von $\zeta_k(f; s)$ und von Satz 6.1.8. □

6.2.11 Korollar:
Der (k, u)*-Erwartungswert einer Funktion* f *eingeschränkt auf* $\mathbb{P}_1$*-*A*-Moduln ist derselbe wie der* (k, u)*-Erwartungswert der Funktion* $f \circ \mathbb{P}_1$.

Beweis: Dies folgt durch eine leichte Rechnung aus der eben in Proposition 6.2.10 gezeigten Eigenschaft für das k-Maß und die k-ζ-Funktion, sowie der in Korollar 6.2.8 bewiesenen Formel zur Berechnung des (k, u)-Erwartungswertes einer Funktion. □

Dies zeigt, dass die einzelnen $\mathfrak{p}$-Komponenten eines zufälligen endlichen A-Moduls sich unabhängig verhalten. In unserer Situation ist es kein Postulat, sondern eine Folgerung aus den Eigenschaften der ζ-Funktion.

6.2.12 Bemerkung:
Der Inhalt, dass ein zufälliger $\mathbb{P}_1$-Modul eine bestimmte Eigenschaft hat und der Inhalt, dass die $\mathbb{P}_1$-Komponente eines zufälligen beliebigen endlichen Moduls diese Eigenschaft hat, sind wahrscheinlichkeitstheoretisch gesehen völlig unterschiedliche Ereignisse und Interpretationen. Diese beiden Inhalte stimmen aber nach dem eben gezeigten Korollar überein.

6.3 Beispiele

Zur effektiven Berechnung der folgenden Beispiele wurden stets Korollar 6.2.8 sowie Proposition 6.2.10 verwendet. Weiter gilt für jedes Beispiel: f sei jeweils die charakteristische Funktion der in dem einzelnen Beispiel beschriebenen Eigenschaft.

Lokale Situation

Wir betrachten $\mathfrak{p}$-Moduln:

6.3.1 Beispiel:
Der u-Inhalt, dass $M_{\mathfrak{p}} \neq 0$ ist, ist

$$1 - \prod_{i=u+1}^{\infty} \left(1 - (N\mathfrak{p})^{-i}\right) = (N\mathfrak{p})^{-u-1} + (N\mathfrak{p})^{-u-2} + (N\mathfrak{p})^{-u-3} \ldots .$$

Beweis: Zunächst berechnen wir:

$$\begin{aligned}
\zeta_k(f,u) &= \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} w_k(M) f(M) (N\mathfrak{a})^{-u} \\
&= \left(\sum_{\alpha \in \mathbb{N}^+} w_k(\mathfrak{p}^\alpha)(N\mathfrak{p})^{-\alpha s} \right) \prod_{\substack{\mathfrak{p}' \in \mathbb{P}, \\ \mathfrak{p}' \neq \mathfrak{p}}} \left(\prod_{1 \leq j \leq k} \left(1 - (N\mathfrak{p}')^{-j-u}\right)^{-1} \right) \\
&= \left(\sum_{\alpha \in \mathbb{N}} w_k(\mathfrak{p}^\alpha)(N\mathfrak{p})^{-\alpha s} - 1 \right) \prod_{\substack{\mathfrak{p}' \in \mathbb{P}, \\ \mathfrak{p}' \neq \mathfrak{p}}} \left(\prod_{1 \leq j \leq k} \left(1 - (N\mathfrak{p}')^{-j-u}\right)^{-1} \right) \\
&= \zeta_k(u) - \prod_{\substack{\mathfrak{p}' \in \mathbb{P}, \\ \mathfrak{p}' \neq \mathfrak{p}}} \left(\prod_{1 \leq j \leq k} \left(1 - (N\mathfrak{p}')^{-j-u}\right)^{-1} \right)
\end{aligned}$$

Und somit gilt:

$$\zeta_k(u) = \prod_{\mathfrak{p}' \in \mathbb{P}} \left(\prod_{1 \leq j \leq k} \left(1 - (N\mathfrak{p}')^{-j-u}\right)^{-1} \right).$$

