Kokerne zufälliger p-adischer Matrizen und deren Zusammenhang mit der Cohen-Lenstra Heuristik

Bachelorarbeit von Malte Londschien
unter der Aufsicht von Prof. Richard Pink

Mai 2017

Inhaltsverzeichnis

Einleitung **2**

Notation **3**

1 Eine natürliche Wahrscheinlichkeitsdichte für Isomorphieklassen abelscher Gruppen einer festen Ordnung **3**

2 Die Verteilung von Kokernen p-adischer Matrizen via des Haarschen Mass **4**
2.1 Die p-adischen Zahlen 5
2.2 Ein Auflug in die Kommutative Algebra 7
2.3 p-adische Matrizen 9
2.4 Wahrscheinlichkeitsdichten für Isomorphieklassen endlicher abelscher p-Gruppen. . 11

3 Allgemeine Aussagen zu Zahlkörpern und deren Idealklassengruppen **12**

4 Die Cohen–Lenstra Heuristik **14**
4.1 Wahrscheinlickeitsdichten für Isomorphieklassen endlicher abelscher Gruppen . . . 14
4.2 Die Cohen–Lenstra Vermutung 19
4.3 Motivation für die Cohen Lenstra Heuristik 20
4.4 Der gerade Anteil der Klassengruppe und nichtquadratische Zahlkörper 21

Einleitung

Eine wichtige Grundlage der elementaren Zahlentheorie liefert der Satz der eindeutigen Primfaktorzerlegung für natürliche Zahlen. Die in der algebraischen Zahlentheorie studierten Glanzheitsringe von Zahlkörpern verallgemeinern den Begriff der ganzen Zahlen. Das Fehlen einer Primfaktorzerlegung in einigen Ganzheitsringen erschwert dort das Beweisen diverser Aussagen. Kummer erkannte dies, als sein Beweis für Fermats letzten Satz für Primzahlen scheiterte, für die der Ganzheitsring des dazugehörigen Kreisteilungskörper die gewünschte Eigenschaft der eindeutigen Zerlegung nicht besass.

Ein Ansatz, um dieses Hindernis zu umgehen, lieferte seine Theorie der idealen Zahlen. Diese führte später zu Dedekinds Definition der Ideale und folgend zu der modernen Definition der Idealklassengruppe eines Dedekindrings. Es stellt sich heraus, dass die Primfaktorzerlegung im Ganzheitsring genau dann scheitert, wenn die Idealklassengruppe des dazugehörigen Zahlkörpers nichttrivial ist, und dass Kummers Beweis für Primzahlen, die die Ordnung der Idealklassengruppe des dazugehörigen Kreisteilungskörper nicht teilen, gültig ist.

Wegen der so in den Klassengruppen von Zahlkörpern enthaltenen Information ist es von grossem Interesse diese zu beschreiben, was sich aufgrund der Komplexität der unterliegenden Theorie jedoch als sehr schwierig herausstellt. Viele elementare Fragen, wie die Existenz unendlich vieler, in den komplexen Zahlen enthaltener Zahlkörper mit trivialer Idealklassengruppe, sind bis heute offen.

H. Cohen und H. W. Lenstra beobachteten, dass für bestimmte Folgen an Zahlkörpern die dazugehörige Folge der Idealklassengruppen sich wie eine bezüglich einer gewissen Wahrscheinlichkeitsdichte zufällige Folge abelscher endlicher Gruppen zu verhalten scheint. Sie veröffentlichten in 1983 eine Arbeit [2], in der sie dieses probabilistische Phänomen für Klassengruppen imaginärquadratischer respektive total reeller Zahlkörper festen Erweiterungsgrads mithilfe einer Heuristik beschrieben. Die Heuristik beruht dabei auf der Idee, Gruppen mit einem Faktor invers proportional zur Ordnung ihrer Automorphismengruppe zu gewichten.

Im folgenden Text werden wir zunächst in Abschnitten 1 und 2 herleiten, wie die von Cohen und Lenstra verwendete Wahrscheinlichkeitsdichte natürlich auftritt. Somit liefern wir eine Motivation für die so genannte Cohen–Lenstra Heuristik. Es stellt sich heraus, dass man durch die Beschränkung auf Gruppen von Primpotenzordnung das Problem vereinfacht, ohne an Allgemeinheit zu verlieren. Wir werden zeigen, dass abelsche p-Gruppen mit einer Wahrscheinlichkeit invers proportional zu der Ordnung ihrer Automorphismengruppe als Kokerne mit dem natürlichen Haarmass versehener p-adischer Matrizen auftreten. Danach werden wir genauer auf die von Cohen und Lenstra präsentierte Heuristik eingehen und mithilfe der bewiesenen Aussage einige von Cohen und Lenstra erwähnte Phänomene konkretisieren und alternative Beweise für bestimmte Aussagen liefern.

Für die Lektüre des folgenden Textes werden Kenntnisse der Kommutativen Algebra sowie der algebraischen Zahlentheorie, die man unter anderem durch die Lektüre von Atiyah und MacDonalds *Introduction to Commutative Algebra* [1] und Neurkirchs *Algebraische Zahlentheorie* [10] erwerben kann, voraus gesetzt. Allerdings werde ich für meine Arbeit wichtige Definitionen und Fakten, auch wenn ich von dessen Kenntnis ausgehe, zur Erinnerung und zum Vorbeugen von Missverständnissen in Abschnitten 2.2 und 3 erwähnen.

Abschnitt 1 habe ich aus einem Gespräch mit Prof. Richard Pink übernommen. Abschnitt 2 dient als Vorbereitung für den Beweis des Satzes 2.37, dessen Beweis ich für den Fall quadratischer Matrizen aus [5] übernommen, und nach Anregung von Prof. Pink auf den nichtquadratischen Fall verallgemeinert habe. Abschnitt 3 folgt Neukirchs Buch, Abschnitt 4 zu einem grossen Teil der Veröffentlichung von H. Cohen und H. W. Lenstra [2]. Genauer sind Definition 4.1, die die Erarbeitung des Unterabschnitts 4.1 motivierte, sowie Unterabschnitt 4.2 von dort übernommen. Einen anderen Zugang zu diesem Thema liefert J. Lengler in seiner Dissertation [8], in welcher er mithilfe von Partitionen ähnliche Ergebnisse zeigt und aus dessen Text ich manche Beispiele übernommen habe. Letztlich ist die Heuristik aus Unterabschnitt 4.3, die die Verteilung Kokerne p-adischer Matrizen mit der Distribution von Klassengruppen quadratischer Zahlkörper verbindet,

aus einem Gespräch mit Prof. Pink entnommen.

Ich möchte mich hier bei Prof. Richard Pink und Alexandre Puttick für die lehrreiche Betreuung und die zahlreichen Verbesserungsvorschläge zu früheren Versionen dieser Arbeit bedanken.

Notation

Für zwei Mengen $A \subset B$ ist die charakteristische Funktion von A definiert als

$$1_A : B \to \{0,1\},\ x \mapsto \begin{cases} 1 & x \in A \\ 0 & x \notin A. \end{cases}$$

Für ein Wahrscheinlichkeitsmass $\mathbb{P}$ und eine komplexwertige Zufallsvariable f ist $\mathbb{E}_{\mathbb{P}}(f)$ der Erwartungswert von f via $\mathbb{P}$.

Für eine Isomorphieklasse $\mathfrak{G}$ einer endlichen Gruppe bezeichne $|\mathfrak{G}|$ die Ordnung eines Repräsentanten der Isomorphieklasse und $\mathrm{Aut}(\mathfrak{G})$ die Isomorphieklasse der Automorphismengruppe eines Repräsentanten. Für eine endliche, abelsche Gruppe G sei $[G]$ die Isomorphieklasse von G.
Um Verwirrung zu vermeiden werde ich im Folgenden Fraktur für Isomorphieklassen, Druckschrift für Gruppen verwenden.

1 Eine natürliche Wahrscheinlichkeitsdichte für Isomorphieklassen abelscher Gruppen einer festen Ordnung

Sei N eine positive ganze Zahl und X eine Menge der Kardinalität N. Sei weiterhin $\mathcal{F}_X$ die Menge aller Verknüpfungen $\circ : X \times X \to X,\ (x,y) \mapsto x \circ y$, die auf X eine abelsche Gruppenstruktur definieren. Sei $\mathcal{G}_{\{N\}}$ die Menge der Isomorphieklassen abelscher Gruppen von Ordnung N.

Satz 1.1. *Für jede Teilmenge $Y \subset \mathcal{F}_X$ setze $\mu(Y) := \frac{|Y|}{|\mathcal{F}_X|}$, was offenbar ein Wahrscheinlichkeitsmass auf $\mathcal{F}_X$ definiert. Dann gilt für jede endliche abelsche Gruppe der Ordnung N*

$$\mu(\{\circ \in \mathcal{F}_X | (X,\circ) \cong G\}) = \frac{|\operatorname{Aut}(G)|^{-1}}{\sum_{\mathfrak{G} \in \mathcal{G}_{\{N\}}} |\operatorname{Aut}(\mathfrak{G})|^{-1}}.$$

Beweis. Betrachten wir die symmetrische Gruppe S_X und definieren für alle $\sigma \in S_X$ und $x, y \in X$

$$\circ_\sigma : X \times X \to X,\ (x,y) \mapsto x \circ_\sigma y := \sigma(\sigma^{-1}(x) \circ \sigma^{-1}(y))$$

wodurch folgendes Diagramm kommutiert

$$\begin{array}{ccc} X \times X & \xrightarrow{\circ} & X \\ \downarrow{\scriptstyle \sigma} \quad \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ X \times X & \xrightarrow{\circ_\sigma} & X. \end{array}$$

Bezeichnen wir für $\circ \in \mathcal{F}_X$ mit $1_\circ$ das neutrale Element von $(X,\circ)$. Man kann leicht nachprüfen, dass $(X, \circ_\sigma))$ mit neutralem Element $\sigma(1_\circ)$ eine abelsche Gruppe ist. Für alle $\sigma \in S_X$ bildet $\circ \mapsto \circ_\sigma$ also Gruppenoperationen auf X wieder auf solche ab. Eine kurze Rechnung zeigt, dass für alle $\sigma \in S_X, \circ \in \mathcal{F}_X$ und $x, y \in X$

$$\begin{aligned} x(\circ_\tau)_\sigma y &= \sigma(\sigma^{-1}(x) \circ_\tau \sigma^{-1}(y)) \\ &= \sigma\tau(\tau^{-1}\sigma^{-1}(x) \circ \tau^{-1}\sigma^{-1}(y)) \\ &= x \circ_{\sigma\tau} y \end{aligned}$$

ist. Mit $\circ_{id} = \circ$ folgt, dass die Abbildung $(\sigma, \circ) \mapsto \circ_\sigma$ eine Linksoperation von S_X auf $\mathcal{F}_X$ ist.

Die Bahnen der einzelnen Verknüpfungen sind mit σ als Isomorphismus Äquivalenzklassen von $\mathcal{F}_X$ unter Gruppenisomorphie. Seien $\circ_1, \ldots, \circ_r$ Repräsentanten dieser Bahnen.