Dann gilt für den u-Inhalt:

$$I_u = \lim_{k \to \infty} \frac{\zeta_k(f;u)}{\zeta_k(u)} = 1 - \prod_{i=u+1}^{\infty} \left(1 - (N\mathfrak{p})^{-i}\right).$$

□

6.3.2 Beispiel:
Der Inhalt, dass ein zufällig gewählter $\mathfrak{p}$-Modul M Rang r hat, ist

$$I(rk(M) = r) = \prod_{i=1}^{\infty} \left(1 - (N\mathfrak{p})^{-i}\right) \frac{(N\mathfrak{p})^{-r^2}}{\left(\prod_{i=1}^{r} \left(1 - (N\mathfrak{p})^{-i}\right)\right)^2}.$$

Beweis: [CL84], Theorem 6.3. □

6.3.3 Beispiel:
Der Inhalt, dass ein zufällig gewählter $\mathfrak{p}$-Modul Ordnung $(N\mathfrak{p})^n$ hat, ist

$$\begin{aligned} I(ord(M) = (N\mathfrak{p})^n) &= (N\mathfrak{p})^{-n} \prod_{i=n+1}^{\infty} (1 - (N\mathfrak{p})^{-i}) \\ &= (N\mathfrak{p})^{-n} - (N\mathfrak{p})^{-2n-1} + (N\mathfrak{p})^{-2n-2} \dots . \end{aligned}$$

Beweis: [CL84], Korollar 3.8. □

6.3.4 Bemerkung:
In der lokalen Situation stimmen die Inhalte mit den Wahrscheinlichkeiten überein.

Semilokale Situation

In der semilokalen Situation betrachten wir für eine Teilmenge $\mathbb{P}_1$ von $\mathbb{P}$ nur den $\mathbb{P}_1$-Anteil eines endlichen A-Moduls.

6.3.5 Beispiel:
Der u-Inhalt, dass der $\mathbb{P}_1$-Anteil eines endlichen A-Moduls M zyklisch ist (d.h. $M_{\mathbb{P}_1} \cong A/\mathfrak{a}$), ist

$$\prod_{\mathfrak{p} \in \mathbb{P}_1} \left(\frac{(1 - (N\mathfrak{p})^{-1} + (N\mathfrak{p})^{-u-2})}{(1 - (N\mathfrak{p})^{-u-1})(1 - (N\mathfrak{p})^{-1})} \prod_{i=u+1}^{\infty} (1 - (N\mathfrak{p})^{-i}) \right).$$

Der 0-Inhalt, dass der $\mathbb{P}_1$-Anteil eines endlichen A-Moduls zyklisch ist, ist

$$\prod_{\mathfrak{p} \in \mathbb{P}_1} \left(\frac{(1 - (N\mathfrak{p})^{-1} + (N\mathfrak{p})^{-2})}{(1 - (N\mathfrak{p})^{-1})} \prod_{i=2}^{\infty} (1 - (N\mathfrak{p})^{-i}) \right).$$

Der 1-Inhalt, dass der $\mathbb{P}_1$-Anteil eines endlichen A-Moduls zyklisch ist, ist

$$\prod_{\mathfrak{p} \in \mathbb{P}_1} \left((1 - (N\mathfrak{p})^{-1} + (N\mathfrak{p})^{-2}) \prod_{i=3}^{\infty} (1 - (N\mathfrak{p})^{-i}) \right).$$

Beweis: Wir erhalten:

$$\begin{aligned}
\zeta_\infty(f,u) &= \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} w(M) f(M) (N\mathfrak{a})^{-u} \\
&= \sum_{\mathfrak{a}} \sum_{\substack{M(\mathfrak{a}),\\ M_{\mathbb{P}_1} \text{ zyklisch}}} w(M) (N\mathfrak{a})^{-u} \\
&= \prod_{\mathfrak{p}\in\mathbb{P}_1} \left(\sum_{\alpha=1}^{\infty} (1-N\mathfrak{p}^{-1})^{-1} (N\mathfrak{p}^{\alpha})^{-1} (N\mathfrak{p}^{\alpha})^{-u} + 1 \right) \\
&\quad \cdot \prod_{\mathfrak{p}\notin\mathbb{P}_1} \left(\prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1} \right) \\
&= \prod_{\mathfrak{p}\in\mathbb{P}_1} \left(\sum_{\alpha=1}^{\infty} (1-N\mathfrak{p}^{-1})^{-1} (N\mathfrak{p}^{\alpha})^{-1-u} + 1 \right) \\
&\quad \cdot \prod_{\mathfrak{p}\notin\mathbb{P}_1} \left(\prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1} \right) \\
&= \prod_{\mathfrak{p}\in\mathbb{P}_1} \left((1-N\mathfrak{p}^{-1})^{-1} \left(\sum_{\alpha=0}^{\infty} (N\mathfrak{p}^{-1-u})^{\alpha} - (N\mathfrak{p})^{-1} \right) \right) \\
&\quad \cdot \prod_{\mathfrak{p}\notin\mathbb{P}_1} \left(\prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1} \right) \\
&= \prod_{\mathfrak{p}\in\mathbb{P}_1} \left((1-N\mathfrak{p}^{-1})^{-1} \left((1-N\mathfrak{p}^{-u-1})^{-1} - (N\mathfrak{p}^{-1}) \right) \right) \\
&\quad \cdot \prod_{\mathfrak{p}\notin\mathbb{P}_1} \left(\prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1} \right) \\
&= \prod_{\mathfrak{p}\in\mathbb{P}_1} \frac{(1-(N\mathfrak{p})^{-1} + (N\mathfrak{p})^{-u-2})}{(1-N\mathfrak{p}^{-1})(1-N\mathfrak{p}^{-u-1})} \prod_{\mathfrak{p}\notin\mathbb{P}_1} \left(\prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1} \right).
\end{aligned}$$

Dann gilt für den u-Inhalt:

$$\begin{aligned} I_u &= \frac{\zeta_\infty(f;u)}{\zeta_\infty(u)} \\ &= \frac{\prod_{\mathfrak{p}\in\mathbb{P}_1} \frac{(1-(N\mathfrak{p})^{-1})+(N\mathfrak{p})^{-u-2}}{(1-N\mathfrak{p}^{-1})(1-N\mathfrak{p}^{-u-1})} \prod_{\mathfrak{p}\notin\mathbb{P}_1} \left(\prod_{1\le j\le\infty}(1-N\mathfrak{p}^{-j-u})^{-1}\right)}{\prod_{\mathfrak{p}\in\mathbb{P}} \left(\prod_{1\le j\le\infty}(1-N\mathfrak{p}^{-j-u})^{-1}\right)} \\ &= \prod_{\mathfrak{p}\in\mathbb{P}_1} \left(\frac{(1-(N\mathfrak{p})^{-1})+(N\mathfrak{p})^{-u-2}}{(1-(N\mathfrak{p})^{-u-1})(1-(N\mathfrak{p})^{-1})} \prod_{i=u+1}^{\infty} (1-(N\mathfrak{p})^{-i}) \right). \end{aligned}$$

□

6.3.6 Beispiel:
Sei L ein $\mathbb{P}_1$-Modul mit $|L| = l$, dann ist der u-Erwartungwert, dass der $\mathbb{P}_1$-Anteil eines endlichen A-Moduls isomorph zu L ist:

$$l^{-u}\left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\in\mathbb{P}_1} \frac{\prod_{1\le j}(1-(N\mathfrak{p})^{-j})}{\prod_{1\le i\le u}(1-(N\mathfrak{p})^{-i})}.$$

Für den 0-Inhalt gilt:

$$\left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\in\mathbb{P}_1} \prod_{1\le j} (1-(N\mathfrak{p})^{-j}).$$

Beweis: Es gilt:

$$\begin{aligned} \zeta_\infty(f,u) &= \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} w(M) f(M) (N\mathfrak{a})^{-u} \\ &= \sum_{\mathfrak{a}} \sum_{\substack{M(\mathfrak{a}),\\ M_{\mathbb{P}_1}\cong L}} w(M) (N\mathfrak{a})^{-u} \\ &= l^{-u}\left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\notin\mathbb{P}_1} \prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1}. \end{aligned}$$