Folgende Rechnung zeigt, dass die Abbildung $\sigma : X \to X$ genau dann ein Automorphismus von $(X, \circ)$ ist, wenn sie im Stabilisator von $\circ$ liegt.

$$\sigma(x \circ y) = \sigma(x) \circ \sigma(y) \iff x \circ y = \sigma^{-1}(\sigma(x) \circ \sigma(y)) = x \circ_{\sigma^{-1}} y$$

Dies zeigt, dass $\mathrm{Aut}(X, \circ) = \mathrm{Stab}_{S_X}(\circ)$ ist. Bezeichnen wir für $\circ \in \mathcal{F}_X$ mit $S_X \cdot \circ$ die Bahn von $\circ$ unter S_X und mit $[\circ]$ dessen Isomorphieklasse. Aus den Bahnengleichungen folgt dann

$$|S_X \cdot \circ| = |[\circ]| = \frac{|S_X|}{|\mathrm{Stab}_{S_X}(\circ)|} = \frac{N!}{|\mathrm{Aut}(X, \circ)|}$$

sowie

$$|\mathcal{F}_X| = \sum_{i=1}^{r} |S_X \cdot \circ_i| = \sum_{i=1}^{r} \frac{|S_X|}{|\mathrm{Stab}_{S_X}(\circ_i)|} = \sum_{i=1}^{r} \frac{N!}{|\mathrm{Aut}(X, \circ_i)|}.$$

Dies zeigt die Behauptung

$$\mu(\{\circ \in \mathcal{F}_X | (X, \circ) \cong G\}) = \frac{|\{\circ \in \mathcal{F}_X | (X, \circ) \cong G\}|}{|\mathcal{F}_X|} = \frac{|\mathrm{Aut}(G)|^{-1}}{\sum_{\mathfrak{G} \in \mathcal{G}_{\{N\}}} |\mathrm{Aut}(\mathfrak{G})|^{-1}}.$$

□

Beispiel 1.2. Seien $N = p^2$ für eine Primzahl p und X eine Menge der Kardinalität N. Nach dem Klassifikationssatz für abelsche Gruppen ist jede abelsche Gruppe der Ordnung N isomorph zu entweder $\mathbb{Z}/p^2\mathbb{Z}$ oder $(\mathbb{Z}/p\mathbb{Z})^2$. Jedes Element $\varphi \in \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ ist für einen beliebigen Erzeugenden $g \in \mathbb{Z}/p^2\mathbb{Z}$ eindeutig bestimmt durch das Bild $\varphi(g)$, welches aufgrund der Injektivität von φ wieder ein Erzeugender ist. Es ist

$$\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \text{ via } \varphi \mapsto \varphi(g).$$

Im Weiteren entsprechen Gruppenautomorphismen auf $(\mathbb{Z}/p\mathbb{Z})^2$ bijektiven linearen Transformationen auf $(\mathbb{Z}/p\mathbb{Z})^2$ als $\mathbb{F}_p$–Vektorraum. Also ist

$$\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{F}_p).$$

Mit $|(\mathbb{Z}/p^2\mathbb{Z})^\times| = p^2 - p$ und $|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{j=0}^{n-1}(p^n - p^j)$ gilt nach Satz 1.1

$$\mu(\{\circ \in \mathcal{F}_X | \ (\{1, \ldots, N\}, \circ) \cong \mathbb{Z}/p^2\mathbb{Z}\}) = \frac{p^2 - 1}{p^2},$$
$$\mu(\{\circ \in \mathcal{F}_X | \ (\{1, \ldots, N\}, \circ) \cong (\mathbb{Z}/p\mathbb{Z})^2\}) = \frac{1}{p^2}.$$

2 Die Verteilung von Kokernen p-adischer Matrizen via des Haarschen Mass

In Abschnitt 1 haben wir eine natürliche Wahrscheinlichkeitsdichte für die Menge von Isomorphieklassen abelscher Gruppen einer festen Odnung hergeleitet. Möchte man diese Wahrscheinlichkeitsdichte für Gruppen beliebiger Ordnungen verallgemeinern, stellt sich die Frage, wie der Gewichtungsfaktor in Abhängigkeit von der Ordnung zu wählen ist. Um dieses Problem zu lösen, erarbeiten wir eine alternative natürliche Methode, endliche abelsche Gruppen zufällig zu generieren.

Für jedes $n \geqslant 0$ kann jede abelsche Gruppe, die von nicht mehr als n Elementen erzeugt werden kann, beschrieben werden als $\mathbb{Z}$-Modul mit n Erzeugenden $\{e_1, \ldots, e_n\}$ versehen mit einer Anzahl

m Relationen der Form $\sum_{i=1}^{n} a_{ij}e_i = 0$ mit $a_{ij} \in \mathbb{Z}$ für $1 \leqslant j \leqslant m$. Fixieren wir die Anzahl Relationen $m(n)$ in Abhängigkeit von n, so gibt uns für alle $n \geqslant 0$ jede Wahrscheinlichkeitsverteilung auf $\mathbb{Z}$ durch zufällige Wahl der a_{ij} eine solche auf der Menge der Isomorphieklassen abelscher Gruppen vom Rang nicht grösser als n. Nehmen wir an, diese konvergieren für immer wachsendes n, so ist die resultierende Dichte nur noch abhängig von dem Wahrscheinlichkeitsmass auf $\mathbb{Z}$ und der Abhängigkeit $m(n)$. Könnten wir eine natürliche Wahrscheinlichkeitsdichte auf $\mathbb{Z}$ wählen, so wäre der Grenzwert der Wahrscheinlichkeitsdichten also fast natürlich.

Leider existiert kein natürliches Wahrscheinlichkeitsmass auf $\mathbb{Z}$. Wir umgehen dieses Problem, indem wir uns auf abelsche p-Gruppen beschränken und $\mathbb{Z}$ durch den Ring der p-adischen ganzen Zahlen $\mathbb{Z}_p$ ersetzen, der mit dem normierten Haarschen Mass eine natürliche Wahrscheinlichkeitsdichte annimmt. Mit dem selben Verfahren wie oben für für $\mathbb{Z}$ erwähnt, erhalten wir so für alle $n, m \geqslant 0$ Wahrscheinlichkeitsmasse auf Isomorphieklassen abelscher p-Gruppen. Wählen wir dabei die Anzahl Relationen $m \geqslant n$, so kann man zeigen, dass das so induzierte Mass der Menge aller Isomorphieklassen abelscher Gruppen unendlicher Ordnung Null ist. Wir erhalten somit bei Konvergenz der Masse für $n \to \infty$ ein bis auf die Wahl der Abhängigkeit von $m(n)$ von n natürliches Wahrscheinlichkeitsmass für Isomorphieklassen abelscher p-Gruppen. Später werden wir zeigen, dass wir durch die Reduktion auf p-Gruppen nicht an Allgemeinheit verlieren.

Im Folgenden werden wir die oben erwähnten Wahrscheinlichkeitsdichten explizit ausrechnen. Wir modellieren dabei die Relationen $\sum_{i=1}^{n} a_{ij}e_i$ auf den Erzeugenden $e_i \in \mathbb{Z}_p^n$ mit einer zufälligen Matrix $A \in \mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$ mit $(A)_{ij} = a_{ij}$ und die Gruppe als $\mathbb{Z}_p^n / \mathrm{Bild}(A) = \mathrm{Koker}(A)$.

2.1 Die p-adischen Zahlen

Definition 2.1. Sei G eine abelsche Gruppe und μ ein Mass auf G. Dieses wird *translationsinvariant* genannt, falls für alle messbare $A \subset G$ und alle $x \in G$ auch $x + A$ messbar mit Mass $\mu(x + A) = \mu(A)$ ist. Ein *Haarmass* ist ein nichttriviales, translationsinvariantes Radonmass.

Satz 2.2 (Haar)**.** *Sei G eine lokal kompakte Hausdorffsche Gruppe. Dann existiert ein bis auf einen konstanten Faktor eindeutiges Haarmass auf G. Ist G kompakt, so ist dieses Mass endlich.*

Beweis. Ein Beweis hierzu lässt sich in den meisten Lehrbüchern zur Masstheorie finden, beispielsweise in [11, Kapitel 8]. □

Definition 2.3. Für eine Primzahl p ist der Ring der *p-adischen ganzen Zahlen* $\mathbb{Z}_p$ definiert als der projektive Limes

$$\mathbb{Z}_p := \varprojlim_{n \geqslant 0} \mathbb{Z}/p^n\mathbb{Z}.$$

Definition 2.4. Wir versehen $\mathbb{Z}_p$ mit der durch der Basis

$$\{\{a + p^n\mathbb{Z}_p\} | a \in \mathbb{Z}_p, n \in \mathbb{Z}^{\geqslant 0}\}$$

erzeugten Topologie.

Bemerkung 2.5. Für ein gegebenes $n \geqslant 0$ und eine $a \in \mathbb{Z}_p$ ist der topologische Raum $\mathbb{Z}_p$ die disjunkte Vereinigung

$$\mathbb{Z}_p = \bigcup_{j=0}^{p^n-1} \{j + a + p^n\mathbb{Z}_p\}.$$

Proposition 2.6. *Die p-adischen Zahlen sind mit dieser Topologie bezüglich der Addition eine kompakte Haussdorfsche topologische Gruppe.*

Beweis. Ausführliche Beweise hierzu finden sich in [6]. □

Proposition 2.7. *Sei μ das natürliche Haarmass auf $\mathbb{Z}_p$, normiert sodass $\mu(\mathbb{Z}_p) = 1$ ist. Dieses nimmt auf der in 2.4 genannten Basis die Werte*

$$\mu(\{a + p^n\mathbb{Z}_p\}) = p^{-n}$$

an.

Beweis. Wir berechnen mithilfe der Translationsinvarianz von μ

$$\mu(a + p^n\mathbb{Z}_p) = p^{-n} \sum_{j=0}^{p^n-1} \mu(j + \{a + p^n\mathbb{Z}_p\}) = p^{-n}\mu(\cup_{j=0}^{p^n-1} j + \{a + p^n\mathbb{Z}_p\}) = p^{-n}\mu(\mathbb{Z}_p) = p^{-n}.$$

□

Definition 2.8. Für jedes $a = (a_n)_{n\geqslant 0} \in \mathbb{Z}_p$ mit $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ für alle $n \geqslant 0$ sei

$$\operatorname{ord}_p(a) := \begin{cases} \infty & \text{falls } a = 0 \\ \max\{n \geqslant 0 \,|\, a_n = 0\} & \text{falls } a \neq 0. \end{cases}$$

Die *p-adische Norm* von $a \in \mathbb{Z}_p$ ist

$$|a|_p := \begin{cases} 0 & \text{falls } a = 0 \\ p^{-\operatorname{ord}_p(a)} & \text{falls } a \neq 0. \end{cases}$$

Bemerkung 2.9. Die Abbildung $|\cdot|_p$ ist eine Norm auf $\mathbb{Z}_p$ und die Metrik $d(a, b) := |a - b|_p$ induziert die Topologie auf $\mathbb{Z}_p$ aus Definition 2.4. Man sieht leicht, dass $|\cdot|$ multiplikativ ist.

Proposition 2.10. *Für alle Borelmengen $A \subset \mathbb{Z}_p$ und alle $a \in \mathbb{Z}_p$ ist*

$$\mu(aA) = |a|_p\mu(A).$$

Beweis. Sei $n \geqslant 0$. Wegen der Translationsinvarianz von μ und da $a \cdot p^n\mathbb{Z}_p = p^{n+\operatorname{ord}_p(a)}\mathbb{Z}_p$ ist, stimmt die Aussage auf den Erzeugenden der Borel σ-Algebra. Da Multiplikation mit einem Element mit den grundlegenden Mengenoperationen verträglich ist, stimmt die Aussage für alle Borelmengen. □

Proposition 2.11. *Der Ring $\mathbb{Z}_p$ ist ein diskreter Bewertungsring, das heisst, es existiert ein Körper mit diskreter Bewertung, sodass $\mathbb{Z}_p$ der dazugehörige Bewertungsring ist.*

Beweis. Für alle $a, b \in \mathbb{Z}_p$ gilt

$$\operatorname{ord}_p(ab) = \operatorname{ord}_p(a) + \operatorname{ord}_p(b),$$

$$\operatorname{ord}_p(a + b) \geqslant \min\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\}.$$

Aufgrund der ersten Gleichung ist $\mathbb{Z}_p$ ein Integritätsbereich. Weiterhin ist $\mathbb{Z}_p$ dann der diskrete Bewertungsring der Fortsetung $\operatorname{ord}_p : \operatorname{Quot}(\mathbb{Z}_p) =: \mathbb{Q}_p \to \mathbb{Z}$, $\frac{a}{b} \mapsto \operatorname{ord}_p(a) - \operatorname{ord}_p(b)$ auf $\mathbb{Q}_p$. □

Korollar 2.12. *Folgende Aussagen folgen direkt aus Proposition 2.11:*

(i) Der Ring $\mathbb{Z}_p$ ist lokal mit maximalem Ideal (p).

(ii) Jedes Ideal $\mathfrak{a} \subset \mathbb{Z}_p$ ist von der Form (0) oder (p^n) für ein $n \in \mathbb{Z}^{\geqslant 0}$. Insbesondere ist $\mathbb{Z}_p$ ein Hauptidealring.

(iii) Ein Element $(a_n)_{n\geqslant 0} \in \mathbb{Z}_p$ mit $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ für alle $n \geqslant 0$ ist genau dann eine Einheit, wenn $a_1 \neq 0$ ist.

(iv) Für jedes $a \in \mathbb{Z}_p$ ist $\mathbb{Z}_p/a\mathbb{Z}_p \cong \mathbb{Z}/p^{\operatorname{ord}_p(a)}\mathbb{Z}$.

Beweis. Der Beweis kann beispielsweise in [1, Kapitel 9] nachgelesen werden. □

2.2 Ein Auflug in die Kommutative Algebra

Sei R ein kommutativer Ring mit Eins.

Lemma 2.13. *Seien M, N zwei R-Moduln mit M frei und sei $\mathfrak{a} \subset R$ ein Ideal. Dann ist die Abbildung*

$$\pi : \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{R/\mathfrak{a}}(M/\mathfrak{a}M, N/\mathfrak{a}N),\ f \mapsto (m + \mathfrak{a}M \mapsto f(m) + \mathfrak{a}N)$$

ein surjektiver R-Homomorphismus.

Beweis. Da $\mathfrak{a}M$ im Kern der Verknüpfung der Abbildungen $M \xrightarrow{f} N \twoheadrightarrow N/\mathfrak{a}N$ liegt, ist die gegebene Abbildung wohldefiniert. Sei $\overline{\varphi} \in \mathrm{Hom}_{R/\mathfrak{a}}(M/\mathfrak{a}M, N/\mathfrak{a}N)$ und sei $(m_i)_{i\in I}$ für eine gewisse Indexmenge I eine Basis von M. Wählen wir für alle $i \in I$ ein $n_i \in \overline{\varphi}(\overline{m_i})$. Die Abbildung $\varphi : M \to N,\ \sum_{i\in I} a_i m_i \mapsto \sum_{i\in I} a_i n_i$ liegt in $\mathrm{Hom}_R(M,N)$ und reduziert auf $\overline{\varphi}$. Folglich ist π surjektiv. □

Sei $j(R) = \bigcap_{\substack{\mathfrak{m}\subset R \\ \text{maximal}}} \mathfrak{m}$ das Jacobson-Radikal. Erinnern wir uns an Nakayamas Lemma:

Proposition 2.14. *Sei M ein endlich erzeugter R-Modul und $\mathfrak{a} \subset j(R)$ ein Ideal mit $\mathfrak{a}M = M$. Dann ist $M = 0$.*

Beweis. [1, Prop. 2.6] □

Sei nun R zusätzlich lokal mit maximalem Ideal $\mathfrak{m}$.

Korollar 2.15. *Sei M ein endlich erzeugter R-Modul. Dann erzeugt jede Menge $\{m_1, \dots, m_r\} \subset M$, für die die Menge der dazugehörigen Restklassen den $R/\mathfrak{m}$-Vektorraum $M/\mathfrak{m}M$ erzeugen, bereits M.*

Beweis. [1, Prop 2.8] □

Proposition 2.16. *Seien M, N zwei R-Moduln, sei N endlich erzeugt und sei $\varphi : M \to N$ ein Homomorphismus. Dann ist φ surjektiv genau dann, wenn seine Reduktion $\overline{\varphi} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ surjektiv ist.*

Beweis. Die Reduktion $\overline{\varphi} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ eines Epimorphismus $\varphi : M \to N$ ist surjektiv.

Sei umgekehrt $\varphi : M \to N$ sodass seine Reduktion $\overline{\varphi} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ surjektiv ist und sei M für eine gewisse Indexmenge I von $\{m_i\}_{i\in I}$ erzeugt. Aufgrund der Surjektivität von $\overline{\varphi}$ und dem Fakt, dass N endlich erzeugt ist, existiert ein $r \geqslant 0$ und $i_1, \dots, i_r \in I$, sodass die $\overline{\varphi}(\overline{m_{i_1}}) = \overline{\varphi(m_{i_1})}, \dots, \overline{\varphi}(\overline{m_{i_r}}) = \overline{\varphi(m_{i_r})}$ den Modul $N/\mathfrak{m}N$ erzeugen. Nach Korollar 2.15 erzeugen die $\varphi(m_{i_j})$ für $1 \leqslant j \leqslant r$ bereits N und folglich ist φ surjektiv. □

Lemma 2.17. *Seien M, N zwei R-Moduln und $\varphi, \psi : M \to N$ surjektive R-Homomorphismen. Dann ist $\mathrm{Kern}(\varphi) = \mathrm{Kern}(\psi)$ genau dann, wenn ein Automorphismus $\sigma \in \mathrm{Aut}(N)$ mit $\varphi = \sigma \circ \psi$ existiert.*

Beweis. Für jedes $\sigma \in \mathrm{Aut}(N)$ ist $\mathrm{Kern}(\sigma \circ \psi) = \mathrm{Kern}(\psi)$.

Umgekehrt liefern φ, ψ mithilfe des Homomorphiesatzes Isomorphismen $\overline{\varphi}, \overline{\psi} : M/\mathrm{Kern}(\psi) \xrightarrow{\sim} N$. Die Verknüpfung $\sigma := \overline{\varphi} \circ \overline{\psi}^{-1}$ besitzt die gewünschte Eigenschaft. □

Proposition 2.18. *Sei G eine endliche abelsche p-Gruppe, sei $n \geqslant 0$ und $r := \dim_{\mathbb{Z}/p\mathbb{Z}}(G/pG)$. Dann gilt:*

$$|\{N \subset \mathbb{Z}_p^n \ \textit{Untermodul} : \mathbb{Z}_p^n/N \cong G\}| = |\operatorname{Aut} G|^{-1} |G|^n \prod_{j=n-r+1}^{n} (1 - p^{-j}).$$

Beweis. Folgender Beweis ist aus [2] entnommen.

Sei $s_n^R(G)$ die Menge aller surjektiver R-Homomorphismen $R^n \to G$. Jeder $\varphi \in s_{n^p}^{\mathbb{Z}_p}(G)$ induziert einen Isomorphismus $\overline{\varphi} : \mathbb{Z}_p^n/\operatorname{Kern}(\varphi) \xrightarrow{\sim} G$ und jeder Untermodul $N \subset \mathbb{Z}_p^n$ mit $\mathbb{Z}_p^n/N \xrightarrow{\sim} G$ induziert einen Epimorphismus $\mathbb{Z}_p^n \to G$. Zwei solche unterscheiden sich nach Lemma 2.17 um einen Automorphismus von links und es gilt

$$|\{N \subset \mathbb{Z}_p^n : \mathbb{Z}_p^n/N \cong G\}|\operatorname{Aut}(G)| = |s_n^{\mathbb{Z}_p}(G)|. \tag{2.19}$$

Sei π die Reduktionsabbildung $\operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p^n, G) \to \operatorname{Hom}_{\mathbb{Z}/p\mathbb{Z}}((\mathbb{Z}/p\mathbb{Z})^n, G/pG)$ aus Lemma 2.13. Nach Proposition 2.16 induziert π eine surjektive Abbildung $\pi|_{s_n^{\mathbb{Z}_p}(G)} : s_n^{\mathbb{Z}_p}(G) \to s_n^{\mathbb{Z}/p\mathbb{Z}}(G/pG)$. Zwei Abbildungen mit gleichem Bild unterscheiden sich durch einen Homomorphismus $\psi : \mathbb{Z}_p^n \to pG$, der durch die Wahl des Bildes jedes Basisvektors angegeben werden kann. Somit ist

$$|s_n^{\mathbb{Z}_p}(G)| = |s_n^{\mathbb{Z}/p\mathbb{Z}}(G/pG)||pG|^n = |s_n^{\mathbb{Z}/p\mathbb{Z}}(G/pG)| \left(\frac{|G|}{p^r}\right)^n. \tag{2.20}$$

Mithilfe eines $\mathbb{Z}$-Isomorphismus $G/pG \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^r$ sehen wir, dass $s_n^{\mathbb{Z}/p\mathbb{Z}}(G/pG)$ in Bijektion mit der Menge der $r \times n$ Matrizen über $\mathbb{Z}/p\mathbb{Z}$ mit Rang r steht. Diese wiederum entsprechen linear unabhängigen r-Tupeln $(v_1, \dots, v_r) \in \boxplus_{i=1}^r (\mathbb{Z}/p\mathbb{Z})^n$, von denen es $\prod_{j=0}^{r-1}(p^n - p^j)$ gibt. Wir erhalten somit

$$|s_n^{\mathbb{Z}/p\mathbb{Z}}(G/pG)| = \prod_{j=0}^{r-1}(p^n - p^j) = p^{nr} \prod_{j=n-r+1}^{n}(1 - p^{-j}). \tag{2.21}$$

Das Zusammenfügen der Gleichungen 2.19, 2.20 und 2.21 liefert das gewünschte Resultat. □

Sei nun R ein nicht mehr zwingend lokaler Hauptidealring und seien $m, n \in \mathbb{Z}^{\geqslant 0}$.

Proposition 2.22. *Jeder Untermodul von R^n ist isomorph zu R^r für ein gewisses $0 \leqslant r \leqslant n$.*

Beweis. Als endlich erzeugter Modul über einem noetherschen Ring ist R^n noethersch. Somit ist jeder Untermodul $M \subset R^n$ endlich erzeugt und ist laut dem Elementarteilersatz für endlich erzeugte Moduln über Hauptidealringen für gewisse $r, \ell \geqslant 0$ und $e_j \in R$ für $1 \leqslant j \leqslant \ell$ von der Form $M \cong R^r \boxplus \coprod_{j=1}^{\ell} R/(e_j)$. Schlussendlich ist $\ell = 0$ und $r \leqslant n$, da M injektiv in R^n eingebettet werden kann. □

Proposition 2.23. *Zwei R-Homomorphismen $\varphi, \psi : R^n \to R^m$ haben gleiches Bild genau dann, wenn ein verbindender Automorphismus $\chi : R^n \to R^n$ sodass $\varphi \circ \chi = \psi$ ist existiert.*

Beweis. Komposition mit einem Automorphismus von rechts verändert das Bild eines Homomorphismus nicht. Fixieren wir nach Proposition 2.22 für ein gewisses $r \geqslant 0$ einen Isomorphismus $\operatorname{Bild}\varphi = \operatorname{Bild}\psi \xrightarrow{\sim} R^r$. Da freie Moduln projektiv sind, zerfällt die kurze exakte Sequenz

$$0 \longrightarrow \operatorname{Kern}\varphi \longrightarrow R^n \xrightarrow{\varphi} \operatorname{Bild}\varphi \longrightarrow 0.$$

Wenden wir zusätzlich Proposition 2.22 auf $\operatorname{Kern}\varphi$ an, so erhalten für ein gewisses $\ell \geqslant 0$ Isomorphismen

$$R^n \xrightarrow{\sim} \operatorname{Kern}\varphi \oplus \operatorname{Bild}\varphi \xrightarrow{\sim} R^\ell \boxplus R^r,$$

wobei aufgrund des Isomorphismus $\ell + r = n$ ist. Wählen wir α_φ als die Komposition der obigen Abbildungen und wiederholen den Vorgang für ψ, so erhalten wir ein kommutatives Diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Kern}\varphi & \longrightarrow & R^n & \xrightarrow{\varphi} & \operatorname{Bild}\varphi & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \alpha_\varphi}\wr & & \downarrow\wr & & \\
 & & & & R^l \boxplus R^r & \longrightarrow & R^r & \longrightarrow & 0 \\
 & & & & \uparrow{\scriptstyle \alpha_\psi}\wr & & \uparrow\wr & & \\
0 & \longrightarrow & \operatorname{Kern}\psi & \longrightarrow & R^n & \xrightarrow{\psi} & \operatorname{Bild}\psi & \longrightarrow & 0.
\end{array}$$

Da die Isomorphismen $\operatorname{Bild}\varphi = \operatorname{Bild}\psi \xrightarrow{\sim} R^r$ gleich sind, gibt uns die Verknüpfung $\chi := {\alpha_\varphi}^{-1} \circ \alpha_\psi$ den gewünschten Isomorphismus.[1] □

2.3 p-adische Matrizen

Sei nun $m \geqslant n$.

Proposition 2.24. *Wir versehen $\mathbb{Z}_p^n$ mit der Produkttopologie der Topologie auf $\mathbb{Z}_p$ aus Definition 2.4. Dann ist $\mathbb{Z}_p^n$ bezüglich der Addition eine kompakte, Hausdorffsche topologische Gruppe.*

Beweis. Das Produkt von Hausdorffräumen ist Hausdorff, das endliche Produkt kompakter Räume ist kompakt und das endliche Produkt topologischer Gruppen ist eine topologische Gruppe. Die Aussage folgt somit aus Proposition 2.6. □

Definition 2.25. Sei μ_n das Haarsche Mass auf $\mathbb{Z}_p^n$, normiert sodass $\mu_n(\mathbb{Z}_p^n) = 1$ ist.

Proposition 2.26. *Dies ist das Produktmass des Masses aus Proposition 2.7.*

Beweis. Das Produktmass auf dem kartesischen Produkt gegebener Massräume ist dadurch charakterisiert, dass es dem kartesichen Produkt von Mengen das Produkt der Masse der Mengen als Mass zuordnet. Es genügt Gleichheit auf den Erzeugenden der Borel σ-Algebra auf $\mathbb{Z}_p^n$ zu überprüfen. Diese sind kartesische Produkte der Erzeugenden der Borel σ-Algebra von $\mathbb{Z}_p$, also von der Form $A := \bigtimes_{j=1}^n (a_j + p^{m_j}\mathbb{Z}_p)$ für gewisse $a_j \in \mathbb{Z}_p$ und $m_j \in \mathbb{Z}^{\geqslant 0}$ für $1 \leqslant j \leqslant n$. Ähnlich wie in Bemerkung 2.5 sehen wir, dass $\mathbb{Z}_p^n$ die disjunkte Vereinigung von $\prod_{j=1}^n p^{m_j}$ linearen Translaten einer solchen Menge A ist. Deshalb ist $\mu_n(A) = \prod_{j=1}^n p^{-m_j}\mu_n(\mathbb{Z}_p^n) = \prod_{j=1}^n \mu(a_j + p^{m_j}\mathbb{Z}_p)$. □

Proposition 2.27. *Für alle Borelmengen $A \subset \mathbb{Z}_p^n$ und $M \in \operatorname{Mat}_{n\times n}(\mathbb{Z}_p)$ gilt*

$$\mu_n(MA) = |\det(M)|_p\, \mu_n(A).$$

Beweis. Wir zeigen dies zunächst für $M \in \mathrm{GL}_n(\mathbb{Z}_p)$. Da die Abbildung $x \mapsto Mx$ ein Homöomorphismus ist, ist $A \mapsto \mu_n(MA)$ ein Haarsches Mass auf $\mathbb{Z}_p^n$. Wegen der Eindeutigkeit des Haar Masses unterscheidet sich dieses nur bis auf eine Konstante von μ_n, welche wir durch Anwendung des Masses auf $\mathbb{Z}_p^n$ als 1 bestimmen können. Somit sind die Masse identisch und für alle Borelmengen $A \subset \mathbb{Z}_p^n$ gilt $\mu_n(MA) = \mu_n(A)$.