Damit ergibt sich für den u-Inhalt:

$$\begin{aligned} I_u &= \frac{\zeta_\infty(f;u)}{\zeta_\infty(u)} \\ &= \frac{l^{-u}\left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\notin\mathbb{P}_1} \prod_{1\le j\le\infty}(1-N\mathfrak{p}^{-j-u})^{-1}}{\prod_{\mathfrak{p}\in\mathbb{P}} \prod_{1\le j\le\infty}(1-N\mathfrak{p}^{-j-u})^{-1}} \\ &= l^{-u}\left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\in\mathbb{P}_1} \prod_{1\le j\le\infty} (1-N\mathfrak{p}^{-j-u})^{-1}. \end{aligned}$$

□

Globale Situation

Wenn wir $\mathbb{P}_1 = \mathbb{P}$ zulassen, können wir die Beispiele der semilokalen Situation auf (globale) endliche A-Moduln übertragen, wie die nächsten beiden Beispiele zeigen.

6.3.7 Beispiel:
Der u-Inhalt, dass ein endlicher A-Modul zyklisch ist (d.h. $M_{\mathbb{P}_1} \cong A/\mathfrak{a}$), ist

$$\prod_{\mathfrak{p}\in\mathbb{P}} \left(\frac{(1-(N\mathfrak{p})^{-1}) + (N\mathfrak{p})^{-u-2}}{(1-(N\mathfrak{p})^{-u-1})(1-(N\mathfrak{p})^{-1})} \prod_{i=u+1}^{\infty} (1-(N\mathfrak{p})^{-i}) \right).$$

Der 0-Inhalt, dass ein endlicher A-Modul zyklisch ist, ist

$$\prod_{\mathfrak{p}\in\mathbb{P}} \left(\frac{(1-(N\mathfrak{p})^{-1}) + (N\mathfrak{p})^{-2}}{(1-(N\mathfrak{p})^{-1})} \prod_{i=2}^{\infty} (1-(N\mathfrak{p})^{-i}) \right).$$

Der 1-Inhalt, dass ein endlicher A-Modul zyklisch ist, ist

$$\prod_{\mathfrak{p}\in\mathbb{P}} \left(\left((1-(N\mathfrak{p})^{-1}) + (N\mathfrak{p})^{-2}\right) \prod_{i=3}^{\infty} (1-(N\mathfrak{p})^{-i}) \right).$$

6.3.8 Beispiel:
Sei L ein Modul mit $|L| = l$. Dann ist der u-Erwartungwert, dass ein endlicher A-Modul isomorph zu L ist:

$$l^{-u} \left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\in\mathbb{P}} \frac{\prod_{1\le j}(1-(N\mathfrak{p})^{-j})}{\prod_{1\le i\le u}(1-(N\mathfrak{p})^{-i})}.$$

Für den 0-Inhalt gilt:

$$\left(|Aut(L)|^{-1}\right) \prod_{\mathfrak{p}\in\mathbb{P}} \prod_{1\le j} (1-(N\mathfrak{p})^{-j}).$$

Wir können noch weitere Aussagen treffen.

6.3.9 Beispiel:
Sei M ein endlicher A-Modul und $\alpha \in \mathbb{R}$, dann ist für $u > \alpha$ der u-Erwartungswert von $f(M) = |M|^{\alpha}$

$$E_u(|M|^{\alpha}) = \frac{C_u}{C_\infty} \prod_{1\le j} \zeta_A(j+u-\alpha).$$

Beweis: Wir berechnen zunächst:

$$\begin{aligned}\zeta_\infty(f,u) &= \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} w(M) f(M) (N\mathfrak{a})^{-u} \\ &= \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} |Aut(M)|^{-1} |M|^{\alpha} (N\mathfrak{a})^{-u}.\end{aligned}$$

Dann gilt für den u-Erwartungswert:

$$\begin{aligned}E_u(f) &= \zeta_\infty(f;u)\frac{C_u}{C_\infty} \\ &= \frac{C_u}{C_\infty} \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} |Aut(M)|^{-1} |M|^{\alpha} (N\mathfrak{a})^{-u} \\ &= \frac{C_u}{C_\infty} \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} |Aut(M)|^{-1} (N\mathfrak{a})^{-(u-\alpha)} \\ &= \frac{C_u}{C_\infty} \zeta_\infty(u-\alpha) \\ &= \frac{C_u}{C_\infty} \prod_{j=1}^{\infty} \zeta_A(j+u-\alpha).\end{aligned}$$