Sei nun $M \in \operatorname{Mat}_{n\times n}(\mathbb{Z}_p)$ beliebig. Nach Korollar 2.12 und dem Elementarteilersatz für Matrizen über Hauptidealringen existiert ein $r \leqslant n$, gewisse $0 \leqslant \nu_1 \leqslant \cdots \leqslant \nu_r \in \mathbb{Z}^{\geqslant 0}$ und $U, V \in \mathrm{GL}_n(\mathbb{Z}_p)$ sodass für $D = \operatorname{diag}(p^{\nu_1}, \ldots, p^{\nu_r}, 0, \ldots, 0)$ die Matrix M von der Form UDV ist. Nach der bewiesenen Aussage für invertierbare Matrizen und nach Propositionen 2.10 und 2.26 ist

$$\mu(MA) = \mu(UDVA) = \left\{ \begin{array}{ll} \prod_{j=1}^n p^{-\nu_j}\mu(VA) & r = n \\ 0 & r < n \end{array} \right\} = |\det(M)|_p\, \mu(A).$$

□

Lemma 2.28. *Sei für $\ell \geqslant 0$ die Abbildung $\pi_n^\ell : \mathbb{Z}_p^n \to (\mathbb{Z}/p^\ell\mathbb{Z})^n$ die natürliche Projektion. Dann ist für alle $A \subset (\mathbb{Z}/p^\ell\mathbb{Z})^n$ das Mass*

$$\mu_n((\pi_n^\ell)^{-1}(A)) = |A|/|(\mathbb{Z}/p^\ell\mathbb{Z})^n| = |A| \cdot p^{-\ell n}.$$

Beweis. Sei $x \in (\mathbb{Z}/p^\ell\mathbb{Z})^n$ und $y \in (\pi_n^\ell)^{-1}(x)$. Aufgrund der Translationsinvarianz des Haar Masses μ_n ist

$$\mu_n((\pi_n^\ell)^{-1}(x)) = \mu_n((\pi_n^\ell)^{-1}(x) - y) = \mu_n((\pi_n^\ell)^{-1}(\{0\})).$$

[1] Danke an Oliver Edtmair, der mir die entscheidende Idee für den Beweis geliefert hat.

Weiterhin ist

$$1 = \mu_n(\mathbb{Z}_p^n) = \sum_{x \in (\mathbb{Z}/p^\ell\mathbb{Z})^n} \mu_n((\pi_n^\ell)^{-1}(x)) = \mu_n((\pi_n^\ell)^{-1}(0)) \cdot |(\mathbb{Z}/p^\ell\mathbb{Z})^n|.$$

Daraus folgt die Aussage für $|A| = 1$. Der allgemeine Fall resultiert schliesslich aus der Additivität des Masses μ_n. □

Definition 2.29. Identifizieren wir $\mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$ via der Standardbasis für Matrizen mit $\mathbb{Z}_p^{nm}$, so erhalten wir via μ_{nm} ein Mass $\mu_{n,m}$ auf $\mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$.

Korollar 2.30. *Für alle $M \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_p)$, alle $N \in \mathrm{Mat}_{m\times m}(\mathbb{Z}_p)$ und alle Borelmengen $A \subset \mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$ ist*

$$\mu_{n,m}(MA) = |\det(M)|_p^m \ \mu_{n,m}(A),$$
$$\mu_{n,m}(AN) = |\det(N)|_p^n \ \mu_{n,m}(A).$$

Beweis. Via der Standardbasis für Matrizen mit passender Indizierung ist die Matrixdarstellung von $\mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \to \mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$, $X \mapsto MX$ respektive $X \mapsto XN$ die $nm \times nm$ Matrix $\mathrm{diag}(M, \ldots, M)$, respektive $\mathrm{diag}(N, \ldots, N)$ mit $\det(X \mapsto MX) = \det(M)^m$ und $\det(X \mapsto XN) = \det(N)^n$. Die Behauptung folgt somit aus Proposition 2.27. □

Korollar 2.31. *Sei für $\ell \geqslant 1$ die Abbildung $\pi_{n,m}^\ell : \mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \to \mathrm{Mat}_{n\times m}(\mathbb{Z}/p^\ell\mathbb{Z})$ die natürliche Projektion. Dann ist für alle $A \subset \mathrm{Mat}_{n\times m}(\mathbb{Z}/p^\ell\mathbb{Z})$ das Mass*

$$\mu_{n,m}((\pi_{n,m}^\ell)^{-1}(A)) = |A|/|\mathrm{Mat}_{n\times m}(\mathbb{Z}/p^\ell\mathbb{Z})| = |A| \cdot p^{-\ell nm}.$$

Beweis. Dies folgt direkt aus der Definition 2.29 des Masses $\mu_{n,m}$ und Lemma 2.28. □

Lemma 2.32. *Die Menge $\mathcal{M}_{n,m}$ aller Matrizen $A \in \mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$, sodass die Abbildung $\mathbb{Z}_p^m \to \mathbb{Z}_p^n$, $x \mapsto Ax$ surjektiv ist, hat Mass*

$$\mu_{n,m}(\mathcal{M}_{n,m}) = \prod_{j=m-n+1}^{m} (1 - p^{-j}).$$

Beweis. Sei $\mathcal{N}_{n,m}$ die Menge aller Matrizen $A \in \mathrm{Mat}_{n\times m}(\mathbb{Z}/p\mathbb{Z})$, sodass die Abbildung $(\mathbb{Z}/p\mathbb{Z})^m \to (\mathbb{Z}/p\mathbb{Z})^n$, $x \mapsto Ax$ surjektiv ist. Nach Proposition 2.16 ist für $\pi_{n,m}^1$ wie aus Korollar 2.31 die Menge $\mathcal{M}_{n,m} = (\pi_{n,m}^1)^{-1}(\mathcal{N}_{n,m})$. Die Menge $\mathcal{N}_{n,m}$ steht in Bijektion zur Menge

$$\big\{(v_1, \ldots, v_n) \in \coprod_{i=1}^{n} (\mathbb{Z}/p\mathbb{Z})^m | \{v_1, \ldots, v_n\} \text{ linear unabhängig}\big\}$$

mit Kardinalität $\prod_{j=0}^{n-1}(p^m - p^j)$. Aus Korollar 2.31 folgt dann, dass

$$\mu(\mathcal{M}_{n,m}) = \mu((\pi_{n,m}^1)^{-1}(\mathcal{N}_{n,m})) = |\mathcal{N}_{n,m}|/|\mathrm{Mat}_{n\times m}(\mathbb{Z}/p^{\mathbb{Z}})| = \prod_{j=m-n+1}^{m} (1 - p^{-j})$$

ist.

□

Korollar 2.33. *Für $n \geqslant 0$ ist das Mass der Menge der invertierbaren $n \times n$ Matrizen*

$$\mu(\mathrm{GL}_n(\mathbb{Z}_p)) = \prod_{i=1}^{n} (1 - p^{-i}).$$

Beweis. Dies ist ein Spezialfall von Lemma 2.32 mit $m = n$. □

Proposition 2.34. *Die Menge aller Matrizen in* $\mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$ *mit über* $\mathbb{Q}_p$ *vollem Rang hat Mass* 1*.*

Beweis. Sei $\mathcal{L}_{n,m} \subset \mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$ die Menge der p-adischen $n \times m$ Matrizen mit vollem Rang über $\mathbb{Q}_p$. Diese enthält $\mathcal{L}_{n,n} \times \mathrm{Mat}_{n\times(m-n)}(\mathbb{Z}_p)$, also gilt $\mu_{m,n}(\mathcal{L}_{m,n}) \geqslant \mu_{n,n}(\mathcal{L}_{n,n}) \cdot 1$ und es genügt $\mu_{n,n}(\mathcal{L}_{n,n}) = 1$ zu zeigen.

Sei für $\ell \geqslant 1$ die Abbildung $\pi^\ell_{n,n}$ wie in Korollar 2.31. Matrizen im Komplement von $\mathcal{L}_{n,n}$ sind singulär über $\mathbb{Q}_p$. Da $\pi^\ell_{n,n}$ mit der Determinante kommutiert, reduzieren diese auf solche in $\mathrm{Mat}_{n\times n}(\mathbb{Z}/p^\ell\mathbb{Z})$ mit Determinante 0. Die Menge $\mathcal{K}^\ell_{n,n}$ dieser hat Kardinalität $p^{-\ell n^2} - \prod_{j=0}^{n-1}(p^{\ell n} - p^{\ell j})$. Nach Korollar 2.31 ist also für alle $\ell \geqslant 1$ das Mass $\mu_{n,n}(\mathcal{L}_{n,n}) \geqslant 1 - \mu_{n,n}((\pi^\ell_{n,n})^{-1}(\mathcal{K}^\ell_{n,n}) = \prod_{j=0}^{n-1}(1 - p^{-\ell j})$. Dieses konvergiert gegen 1 für $\ell \to \infty$. □

2.4 Wahrscheinlichkeitsdichten für Isomorphieklassen endlicher abelscher p-Gruppen.

Wir kommen nun zum Beweis der Hauptaussage dieses Textes.

Sei $\Lambda \subset \mathbb{Z}^{\geqslant 1}$ und $\mathcal{G}_\Lambda$ die Menge der Isomorphieklassen aller abelscher Gruppen deren Ordnung in Λ liegt. Sei p eine Primzahl und $\Pi(p)$ die Menge aller ganzzahligen p-Potenzen und seien $m \geqslant n$ positive ganze Zahlen.

Definition 2.35. Wir definieren ein Mass auf $\mathcal{G}_{\Pi(p)}$ durch

$$\mu_{n,m}(A) := \mu_{n,m}(\{M \in \mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \mid \exists \mathfrak{G} \in A : \mathrm{Koker}(M) \in \mathfrak{G}\}).$$

Bemerkung 2.36. Sei $\mathcal{L}_{m,n}$ wie im Beweis von Proposition 2.34. Da der Kokern jeder Matrix in $\mathcal{L}_{m,n}$ eine abelsche p-Gruppe ist, ist nach Proposition 2.34 das Mass $\mu_{n,m}$ ein Wahrscheinlichkeitsmass auf $\mathcal{G}_{\Pi(p)}$.

Satz 2.37. *Seien* $m \geqslant n \geqslant 0$*, sei* $\mathfrak{G} \in \mathcal{G}_{\Pi(p)}$*, sei* $G \in \mathfrak{G}$ *und sei* $r := \dim_{\mathbb{Z}/p\mathbb{Z}}(G/pG)$*. Dann ist*

$$\mu_{n,m}(\{\mathfrak{G}\}) = |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{m-n} \prod_{j=n-r+1}^{n}(1-p^{-j}) \prod_{j=m-n+1}^{m}(1-p^{-j}).$$

Beweis. Wir definieren $\mathrm{col} : \mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \to \{N \subset \mathbb{Z}_p^n |\ N \text{ Untermodul}\}$, $M \mapsto \mathrm{Bild}(M)$. Die Menge $\{M \in \mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \mid \mathrm{Koker}(M) \in \mathfrak{G}\}$ ist die disjunkte Vereinigung der $\mathrm{col}^{-1}(N)$ über alle Untermoduln $N \subset \mathbb{Z}_p^n$ sodass $\mathbb{Z}_p^n/N \in \mathfrak{G}$ ist. Deshalb ist

$$\mu_{n,m}(\{M \in \mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \mid \mathrm{Koker}(M) \in \mathfrak{G}\}) = \sum_{N\subset\mathbb{Z}_p^n,\ \mathbb{Z}_p^n/N\in\mathfrak{G}} \mu_{n,m}(\mathrm{col}^{-1}(N)). \tag{2.38}$$

Für $r > n$ reduziert sich die Behauptung auf $0 = 0$. Andernfalls ist $\mathrm{col}^{-1}(N)$ jeweils nichtleer. Wir wählen somit für jeden $\mathbb{Z}_p$-Untermodul $N \subset \mathbb{Z}_p^n$ mit $\mathbb{Z}_p^n/N \in \mathfrak{G}$ ein $A \in \mathrm{col}^{-1}(N)$. Nach dem Elementarteilersatz existieren $U \in \mathrm{GL}_n(\mathbb{Z}_p)$ und $V \in \mathrm{GL}_m(\mathbb{Z}_p)$, eine Zahl $0 \leqslant d \leqslant n$ sowie Elemente $0 \leqslant \nu_1 \leqslant \cdots \leqslant \nu_d$ sodass $UAV = \mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_d}, 0, \cdots, 0)(I_n|0) =: D$ ist. Da $\mathfrak{G}$ endlich ist, ist $d = n$. Nach Proposition 2.23 ist

$$\mathrm{col}^{-1}(N) = \{AT \mid T \in \mathrm{GL}_m(\mathbb{Z}_p)\}.$$

Weiterhin ist mit Proposition 2.30 und Lemma 2.32

$$\begin{aligned}
\mu_{n,m}(\mathrm{col}^{-1}(N)) &= \mu_{n,m}(\{U^{-1}DV^{-1}T | T \in \mathrm{GL}_m(\mathbb{Z}_p)\} \\
&\overset{2.30}{=} |\det(U^{-1})|_p^n\ |\det(\mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_n})|_p^m\ |\det(V^{-1})|_p^n\ \mu_{n,m}(\{(I_n|0)T | T \in \mathrm{GL}_m(\mathbb{Z}_p)\} \\
&\overset{2.30}{=} |\prod_{j=1}^{n} p^{-\nu_j}|^m\ \mu_{n,m}(\{(A_{ij})_{i=1,\ldots,n}^{j=1,\ldots,m} | A \in \mathrm{GL}_m(\mathbb{Z}_p)\}) \\
&\overset{2.32}{=} |\mathfrak{G}|^{-m} \prod_{j=m-n+1}^{m}(1-p^{-j}).
\end{aligned} \tag{2.39}$$

Dies ist unabhängig vom Modul N. Gleichungen (2.38) und (2.39) zusammen mit Proposition 2.18 ergeben somit die gewünschte Formel

$$\begin{aligned}
&\mu_{n,m}(\{M \in \mathrm{Mat}_{n\times m}(\mathbb{Z}_p) \mid \mathrm{Koker}(M) \in \mathfrak{G}\}) \\
&\overset{(2.38)}{=} \sum_{N\subset\mathbb{Z}_p^n,\ \mathbb{Z}_p^n/N\in\mathfrak{G}} \mu_{n,m}(\mathrm{col}^{-1}(N)) \\
&\overset{(2.39)}{=} \sum_{N\subset\mathbb{Z}_p^n,\ \mathbb{Z}_p^n/N\in\mathfrak{G}} |\mathfrak{G}|^{-m} \prod_{j=m-n+1}^{m} (1-p^{-j}) \\
&\overset{2.18}{=} |\mathrm{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{n-m} \prod_{j=n-r+1}^{n} (1-p^{-j}) \prod_{j=m-n+1}^{m} (1-p^{-j}).
\end{aligned}$$

□

Definition 2.40. Seien $s \in \mathbb{Z}^{\geqslant 0}$ und $\mathfrak{G} \in \mathcal{G}_{\Pi(p)}$. Sei $\mu_{n,m,u}(\{\mathfrak{G}\})$ die Wahrscheinlichkeit, dass für eine zufällig per $\mu_{m,n}$ gezogene Isomorphieklasse $\mathfrak{H} \in \mathcal{G}_{\Pi(p)}$ und für aus einen Repräsentanten $H \in \mathfrak{H}$ via Gleichverteilung gezogene $h_1, \ldots, h_s \in H$ die Gruppe $H/\langle h_1, \ldots, h_s\rangle$ in $\mathfrak{G}$ liegt.

Proposition 2.41. *Für alle $s \in \mathbb{Z}^{\geqslant 0}$ ist*

$$\mu_{n,m,s} = \mu_{n,m+s}.$$

Beweis. Sei $A \in \mathrm{Mat}_{n,m}(\mathbb{Z}_p)$ und $h_1, \ldots, h_s \in \mathbb{Z}_p^n/\operatorname{Bild}(A)$. Dann ist mit dem 2. Isomorphiesatz für alle $(v_1, \ldots, v_s) \in h_1 \times \cdots \times h_s$

$$\frac{\mathbb{Z}_p^n/\operatorname{Bild} A}{\langle h_1, \ldots, h_s\rangle} \cong \frac{\mathbb{Z}_p^n}{\operatorname{Bild}(A) + \sum_{i=1}^{s} \operatorname{Bild}(v_i)} = \frac{\mathbb{Z}_p^n}{\operatorname{Bild}((A|v_1|\ldots|v_s))}.$$

Weiterhin ist wegen der Translationsinvarianz des Haarschen Masses μ_n auf $\mathbb{Z}_p^n$ für $i = 1, \ldots, s$

$$\mu(h_i) = \frac{1}{\mathbb{Z}_p^n/\operatorname{Bild}(A)},$$

was genau der Wahrscheinlichkeit h_i via Gleichverteilung aus $\mathbb{Z}_p^n/\operatorname{Bild}(A)$ zu ziehen entspricht.

Da $\mu_{n,m+s}$ genau das Produktmass von $\mu_{n,m}$ und s-mal μ_n ist, ist also für alle $\mathfrak{G} \in \mathcal{G}_{\Pi(p)}$ die Wahrscheinlichkeit $\mu_{n,m+s}(\{\mathfrak{G}\})$ des Ziehens einer Matrix $\tilde{A} \in \mathrm{Mat}_{n,m+s}(\mathbb{Z}_p)$ mit $\mathbb{Z}_p^n/\operatorname{Bild}(\tilde{A}) \in \mathfrak{G}$ gleich der Wahrscheinlichkeit eine Matrix $A \in \mathrm{Mat}_{n,m}(\mathbb{Z}_p)$ und via Gleichverteilung $h_1, \ldots, h_s$ aus $\mathbb{Z}_p^n/\operatorname{Bild}(A) =: H$ zu ziehen sodass $H/\langle h_1, \ldots, h_s\rangle$ in $\mathfrak{G}$ liegt. Dies wiederum ist genau die Wahrscheinlichkeit $\mu_{n,m,s}(\{\mathfrak{G}\})$ aus Definition 2.40. □

3 Allgemeine Aussagen zu Zahlkörpern und deren Idealklassengruppen

Wir möchten nun die erarbeitete Theorie auf die Verteilung von Idealklassengruppen von Zahlkörpern anwenden. Zur Erinnerung und zum Vermeiden von Missverständnisswen werde ich benötigte Begriffe und Aussagen hier kurz erwähnen. Für Leser ohne elementare Kenntnisse aus der algebraischen Zahlentheorie empfehle ich jedoch die Lektüre der ersten sieben Abschnitte des ersten Kapitels aus [10], wo ausführliche Beweise der von dort übernommenen, unten aufgeführten Aussagen, zu finden sind.

Sei K ein Zahlkörper, das heisst eine endliche, algebraische Erweiterung von $\mathbb{Q}$. Nach dem Satz vom primitiven Element ist jeder solche $K = \mathbb{Q}(\alpha)$ für ein gewisses $\alpha \in K$. Ist P das Minimalpolynom von α über $\mathbb{Q}$, so ist $K \cong \mathbb{Q}[X]/(P)$. Sei $n := [K : \mathbb{Q}]$ und seien $\beta_1, \ldots, \beta_n$ die unterschiedlichen Nullstellen von P in $\mathbb{C}$.

Für alle $1 \leqslant i \leqslant n$ induziert der Homomorphismus $\mathbb{Q}[X] \to \mathbb{C},\ f(X) \mapsto f(\beta_i)$ einen Homomorphismus $\sigma_i : K \to \mathbb{C}$. Diese sind bis auf Vertauschung unabhängig von der Wahl von α und des Isomorphismus $K \xrightarrow{\sim} \mathbb{Q}[X]/(P)$

Definition 3.1. Diese σ_i sind die *Einbettungen* von K in $\mathbb{C}$. Solche mit $\sigma_i(K) \subset \mathbb{R}$ sind reelle Einbettungen, sei $r_{1,K}$ die Anzahl dieser, die restlichen sind komplexe Einbettungen und treten immer in Paaren auf, sei $r_{2,K}$ die Anzahl dieser Paare. Wir verzichten auf den Index K wenn Verwechslungen unwahrscheinlich sind.

Definition 3.2. Ein total reller Zahlkörper ist einer mit lediglich reellen Einbettungen, ein total imaginärer Zahlkörper ist ein solcher mit nur komplexen Einbettungen. Ein quadratischer Zahlkörper ist einer vom Grad 2 über $\mathbb{Q}$.

Definition 3.3. Der *Ganzheitsring* $\mathcal{O}_K$ von K ist der ganze Abschluss von $\mathbb{Z}$ in K.

Proposition 3.4. *Der Ganzheitsring $\mathcal{O}_K$ jedes Zahlkörpers K ist ein freier $\mathbb{Z}$-Modul vom Rang $[K : \mathbb{Q}]$.*

Beweis. [10, Kapitel 1 Satz 2.10] □

Definition 3.5. Seien $v_1, \ldots, v_n$ Erzeugende des Ganzheitsring eines Zahlkörpers K als $\mathbb{Z}$-Modul. Seien $\sigma_1, \ldots, \sigma_n$ dessen Einbettungen in $\mathbb{C}$. Die *Fundamentaldiskriminante* von K ist der Wert $\Delta_K := \det((\sigma_i(v_j))_{i,j=1}^n)^2$. Diese ist unabhängig von der Wahl der v_i.

Bemerkung 3.6. Für quadratfreie $d \in \mathbb{Z}$ ist

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} d & d \equiv 1 \bmod 4 \\ 4d & d \equiv 2, 3 \bmod 4. \end{cases}$$

Definition 3.7. Die *Norm* eines nichttrivialen Ideals $\mathfrak{a} \subset \mathcal{O}_K$ ist die Kardinalität $N(\mathfrak{a}) := |R/\mathfrak{a}|$. Wir definieren weiterhin $N((0)) := 0$.

Definition 3.8. *Gebrochene Ideale* über $\mathcal{O}_K$ sind endlich erzeugte, nichttriviale $\mathcal{O}_K$-Moduln $\mathfrak{a} \subset K$. Die Menge dieser bildet mit einer Erweiterung der üblichen Multiplikation von Idealen eine abelsche Gruppe J_K. Die Menge der von einem Element erzeugten gebrochenen Ideale bildet eine Untergruppe $P_K < J_K$. Die *Idealklassengruppe* von K ist die Gruppe $\mathrm{Cl}(K) := J_K/P_K$.

Satz 3.9. *Für alle Zahlkörper K ist folgende Sequenz exakt:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & J & \longrightarrow & \mathrm{Cl}(K) \longrightarrow 1. \\ & & & & x & \longmapsto & (x), & \mathfrak{a} & \longmapsto \mathfrak{a}P \end{array}$$

Beweis. [10, Kapitel 1 Abschnitt 3] □

Satz 3.10 (Minkowski)**.** *Jede Restklasse eines gebrochenen Ideals enthält ein Ideal mit Norm nicht grösser als*

$$M_K := \left(\frac{4}{\pi}\right)^{r_2} \frac{n^n}{n!}.$$

Beweis. [10, Kapitel 1 Abschnitt 5] □

Korollar 3.11. *Die Idealklassengruppe eines Zahlkörpers ist endlich.*

Beweis. [10, Kapitel 1 Theorem 6.3] □

Definition 3.12. Die *Klassenzahl* von K ist die Zahl $h_K := |\mathrm{Cl}(K)|$.

Korollar 3.13. *Für einen Zahlkörper K ist $\mathcal{O}_K$ ein Hauptidealring genau dann, wenn er faktoriell ist, genau dann, wenn $\mathrm{Cl}(K) = 1$ ist.*

Beweis. Die Äquivalenz zwischen faktoriell und Hauptidealring folgt aus der Zerlegung von Idealen in Primidealen in Dedekindringen wie $\mathcal{O}_K$. Die andere Äquivalenz folgt aus der Definition und der Tatsache, dass für jedes faktorielle Ideal $\mathfrak{a} \subset K$ ein $x \in K^\times$ mit $x \cdot \mathfrak{a} \subset \mathcal{O}_K$ existiert. □

Satz 3.14 (Dirichlet). *Sei* $\mu(K) := \{x \in K \mid \exists n \in \mathbb{Z}^{\geqslant 1} : x^n = 1\}$ *die Gruppe der Einheitswurzeln eines Zahlkörpers* K*. Dann ist*

$$\mathcal{O}_K^\times \cong \mu(K) \boxplus \mathbb{Z}^{r_1+r_2-1}.$$

Sei zusätzlich S *eine endliche Menge an Primidealen in* $\mathcal{O}_K$ *und* $R_S := \{\frac{a}{b} \in K \mid \forall \mathfrak{p} \subset \mathcal{O}_K : (b) \subset \mathfrak{p} \Rightarrow \mathfrak{p} \in S\}$*. Dann ist*

$$R_S^\times \cong \mu(K) \boxplus \mathbb{Z}^{r_1+r_2-1+|S|}$$

Beweis. [10, Kapitel 1 Satz 7.3] und [10, Kapitel 1 Korollar 11.7]. □

4 Die Cohen–Lenstra Heuristik

In den Klassengruppen von Zahlkörpern ist nach Korollar 3.13 gewisse Information enthalten. Man kann argumentieren, dass die Klassenzahl eines Zahlkörpers misst, wie weit der dazugehörige Ganzheitsring von einem faktoriellen Ring abweicht. Diese Information kann genutzt werden, um Lösungen gewisser diophantiner Gleichungen zu berechnen. Ein prominentes Beispiel ist die Gleichung

$$x^n + y^n = z^n,$$

die nach Fermats letztem Satz für $n > 2$ keine nichttriviale, ganzzahlige Lösung besitzt. Ein wesentliches Hindernis für den Beweis dieser Aussage ist die Tatsache, dass für gewisse $n > 2$ die Primfaktorzerlegung in $\mathbb{Z}[e^{\frac{2\pi i}{n}}]$ nicht eindeutig, also $\mathrm{Cl}(\mathbb{Z}[e^{\frac{2\pi i}{n}}])$ nichttrivial ist.