Der u-Erwartungswert ist:

$$E_u(|M|^{\alpha}) = \frac{C_u}{C_\infty} \prod_{j=1}^{\infty} \zeta_A(j+u-\alpha).$$

□

6.3.10 Beispiel:
Der Inhalt, dass ein A-Modul elementar ist, ist

$$\left(\prod_{\substack{k \not\equiv 1,4 \bmod 5 \\ k \geq 2}} \zeta_A(k)^{-1} \right) = 1 - q^{-1} - q^{-2} + q^{-3} - q^{-4} + q^{-5} \ldots.$$

Der 1-Inhalt, dass ein A-Modul elementar ist, ist

$$\left(\prod_{\substack{k \not\equiv 2,3 \bmod 5 \\ k \geq 2}} \zeta_A(k)^{-1} \right) = 1 - q^{-3} - q^{-4} - q^{-5} + q^{-7} \ldots.$$

Beweis: Zunächst erhalten wir:

$$\begin{aligned}
\zeta_\infty(f,u) &= \sum_{\mathfrak{a}} \sum_{M(\mathfrak{a})} w(M) f(M) (N\mathfrak{a})^{-u} \\
&= \prod_{\mathfrak{p}} \sum_{k_\mathfrak{p}=0}^{\infty} w((A/\mathfrak{p})^{k_\mathfrak{p}}) ((N\mathfrak{p})^{k_\mathfrak{p}})^{-u} \\
&= \prod_{\mathfrak{p}} \sum_{k_\mathfrak{p}=0}^{\infty} \frac{1}{(N\mathfrak{p})^{k_\mathfrak{p}^2}} \frac{1}{\prod_{1\le i\le k_\mathfrak{p}} (1-(N\mathfrak{p})^{-i})} ((N\mathfrak{p})^{k_\mathfrak{p}})^{-u} \\
&= \prod_{\mathfrak{p}} \sum_{k_\mathfrak{p}=0}^{\infty} \frac{1}{\prod_{1\le i\le k_\mathfrak{p}} (1-(N\mathfrak{p})^{-i})} ((N\mathfrak{p})^{k_\mathfrak{p}})^{-u-k_\mathfrak{p}}.
\end{aligned}$$

Für $u = 0$ folgt mit den Rogers-Ramanujan-Identitäten 2.3.2

$$\begin{aligned}
\zeta_\infty(f,u) &= \prod_{\mathfrak{p}} \sum_{k_\mathfrak{p}=0}^{\infty} \frac{1}{\prod_{1\le i\le k_\mathfrak{p}} (1-(N\mathfrak{p})^{-i})} (N\mathfrak{p}^{-1})^{k_\mathfrak{p}^2} \\
&\overset{(2.3.2)}{=} \prod_{\mathfrak{p}} \prod_{n=1}^{\infty} \frac{1}{(1-((N\mathfrak{p})^{-1})^{5n-1})\,(1-((N\mathfrak{p})^{-1})^{5n-4})}.
\end{aligned}$$

Somit gilt für den Inhalt unter Verwendung von 6.1.8:

$$\begin{aligned}
I &= \lim_{u\to 0} \frac{\zeta_\infty(f;u)}{\zeta_\infty(u)} \\
&= \frac{\prod_{\mathfrak{p}} \prod_{n=1}^{\infty} \left(1-((N\mathfrak{p})^{-1})^{5n-1}\right)^{-1} \left(1-((N\mathfrak{p})^{-1})^{5n-4}\right)^{-1}}{\prod_{\mathfrak{p}} \prod_{n=1}^{\infty} \left(1-((N\mathfrak{p})^{-1})^{n}\right)^{-1}} \\
&= \prod_{\substack{k\ge 2 \\ k\not\equiv 1,4 \bmod 5}} \zeta_A(k)^{-1}.
\end{aligned}$$