Wie in der Einleitung erwähnt, hat es sich als schwierig herausgestellt, Aussagen über Klassengruppen zu beweisen. Cohen und Lenstra präsentierten in [2] eine Heuristik, um die Klassengruppe bestimmter Zahlkörper besser beschreiben zu können. Wir werden in diesem Abschnitt auf diese genauer eingehen.

4.1 Wahrscheinlickeitsdichten für Isomorphieklassen endlicher abelscher Gruppen

Der folgende Unterabschnitt ist frei von heuristischen Aussagen.

Sei P die Menge aller Primzahlen, und für eine Teilmenge $Q \subset P$ sei $\Pi(Q)$ die Menge aller Produkte von Elementen aus Q. Wie im Unterabschnitt 2.4 bezeichnen wir weiterhin für eine Primzahl p mit $\Pi(p) := \Pi(\{p\})$ die Menge aller ganzzahligen p-Potenzen. Sei für nichtleere $\Lambda \subset \mathbb{Z}^{\geqslant 1}$ die Menge $\mathcal{G}_\Lambda$ definiert als die Menge aller Isomorphieklassen abelscher Gruppen mit Ordnung in Λ. Im folgenden werden wir für $\Lambda = \mathbb{Z}^{\geqslant 1}$ auf den Index Λ verzichten. Wir führen nun für solche Λ und für $u \in \mathbb{Z}^{\geqslant 0}$ eine Distribution auf $\mathcal{G}_\Lambda$ ein. Diese ist die selbe wie diejenige, die Cohen und Lenstra bereits in [2] definierten. Sei dafür f eine komplexwertige Abbildung auf $\mathcal{G}$.

Definition 4.1. Der *u-Erwartungswert von* f auf Gruppen mit Ordnung in Λ ist folgender Grenzwert, falls er existiert:

$$M_{\Lambda,u}(f) := \lim_{N\to\infty} \frac{\sum_{\mathfrak{G}\in\mathcal{G}_\Lambda,\ |\mathfrak{G}|\leqslant N} f(\mathfrak{G})|\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}}{\sum_{\mathfrak{G}\in\mathcal{G}_\Lambda,\ |\mathfrak{G}|\leqslant N} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}}.$$

Falls der Ausdruck

$$\lim_{N\to\infty} \sum_{\mathfrak{G}\in\mathcal{G}_\Lambda,\ |\mathfrak{G}|\leqslant N} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u} \tag{4.2}$$

konvergiert, können wir zusätzlich folgendes Wahrscheinlichkeitsmass definieren:

Definition 4.3. Ein Wahrscheinlichkeitsmass auf der Menge $\mathcal{G}_\Lambda$ ist

$$\mathbb{P}_{\Lambda,u}(A) = \frac{\sum_{\mathfrak{G}\in A} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}}{\sum_{\mathfrak{G}\in\mathcal{G}_\Lambda} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}}.$$

Für eine Isomorphieklasse $\mathfrak{G} \in \mathcal{G}_\Lambda$ ist $\mathbb{P}_{\Lambda,u}(\{\mathfrak{G}\})$ die *u-Wahrscheinlichkeit* von $\mathfrak{G}$.

Bemerkung 4.4. In diesem Fall gilt

$$M_{\Lambda,u}(f) = \mathbb{E}_{\mathbb{P}_{\Lambda,u}}(f).$$

Wir werden uns im Folgenden mit der Frage beschäftigen, für welche Tupel $(u, \Lambda) \in \mathbb{Z}^{\geqslant 0} \times \mathcal{P}(\mathbb{Z}^{\geqslant 1})$ der Ausdruck (4.2) konvergiert.

Proposition 4.5. *Für $u = 0$ und $P \subset \Lambda$ ist der Ausdruck (4.2) nicht konvergent.*

Beweis. Wir können den Ausdruck (4.2) von unten abschätzen

$$\sum_{\mathfrak{G} \in \mathcal{G}_\Lambda} |\operatorname{Aut}(\mathfrak{G})|^{-1} \geqslant \sum_{\mathfrak{G} \in \mathcal{G}_P} |\operatorname{Aut}(\mathfrak{G})|^{-1} = \sum_{\mathfrak{G} \in \mathcal{G}_P} |\operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})|^{-1} = \sum_{\mathfrak{G} \in \mathcal{G}_P} \frac{1}{p-1},$$

wobei die letzte Reihe bekannterweise nicht konvergent ist. □

Bemerkung 4.6. In diesem Fall können wir trotzdem allen Teilmengen $A \subset \mathcal{G}_\Lambda$, für die $M_{\Lambda,0}(1_A)$ existiert, dies als Wahrscheinlichkeit zuordnen. Die Abbildung $A \mapsto M_{\Lambda,0}(1_A)$ liefert dann jedoch kein Wahrscheinlichkeitsmass und für alle $A \subset \mathcal{G}_\Lambda$ mit $|A| < \infty$ ist $M_{\Lambda,0}(1_A) = 0$.

Proposition 4.7. *Für $N \in \mathbb{Z}^{\geqslant 1}$ ist das durch das Mass μ aus Satz 1.1 auf $\mathcal{G}_{\{N\}}$ induzierte Mass für alle $u \geqslant 0$ gleich $\mathbb{P}_{\{N\},u}$.*

Beweis. Dies folgt direkt aus Satz 1.1. □

Um Aussagen über die Konvergenz von Massen aus Unterabschnitt 2.4 zeigen zu können, benötigen wir folgenden Satz aus der Masstheorie:

Satz 4.8 (Vitali-Hahn-Saks)**.** *Sei (Ω, Σ) ein Massraum und $(\mu_n)_{n\geqslant 1}$ eine Folge von Massen darauf, sodass für jedes messbare $A \in \Sigma$ die Folge $(\mu_n(A))_{n\geqslant 1}$ für $n \to \infty$ konvergiert. Dann definiert $\mu := \lim_{n\to\infty} \mu_n$ ein Mass auf (Ω, Σ).*

Beweis. [4, Kapitel IX, Abschnitt 10] □

Um diesen anwenden zu können, benötigen wir zusätzlich folgende Aussagen:

Lemma 4.9. *Für jede reelle Folge $(a_n)_{n\geqslant 1}$, für die $\sum_{n=1}^{\infty} |a_n|$ konvergiert, konvergiert das Produkt $\prod_{n=1}^{\infty}(1 + a_n)$ absolut. Dieses konvergiert gegen 0 genau dann, wenn einer der Faktoren 0 ist.*

Beweis. [12, Proposition 3.1] □

Korollar 4.10. *Für alle Primzahlen $p \in P$ und alle $u \geqslant 0$ konvergiert das Produkt*

$$\lim_{N\to\infty} \prod_{j=u+1}^{N} (1 - p^{-j})^{-1}$$

absolut.

Beweis. Dies folgt aus der Konvergenz der geometrischen Reihe und Lemma 4.9. □

Mit Korollar 4.10 können wir nun folgendes Konvergenzverhalten vom Mass aus Definition 2.35 zeigen:

Proposition 4.11. *Für alle Primzahlen $p \in P$ und $\Lambda = \Pi(p)$ ist (4.2) konvergent mit*

$$\lim_{N\to\infty} \sum_{\mathfrak{G} \in \mathcal{G}_{\Pi(p)},\, |\mathfrak{G}| \leqslant N} |\operatorname{Aut}(\mathfrak{G})|^{-1} |\mathfrak{G}|^{-u} = \prod_{j=u+1}^{\infty} (1 - p^{-j})^{-1}$$

und für $u \geqslant 0$ konvergiert das Mass $\mu_{n,(n+u)}$ auf $\mathcal{G}_{\Pi(p)}$ aus Definition 2.35 gegen $\mathbb{P}_{\Pi(p),u}$ für $n \to \infty$.

Beweis. Nach Satz 2.37 und Korollar 4.10 ist für alle $\mathfrak{G} \in \mathcal{G}_{\Pi(p)}$ die Folge $(\mu_{n,(n+u)}(\{\mathfrak{G}\}))_{n\geqslant 1}$ konvergent. Mit der σ-Additivität der jeweiligen Masse ist dies auch für alle $A \subset \mathcal{G}_{\Pi(p)}$ die Folge $(\mu_{n,(n+u)}(A))_{n\geqslant 1}$. Die Abbildung $\mu := \lim_{n\to\infty} \mu_{n,(n+u)}$ ist folglich nach Satz 4.8 ein Mass. Mit der $\sigma-$Additivität von μ, Satz 2.37 und Proposition 2.34 gilt dann

$$\begin{aligned} 1 &= \lim_{n\to\infty} \mu_{n,(n+u)}(\mathcal{G}_{\Pi(p)}) \\ &= \mu(\mathcal{G}_{\Pi(p)}) \\ &= \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(p)}} \mu(\{\mathfrak{G}\}) \\ &= \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(p)}} \lim_{n\to\infty} \mu_{n,(n+u)}(\{\mathfrak{G}\}) \\ &= \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(p)}} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u} \prod_{j=u+1}^{\infty} (1-p^{-j}). \end{aligned}$$

Daraus folgt die Behauptung. □

Korollar 4.12. *Seien $s \in \mathbb{Z}^{\geqslant 0}$ und $\mathfrak{G} \in \mathcal{G}_{\Pi(p)}$. Dann ist die Wahrscheinlichkeit, dass für ein zufällig per $\mathbb{P}_{\Pi(p),u}$ gezogenes $\mathfrak{H} \in \mathcal{G}_{\Pi(p)}$ und für aus einem Repräsentanten $H \in \mathfrak{H}$ via Gleichverteilung gezogene $h_1, \ldots, h_s \in H$ die Gruppe $H/\langle h_1, \ldots, h_s\rangle \in \mathfrak{G}$ ist, gleich $\mathbb{P}_{\Pi(p),u+s}(\{\mathfrak{G}\})$.*

Beweis. Dies folgt mit Proposition 4.11 aus Proposition 2.41 mit $n \to \infty$. □

Lemma 4.13. *Für alle $u \geqslant 1$ und $Q \subset P$ ist*

$$\prod_{p\in Q} \prod_{j=u+1}^{\infty} (1-p^{-j})^{-1}$$

konvergent und es gilt

$$\prod_{p\in P} \prod_{j=u+1}^{\infty} (1-p^{-j})^{-1} = \prod_{j=u+1}^{\infty} \zeta(j),$$

wobei ζ die Riemannsche Zetafunktion ist.

Beweis. Wir zeigen die Konvergenz für $Q = P$. Der allgemeine Fall folgt aus der Ungleichung $\prod_{j=u+1}^{\infty}(1-p^{-j})^{-1} > 1$ für alle $p \in P$. Nach Lemma 4.9 ist für alle $p \in P$ dieses Produkt absolut konvergent und wir können Grenzwerte vertauschen. Wenden wir die Euler-Produkt Formel an, sehen wir, dass

$$\prod_{p\in P} \prod_{j=u+1}^{\infty} (1-p^{-j})^{-1} = \prod_{j=u+1}^{\infty} \prod_{p\in P} (1-p^{-j})^{-1} = \prod_{j=u+1}^{\infty} \zeta(j) \leqslant \prod_{j=2}^{\infty} \zeta(j)$$

ist. Wir wenden Lemma 4.9 erneut auf $a_j = \zeta(j) - 1 = \sum_{n=2}^{\infty} n^{-j}$ an. Da diese Reihe bekanntermassen für $j > 1$ absolut konvergiert, können wir im folgenden die Grenzwerte vertauschen und mithilfe der geometrischen Reihe

$$\sum_{j=2}^{\infty}\sum_{n=2}^{\infty} n^{-j} = \sum_{n=2}^{\infty}\sum_{j=2}^{\infty} n^{-j} = \sum_{n=2}^{\infty} \frac{1}{1-n^{-1}} - 1 - \frac{1}{n} = \sum_{n=2}^{\infty} \frac{n}{n-1} - \frac{n+1}{n} = 2$$

berechnen. Folglich konvergiert $\prod_{j=u+1}^{\infty} \zeta(j) \geqslant \prod_{p\in Q} \prod_{j=u+1}^{\infty}(1-p^{-j})^{-1}$. □

Definition 4.14. Für eine endliche, abelsche Gruppe G und eine natürliche Zahl N ist der *zu N teilerfremde Anteil von G* definiert als die grösste Untergruppe von G mit einer zu N teilerfremden Ordnung. Für Menge $Q \subset P$ ist der Q-Anteil G_Q von G die grösste Untergruppe, deren Ordnung in $\Pi(Q)$ liegt. Für einelementige Mengen lassen wir die Mengenklammern weg.