Für $u = 1$ folgt mit den Rogers-Ramanujan-Identitäten 2.3.2

$$\begin{aligned}
\zeta_\infty(f,u) &= \prod_{\mathfrak{p}} \sum_{k_\mathfrak{p}=0}^{\infty} \frac{1}{\prod_{1\le i\le k_\mathfrak{p}} (1-(N\mathfrak{p})^{-i})} (N\mathfrak{p}^{-1})^{k_\mathfrak{p}(k_\mathfrak{p}+1)} \\
&\overset{(2.3.2)}{=} \prod_{\mathfrak{p}} \prod_{n=1}^{\infty} \frac{1}{(1-((N\mathfrak{p})^{-1})^{5n-2})\,(1-((N\mathfrak{p})^{-1})^{5n-3})}.
\end{aligned}$$

Dann gilt für den 1-Inhalt, wieder unter Verwendung von 6.1.8:

$$
\begin{aligned}
I_1 &= \lim_{u\to 1} \frac{\zeta_\infty(f;u)}{\zeta_\infty(u)} \\
&= \frac{\prod_{\mathfrak{p}} \prod_{n=1}^{\infty} \left(1-((N\mathfrak{p})^{-1})^{5n-2}\right)^{-1} \left(1-((N\mathfrak{p})^{-1})^{5n-3}\right)^{-1}}{\prod_{\mathfrak{p}} \prod_{n=2}^{\infty} \left(1-((N\mathfrak{p}))^{-1})^{n}\right)^{-1}} \\
&= \prod_{\substack{k\geq 2 \\ k\not\equiv 2,3 \bmod 5}} \zeta_A(k)^{-1}.
\end{aligned}
$$

□

Theoretisch könnten wir wie in Kapitel 3 Varianzen und Kovarianzen berechnen, allerdings stellt sich dann die Frage, ob diese über einem Inhaltsraum die gleiche Interpretation haben wie über einem Wahrscheinlichkeitsraum. Über Wahrscheinlichkeitsräumen stellt die Varianz ein Streuungsmaß für die Verteilung um den Mittelwert dar, dies muss über Inhaltsräumen neu definiert werden, da wir keine σ-Additivität haben. Zunächst müsste überprüft werden, ob es eine sinnvolle Definition und eventuell eine ähnliche Formel wie in 2.4.3 gibt. Ist dies der Fall, so stellt sich die Frage der Konvergenz der berechneten Reihen.

Kapitel 7

Zusammenfassung und Ausblick

Abschließend fassen wir die Resultate dieser Arbeit nochmal zusammen. Zunächst werden wir auf die Ergebnisse eingehen, die wir für $\mathfrak{p}$-Moduln für ein fixiertes Primideal $\mathfrak{p}$ erhalten haben und anschließend die Resultate der globalen Theorie zusammentragen.
In Kapitel 3 haben wir gesehen, dass wir einen natürlichen stochastischen Prozess zum Erzeugen von $\mathfrak{p}$-Moduln erhalten und mit Hilfe der Automorphismengruppe ein Wahrscheinlichkeitsmaß auf der Menge aller $\mathfrak{p}$-Moduln definieren können. Als konkrete Ergebnisse haben wir die Wahrscheinlichkeiten dafür, dass ein Modul zyklisch, elementar bzw. zyklisch und elementar ist mit zugehörigen Varianzen und Kovarianzen berechnet. Des Weiteren wurden die Wahrscheinlichkeiten bestimmt, dass ein Modul der triviale Modul ist oder Rang zwei hat. Zum Abschluss des Kapitels haben wir die Wahrscheinlichkeit bestimmt, dass ein vorgegebener Modul M von einem zufälligen Element x erzeugt wird.
Der Zusammenhang zwischen der Cohen-Lenstra-Heuristik und Partitionen sowie die zugehörige Theorie der Cohen-Lenstra-Abbildung wurde in Kapitel 4 dazu benutzt, die Wahrscheinlichkeit anzugeben, mit der ein $\mathfrak{p}$-Modul einen Exponenten kleiner oder gleich einer bestimmten Schranke hat.
Mit Hilfe der Interpretation der Cohen-Lenstra-Heuristik mittels Konjugationsklassen der allgemeinen linearen Gruppe über einem endlichen Körper wurden in Kapitel 5 die Wahrscheinlichkeiten, dass ein $\mathfrak{p}$-Modul einen betimmten Rang hat sowie die Wahrscheinlichkeiten, dass ein $\mathfrak{p}$-Modul einen bestimmten Rang und eine feste Ordnung besitzt, angegeben. Genau wie in Kapitel 4 wurde auch mit Hilfe dieser Theorie die Wahrscheinlichkeit, mit der ein $\mathfrak{p}$-Modul einen Exponenten kleiner oder gleich einer bestimmten Schranke hat, angeführt.
In Kapitel 6 haben wir die globale Theorie entwickelt und mit Hilfe der Zeta-Funktionen und einem Tauber-Satz eine effektive Methode gefunden, um die vorher definierten Inhalte und Erwartungswerte zu berechnen. Als Nebenresultat haben wir gesehen, dass sich die einzelnen $\mathfrak{p}$-Komponenten eines endlichen

Moduls unabhängig voneinander verhalten. Zunächst konnten wir überprüfen, dass diese Theorie auch im Spezialfall der lokalen Situation funktioniert. Dazu wurden die Wahrscheinlichkeit, dass ein $\mathfrak{p}$-Modul nicht der triviale Modul ist, die Wahrscheinlichkeit, dass ein $\mathfrak{p}$-Modul einen bestimmten Rang hat sowie die Wahrscheinlichkeit, dass ein $\mathfrak{p}$-Modul eine vorgegebene Ordnung besitzt, berechnet. In der semilokalen Situation konnten wir bestimmen, wie wahrscheinlich es ist, dass für eine Teilmenge $\mathbb{P}_1$ der Menge aller Primideale in A ein $\mathbb{P}_1$-Modul zyklisch ist bzw. dass der $\mathbb{P}_1$-Anteil isomorph zu einem vorgegebenen Modul ist. Diese beiden Beispiele wurden auf die allgemeine Situation übertragen. Zudem wurde noch die Wahrscheinlichkeit angegeben, dass ein endlicher A-Modul elementar ist.

Es ist möglich, mittels der behandelten Theorien noch weitere Ergebnisse über endliche A-Moduln zu erhalten. So könnte man z.B. untersuchen, wie wahrscheinlich es ist, dass r zufällige Elemente einen zufälligen Modul erzeugen. Allerdings erfordert dies einen geschickten Umgang mit q-Reihen und Zeta-Funktionen.
In der globalen Theorie könnte untersucht werden, ob es auch über Inhaltsräumen möglich ist, Varianzen und Kovarianzen sinnvoll zu definieren.

Literaturverzeichnis

[AE04] George E. Andrews and Kimmo Eriksson, *Integer partitions*, Cambridge University Press, Cambridge, 2004. MR 2122332 (2006b:11125)

[And98] George E. Andrews, *The theory of partitions*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1998, Reprint of the 1976 original. MR 1634067 (99c:11126)

[Bos06] Siegfried Bosch, *Lineare Algebra*, 3. ed., Springer-Verlag, Berlin, Heidelberg, New York, 2006.

[CL84] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR 756082 (85j:11144)

[Ful97] Jason Edward Fulman, *Probability in the classical groups over finite fields: Symmetric functions, stochastic algorithms, and cycle indices*, ProQuest LLC, Ann Arbor, MI, 1997, Thesis (Ph.D.)–Harvard University. MR 2695900

[Ful99] Jason Fulman, *A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups*, J. Algebra **212** (1999), no. 2, 557–590. MR 1676854 (2000c:20072)

[Hal38] P. Hall, *A partition formula connected with Abelian groups*, Comment. Math. Helv. **11** (1938), no. 1, 126–129. MR 1509594

[Kre05] Ulrich Krengel, *Einführung in die Wahrscheinlichkeitstheorie und Statistik*, 8. ed., Vieweg Verlag, Wiesbaden, 2005.

[Lan69] Serge Lang, *Analysis II*, Addison–Wesley Publishing Company, Inc., 1969.

[Len09] Johannes Lengler, *The Cohen–Lenstra heuristic for finite abelian groups, Doktorarbeit*, Universität des Saarlandes, Saarbrücken, Germany, 2009.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657 (2003d:11171)