Notation. Für eine Isomorphieklasse $[G]$ und $Q \subset P$ ist $[G]_Q := [G_Q]$.

Satz 4.15. *Für jegliche $\Lambda \subset \mathbb{Z}^{\geqslant 1}$ und $u \geqslant 1$ konvergiert (4.2). Sei $Q \subset P$. Dann ist*

$$\lim_{N\to\infty} \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(Q)},|\mathfrak{G}|\leqslant N} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u} = \prod_{p\in Q}\prod_{j=u+1}^{\infty}(1-p^{-j})^{-1}$$

und für $\mathfrak{G} \in \mathcal{G}_{\Pi(Q)}$ ist

$$\mathbb{P}_{\Pi(Q),u}(\{\mathfrak{G}\}) = \prod_{p\in Q}\mathbb{P}_{\Pi(p),u}(\{\mathfrak{G}_p\}).$$

Beweis. Wir zeigen die Konvergenz von (4.2) für $\Lambda = \mathbb{Z}^{\geqslant 1}$, woraus der allgemeine Fall der Konvergenz von (4.2) für $\Lambda \subset \mathbb{Z}^{\geqslant 1}$ folgt. Sei für alle $N \in \mathbb{Z}^{\geqslant 0}$ die Menge $Q_N := \{p \in Q \mid p \leqslant N\}$. Wir definieren durch

$$\mu_N(A) := \sum_{\mathfrak{G}\in A}\prod_{p\in Q_N}\mathbb{P}_{\Pi(p),u}(\{\mathfrak{G}_p\}) = \sum_{\mathfrak{G}\in A}\prod_{p\in Q_N}|\operatorname{Aut}(\mathfrak{G}_p)|^{-1}|\mathfrak{G}_p|^{-u}\prod_{j=u+1}^{\infty}(1-p^{-j})$$

ein Mass auf $\mathcal{G}_{\Pi(Q)}$. Nach Lemma 4.13 und Satz 4.8 existiert der Grenzwert $\mu := \lim_{N\to\infty}\mu_N$ als Mass.

Falls N eine Primzahl ist, können wir $\mathcal{G}_{\Pi(Q_N)}$ wie folgt zerlegen:

$$\mathcal{G}_{\Pi(Q_N)} = \{\,[G\times H] \mid \mathfrak{G}\in\mathcal{G}_{\Pi(Q_{N-1})},\, G\in\mathfrak{G},\, \mathfrak{H}\in\mathcal{G}_{\Pi(N)},\, H\in\mathfrak{H}\}. \tag{4.16}$$

Wir zeigen per Induktion, dass

$$\mu(\mathcal{G}_{\Pi(Q_N)}) = \prod_{p\in Q,\,p>N}\prod_{j=u+1}^{\infty}(1-p^{-j})$$

ist.

Für $N = 0$ ist $\mathcal{G}_{\Pi(Q_N)} = \{[1]\}$ und die Behauptung folgt direkt aus der Definition. Angenommen die Aussage stimmt für $N-1 \geqslant 0$. Falls N keine Primzahl ist, ist $Q_N = Q_{N-1}$ und $\{p \in Q \mid p > N\} = \{p \in Q|\ p > N-1\}$ woraus die Aussage für N folgt. Sei nun N eine Primzahl. Wir berechnen $\mu(\mathcal{G}_{\Pi(Q_N)})$ mithilfe von (4.16), Proposition 4.11 und dem Fakt, dass für zwei endliche Gruppen teilerfremder Ordnungen die Automorphismengruppe des Produkts der Gruppen isomorph zum Produkt der jeweiligen Automorphismengruppen ist.

$$\begin{aligned}
\mu(\mathcal{G}_{\Pi(Q_N)}) &= \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(Q_N)}}|\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}\prod_{p\in Q}\prod_{j=u+1}^{\infty}(1-p^{-j})\\
&\overset{(4.16)}{=} \sum_{\mathfrak{H}\in\mathcal{G}_{\Pi(N)}}|\operatorname{Aut}(\mathfrak{H})|^{-1}|\mathfrak{H}|^{-u}\sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(Q_{N-1})}}|\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}\prod_{p\in Q}\prod_{j=u+1}^{\infty}(1-p^{-j})\\
&= \sum_{\mathfrak{H}\in\mathcal{G}_{\Pi(N)}}|\operatorname{Aut}(\mathfrak{H})|^{-1}|\mathfrak{H}|^{-u}\,\mu(\mathcal{G}_{Q_{\Pi(N-1)}})\\
&\overset{4.11}{=} \prod_{j=u+1}^{\infty}(1-N^{-j})^{-1}\mu(\mathcal{G}_{Q_{\Pi(N-1)}})\\
&\overset{\text{IV.}}{=} \prod_{j=u+1}^{\infty}(1-N^{-j})^{-1}\prod_{p\in Q,\,p>N-1}\prod_{j=u+1}^{\infty}(1-p^{-j})\\
&= \prod_{p\in Q,\,p>N}\prod_{j=u+1}^{\infty}(1-p^{-j})
\end{aligned}$$

Somit gilt die Behauptung für N und mit vollständiger Induktion für alle $N \geqslant 0$.

Da nach Lemma 4.13 das Produkt $\prod_{n=1}^{\infty}\prod_{p\in P}(1-p^{-j})$ konvergiert, geht $\mu(\mathcal{G}_{\Pi(Q_N)}) \to 1$ für $N \to \infty$. Somit ist μ ein Wahrscheinlichkeitsmass auf $\mathcal{G}_{\Pi(Q)}$. Mit der σ-Additivität von μ können wir

$$1 = \mu(\mathcal{G}_{\Pi(Q)}) = \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(Q)}} |\operatorname{Aut}(\mathfrak{G})|^{-1}|\mathfrak{G}|^{-u}\prod_{p\in Q}\prod_{j=u+1}^{\infty}(1-p^{-j})^{-1}$$

direkt berechnen. Folglich konvergiert (4.2) für alle Tupel $(u,\Pi(Q))$ mit $Q \subset P$ und $u \geqslant 1$, insbesondere also auch für $\Pi(P) = \mathbb{Z}^{\geqslant 1}$.

Weiterhin sehen wir, dass $\mu = \mathbb{P}_{\Pi(Q),u}$ ist. Ein direkter Vergleich mit Proposition 4.11 liefert die zweite Behauptung. □

Korollar 4.17. *Sei $Q \subset P$ und die Abbildung $f : \mathcal{G} \to \mathbb{C}$ nur von den p-Anteilen der Isomorphieklassen, für die p in Q liegt, abhängig. Dann ist für $u \geqslant 1$*

$$M_u(f) = M_{\Pi(Q),u}(f).$$

Beweis. Nach Satz 4.15 konvergiert (4.2) für $u \geqslant 1$. Für alle $\mathfrak{G} \in \mathcal{G}$ ist nach Satz 4.15

$$\begin{aligned}\mathbb{P}_u(\{\mathfrak{G}\}) &= \prod_{p\in P}\mathbb{P}_{\Pi(p),u}(\{\mathfrak{G}\})\\ &= \prod_{p\in Q}\mathbb{P}_{\Pi(Q),u}(\{\mathfrak{G}_Q\})\prod_{p\in P\setminus Q}\mathbb{P}_{\Pi(P\setminus Q),u}(\{\mathfrak{G}_{P\setminus Q}\})\\ &= \mathbb{P}_{\Pi(Q),u}(\{\mathfrak{G}_Q\})\ \mathbb{P}_{\Pi(P\setminus Q),u}(\{\mathfrak{G}_{P\setminus Q}\})\end{aligned}$$

Ähnlich wie im Beweis von Satz 4.15 teilen wir

$$\mathcal{G} = \{[G\times H]\,|\,\mathfrak{G}\in\mathcal{G}_{\Pi(Q)},\, G\in\mathfrak{G},\, \mathfrak{H}\in\mathcal{G}_{\Pi(P\setminus Q)},\, H\in\mathfrak{H}\}$$

auf und wir können mit Bemerkung 4.4

$$\begin{aligned}M_u(f) &= \mathbb{E}_{\mathbb{P}_u}(f)\\ &= \sum_{\mathfrak{G}\in\mathcal{G}} f(\mathfrak{G})\mathbb{P}_u(\{\mathfrak{G}\})\\ &= \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(Q)}} f(\mathfrak{G})\mathbb{P}_{\Pi(Q),u}(\{\mathfrak{G}\})\sum_{\mathfrak{H}\in\mathcal{G}_{\Pi(P\setminus Q)}}\mathbb{P}_{\Pi(P\setminus Q),u}(\{\mathfrak{H}\})\\ &= \sum_{\mathfrak{G}\in\mathcal{G}_{\Pi(Q)}} f(\mathfrak{G})\mathbb{P}_{\Pi(Q),u}(\{\mathfrak{G}\})\cdot 1\\ &= \mathbb{E}_{\mathbb{P}_{\Pi(Q),u}}(f) = M_{\Pi(Q),u}(f)\end{aligned}$$

berechnen. □

Cohen und Lenstra zeigten in ihrer Arbeit die etwas allgemeinere Aussage

Proposition 4.18. *Korollar 4.17 gilt für alle $u \in \mathbb{Z}^{\geqslant 0}$.*

Beweis. [2, Prop. 5.6] □

Unter Verwendung von Satz 4.15 und Korollar 4.17 respektive Proposition 4.18 können wir nun einige Wahrscheinlichkeiten berechnen:

Beispiel 4.19. Für $u \geqslant 1$ ist die u-Wahrscheinlichkeit der Isomorphieklasse [1] gleich

$$\mathbb{P}_u([1]) = \prod_{j=u+1}^{\infty}\zeta(j)^{-1}.$$

Beispiel 4.20. Für eine Primzahl p und ein $u \geqslant 0$ ist die u-Wahrscheinlichkeit, dass die Ordnung einer zufällig aus $\mathcal{G}$ gezogenen Isomorphieklasse durch p teilbar ist gleich

$$1 - \mathbb{P}_{\Pi(p),u}([1]) = 1 - \prod_{j=u+1}^{\infty} (1 - p^{-j}) =: A_{p,u} = p^{-u-1} + \mathcal{O}(p^{-u-2}).$$

Tabelle 1 wurde mit Wolfram Mathematica 11.0 berechnet und enthält numerische Approximationen der $A_{p,u}$ für $0 \leqslant u \leqslant 3$ und Primzahlen $p \leqslant 19$.

	p=2	p=3	p=5	p=7	p=11	p=13	p=17	p=19
$A_{p,0}$	0.71121	0.43987	0.23967	0.16320	0.09917	0.08283	0.06228	0.05540
$A_{p,1}$	0.42242	0.15981	0.04958	0.02374	0.00908	0.00641	0.00368	0.00292
$A_{p,2}$	0.22990	0.05479	0.00998	0.00340	0.00083	0.00049	0.00022	0.00015
$A_{p,3}$	0.11988	0.01843	0.00200	0.00049	0.00008	0.00004	0.00001	$< 10^{-5}$

Tabelle 1: Numerische Approximationen gewisser $A_{p,u}$.

Beispiel 4.21. Für eine Primzahl p und ein $u \geqslant 0$ ist die u-Wahrscheinlichkeit, dass der p-Anteil einer zufällig gezogenen Gruppe zyklisch ist, gleich

$$\begin{aligned}
\sum_{n \geqslant 0} \mathbb{P}_{\Pi(p),u}([\mathbb{Z}/p^n\mathbb{Z}]) &= \prod_{j=u+1}^{\infty} (1 - p^{-j}) \sum_{n \geqslant 0} |\mathbb{Z}/p^n\mathbb{Z}|^{-u} |\operatorname{Aut}(\mathbb{Z}/p^n\mathbb{Z})|^{-1} \\
&= \prod_{j=u+1}^{\infty} (1 - p^{-j}) \sum_{n \geqslant 0} \frac{1}{p^{un}} \frac{1}{p^n - p^{n-1}} \\
&= \prod_{j=u+1}^{\infty} (1 - p^{-j}) \sum_{n \geqslant 0} \frac{1}{p^{nu+n}} \frac{1}{1 - p^{-1}} \\
&= \left(\prod_{j=u+2}^{\infty} (1 - p^{-j}) \right) \frac{1}{1 - p^{-1}} \\
&= 1 - p^{-u-1} + \mathcal{O}(p^{-u-2}).
\end{aligned}$$

4.2 Die Cohen–Lenstra Vermutung

In diesem Abschnitt werde ich die von Cohen und Lenstra gemachten Vermutungen formulieren.

Definition 4.22. Für eine Menge $\mathcal{K}$ von Zahlkörpern und eine komplexwertige Abbildung f auf Isomorphieklassen endlicher abelscher Gruppen ist *der Durchschnitt von f auf $\mathcal{K}$* der folgende Grenzwert, falls er existiert

$$M_{\mathcal{K}}(f) := \lim_{N \to \infty} \frac{\sum_{K \in \mathcal{K},\, |\Delta_K| \leqslant N} f([\mathrm{Cl}(K)])}{\sum_{K \in \mathcal{K},\, |\Delta_K| \leqslant N} 1}.$$

Sei $\mathcal{K} = \mathcal{K}_{\mathrm{imag},2} := \{\mathbb{Q}(\sqrt{d}) | \, d \in \mathbb{Z}^{<0} \text{ quadratfrei}\}$ die Menge aller in $\mathbb{C}$ enthaltener imaginärquadratischer Zahlkörper. Cohen und Lenstra postulierten für komplexwertige Abbildungen f, die nur vom ungeraden Anteil der Isomorphieklasse abhängen:

Vermutung 4.23. *Endliche, abelsche Gruppen ungerader Ordnung treffen mit einer Häufigkeit invers proportional zur Ordnung derer Automorphismengruppe als ungerader Anteil von Idealklassengruppen imaginärquadratischer Zahlkörper auf. Konkreter gilt:*

$$M_{\mathcal{K}_{\mathrm{imag},2}}(f) = M_0(f)$$

Sei $N \in \mathbb{Z}^{\geqslant 2}$ und $\mathcal{K} = \mathcal{K}_{\text{reell},N} := \{K \subset \mathbb{C} \text{ Körper} \mid [K : \mathbb{Q}] = N,\ K \text{ total reell}\}$. Cohen und Lenstra postulierten für Abbildungen f, die nur vom zu N teilerfremden Anteil abhängen:

Vermutung 4.24. *Endliche, abelsche Gruppen von zu N teilerfremder Ordnung treffen mit einer Häufigkeit invers proportional zur Ordnung derer Automorphismengruppe als zu N teilerfremder Anteil von Idealklassengruppen total reeller Zahlkörper von Grad N über $\mathbb{Q}$ auf. Konkreter gilt:*

$$M_{\text{reell},N}(f) = M_1(f).$$

Aufbauend auf Vermutungen 4.23 und 4.24 konnten Cohen und Lenstra für $N = 2$ einige Phänomene erklären, die schon früher aus Tabellen herausgelesen wurden aber nicht erklärt werden konnten.

Der Fall $N > 2$ wird von Cohen und Lenstra in [2] nur schwach motiviert und stimmt nicht gut mit numerischen Beobachtungen überein. Wir werden im Unterabschnitt 4.4 weitere Versuche, diese und allgemeinere Fälle zu beschreiben, untersuchen.

Wir können nun mit Hilfe von Unterabschnitt 4.1 einige Folgen von den Vermutungen 4.23 und 4.24 besprechen.

Folge 4.25. Für eine Primzahl $p \neq 2$ ist eine abelsche p-Gruppe G mit einer Wahrscheinlichkeit von $\mathbb{P}_{\Pi(p),0}(\{[G]\})$ respektive $\mathbb{P}_{\Pi(p),1}(\{[G]\})$ isomorph zum p-Anteil eines imaginärquadratischen respektive reellquadratischen Zahlkörpers.

Folge 4.26. Die Wahrscheinlichkeit, dass der zu 2 teilerfremde Anteil der Idealklassengruppe eines reellquadratischen Zahlkörpers trivial ist, ist

$$\mathbb{P}_{\Pi(P\setminus\{2\}),1}([1]) = \prod_{p \in P\setminus\{2\}} \prod_{j=2}^{\infty} (1 - p^{-j}) \approx 0.75446.$$

4.3 Motivation für die Cohen Lenstra Heuristik

In Abschnitt 2.4 haben wir natürliche Wahrscheinlichkeitsdichten für die Menge der Isomorphieklassen abelscher p-Gruppen hergeleitet und haben im Unterabschnitt 4.1 gezeigt, dass wir durch die Reduktion von endlichen abelschen Gruppen auf abelsche p-Gruppen nicht an Allgemeinheit verlieren. Wir sind bis jetzt jedoch nicht darauf eingegangen, wie die Anzahl Relationen m in Abhängigkeit vom freien Rang n der erzeugenden Gruppe im Modell zu wählen ist. Dies bestimmt die der Gewichtung der jeweiligen Gruppen in Abhängigkeit der Gruppenordnung. Wir werden dies jetzt heuristisch für den quadratischen Fall nachholen.

Sei dafür K ein quadratischer Zahlkörper und sei für jedes $N \geqslant 0$ die Gruppe $I_{K,N} < J_K$ die Untergruppe, die von der Menge der nichttrivialen Primideale in $\mathcal{O}_K$ mit Norm nicht grösser als N erzeugt wird. Sei $R_{K,N} := \{\frac{a}{b} \in K \mid \forall \mathfrak{p} \subset \mathcal{O}_K \text{ Primideal} : (b) \subset \mathfrak{p} \Rightarrow N(\mathfrak{p}) \leqslant N\} \subset K$ der Unterring aller Elemente, sodass das vom Nenner erzeugte Hauptideal nur Primideale mit Norm nicht grösser als N als Faktoren besitzt. Nach Satz 3.10 ist für N gross genug die Projektion $I_{K,N} \to \mathrm{Cl}(K)$ surjektiv. Einheiten in $R_{K,N}$ sind solche, für die Nenner und Zähler nur durch Primideale von Norm nicht grösser als N teilbar sind. Also existiert ein Gruppenhomomorphismus $R_{K,N}^{\times} \to I_{K,N},\ x \mapsto (x)$. Mit der Inklusion $\mathcal{O}_K^{\times} \to R_{K,N}^{\times}$ erhalten wir folgende exakte Sequenz:

$$1 \longrightarrow \mathcal{O}_K^{\times} \longrightarrow R_{K,N}^{\times} \longrightarrow I_{K,N} \longrightarrow \mathrm{Cl}(K) \longrightarrow 1.$$

Sei M die Anzahl nichttrivialer Primideale von $\mathcal{O}_K$ mit Norm nicht grösser als N. Teilen wir die ersten zwei Gruppen in der obigen Sequenz durch $\mu(K)$, dann sind die in der Sequenz vorkommenden Gruppen von links nach Satz 3.14 freie $\mathbb{Z}$-Moduln vom Rang $0, M, M$ im imaginärquadratischen respektive $1, M+1, M$ im reellquadratischen Fall. Die Klassengruppe von K ist somit isomorph zum Kokern einer linearen Abbildung $\mathbb{Z}^M \to \mathbb{Z}^M$ respektive $\mathbb{Z}^{M+1} \to \mathbb{Z}^M$.

Wie in Abschnitt 2 schon erwähnt, existiert jedoch kein natürliches Wahrscheinlichkeitsmass auf $\mathrm{Hom}(\mathbb{Z}^M, \mathbb{Z}^M)$ respektive $\mathrm{Hom}(\mathbb{Z}^{M+1}, \mathbb{Z}^M)$. Beschränken wir und deshalb auf den p-Anteil der Klassengruppe.

Bilden wir dafür in der oben erwähnten Sequenz für eine Primzahl p das Tensorprodukt mit $\mathbb{Z}_p$ über $\mathbb{Z}$, so erhalten wir aufgrund der Rechtsexaktheit des Tensorproduktes eine rechtsexakte Sequenz

$$R_{K,N}^{\times}/\mu(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow I_{K,N} \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \mathrm{Cl}(K)_p \longrightarrow 1.$$

Nach Unterabschnitten 2.4 und 4.1 entstehen die Vermutungen 4.23 und 4.24 von Cohen und Lenstra im quadratischen Fall aus dem Prinzip, dass die Abbildung $R_{K,N}^{\times}/\mu(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to I_{K,N} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ eine via des Haar Masses zufällige $\mathbb{Z}_p$-lineare Abbildung ist.

Zuletzt möchte ich noch die Cohen Lenstra Heuristik mit numerischen Ergebnissen stärken. In Tabelle 4.3 sind Ergebnisse aus [7] aufgelistet. Für eine Primzahl p gibt hier die Zahl $q_p(D)$ das numerisch berechnete Verhältnis des Anteils durch p teilbarer Klassenzahlen imaginärquadratischer Zahlkörper mit Diskriminante kleiner als D durch den von Cohen und Lenstra vorhergesagten Wert an. Die $q_p(D)$ scheinen für $D \to \infty$ gegen 1 zu streben, jedoch besonders für kleine Primzahlen nur sehr langsam.

D	$q_3(D)$	$q_5(D)$	$q_7(D)$	$q_{11}(D)$	$q_{13}(D)$	$q_{17}(D)$	$q_{19}(D)$
10^9	0.97327	0.99348	0.99609	0.99576	0.99489	0.99474	0.99347
10^{10}	0.98191	0.99653	0.99818	0.99810	0.99812	0.99771	0.99770
10^{11}	0.98770	0.99815	0.99915	0.99919	0.99924	0.99914	0.99910

4.4 Der gerade Anteil der Klassengruppe und nichtquadratische Zahlkörper

Die Cohen–Lenstra Heuristik beschreibt im quadratischen Fall lediglich den ungeraden Anteil der Idealklassengruppe. In ihrer Veröffentlichung [2] begründen die Autoren dies dadurch, dass über die Struktur des 2-Anteil der Idealklassengruppen imaginärquadratischer Zahlkörper durch Gausssche Genus Theorie bereits viel bekannt sei. In der Tat bewies Gauss, dass für eine Diskriminante, die durch r verschiedene Primzahlen geteilt wird, die Idealklassengruppe des dazugehörigen imaginärquadratischen Zahlkörpers den 2-Rang $r-1$ besitzt. Mittlerweile sind mehr Fakten über den 2-Anteil der Idealklassenkörper bekannt.

Im Jahr 1987 veröffentlichten H. Cohen und J. Martinet eine Arbeit, in der sie das Verhalten der Klassengruppen allgemeiner Zahlkörper zu untersuchen versuchten [3]. In ihrer Heuristik führten sie den Begriff der "schlechten Primzahlen" ein. Dies sind Primzahlen p, für die die Heuristik für den p-Anteil scheitert. Sie postulierten, dass zusätzlich zu den Teilern des Körpergrades auch einige Teiler des Grades des Galoischen Abschluss über $\mathbb{Q}$ schlecht sind. Ihre Heuristik scheiterte trotzdem für den Fall $N > 3$, im dem Sinne, dass die vorhergesagten Werte von numerisch berechneten zu stark abweichen.

Im Jahr 2005 verallgemeinerte G. Malle in [9] die Cohen Lenstra Heuristik auf die Betrachtung Idealklassengruppen endlich galoischer Erweiterungen gewisser Zahlkörper. Die Heuristik scheitert für den p-Anteil, falls der Grundkörper eine primitive, p-te Einheitswurzel enthält.

Die Tatsache, dass der 2-Anteil der Idealklassengruppe sich tatsächlich nicht der Cohen Lenstra Heuristik entsprechend verhält, scheint also auch damit zusammen zu hängen, dass der Grundkörper $\mathbb{Q}$ die primitive, 2-te Einheitswurzel -1 enthält.

Literatur

[1] Michael F. Atiyah und Ian G. Macdonald: *Introduction to commutative algebra.* Addison-Wesley Reading, 1969.

[2] Henri Cohen und Hendrik W. Lenstra: *Heuristics on class groups of number fields.* Number Theory Noordwijkerhout, Seiten 33–62, 1983.

[3] Henri Cohen und Jacques Martinet: *Class groups of number fields: numerical heuristics*. Mathematics of Computation, 48(177):123–137, 1987.

[4] Joseph L. Doob: *Measure theory*, Band 143. Springer Science & Business Media, 2012.

[5] Eduardo Friedman und Lawrence C. Washington: *On the distribution of divisor class groups of curves over a finite field*. Théorie des Nombres, Number Theory Laval, 1987.

[6] Fernando Q. Gouvêa: *p-adic Numbers*. Springer, 1997.

[7] Michael J. Jacobson Jr, Shanta Ramachandran und Hugh C. Williams: *Supplementary Tables for Numerical Results on Class Groups of Imaginary Quadratic Fields*, 2006.

[8] Johannes Lengler: *The Cohen-Lenstra heuristic for finite abelian groups*. Doktorarbeit, Universität des Saarlandes, Saarbrücken, 2009.

[9] Gunter Malle: *Cohen–Lenstra heuristic and roots of unity*. Journal of Number Theory, 2008.

[10] Jürgen Neukirch: *Algebraische Zahlentheorie*. In: *Ein Jahrhundert Mathematik 1890–1990*. Springer, 1990.

[11] Dietmar Salamon: *Measure and Integration*. 2016. Preprint, https://people.math.ethz.ch/~salamon/PREPRINTS/measure.pdf.

[12] Elias M. Stein und Rami Shakarchi: *Complex analysis. Princeton Lectures in Analysis, II*. Princeton University Press, 2003.